Manual for the Review and Approval of Prescribed Organizations

Information and Privacy Commissioner of Ontario

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

Contents

Process for the Review and Approval of Prescribed Organizations

Under subsection 55.2 (1) of the *Personal Health Information Protection Act, 2004* ("the *Act*"), the prescribed organization has the power and the duty to develop and maintain the electronic health record in accordance with Part V.1 of the *Act* and the regulations in Ontario Regulation 329/04 made under Part V.1 (the "regulations").

Under subsection 55.2 (2) of the *Act*, the prescribed organization must perform the following functions:

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

Under subsection 55.2 (3) of the *Act*, in addition to carrying out the powers, duties and functions in Part V.1, the prescribed organization is required to carry out any prescribed powers, duties or functions.

For the purpose of Part V.1 of the *Act*, "electronic health record" means the electronic systems that are developed and maintained by the prescribed organization for the purpose of enabling health information custodians to collect, use and disclose personal health information by means of the systems in accordance with Part V.1 and the regulations made under Part V.1.

Subsection 55.1 (3) of the *Act* states that when a health information custodian provides personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record, the health information custodian is considered not to be disclosing the information to the prescribed organization and the prescribed organization is considered not to be collecting the information.

Subsection 55.9.1 (1) of the *Act* states that where the prescribed requirements, if any, are met, the prescribed organization may provide personal health information that is accessible by means of the electronic health record to a coroner in relation to an investigation conducted under the *Coroners Act*. With respect to the provision of personal health information to a coroner, the prescribed organization shall comply with section 55.3 of the *Act* and with the requirements of this *Manual for the Review and Approval of Prescribed Organizations* ("the Manual").

Requirements for a Prescribed Organization

On or after the first anniversary of the day section 55.3 of the *Act* comes in force paragraph 14 of section 55.3 of the *Act* requires the prescribed organization to have in place and comply with practices and procedures that are for the purpose of protecting the privacy of the individuals whose personal health information it receives for the purpose of developing or maintaining the electronic health record and for maintaining the confidentiality of the information, and that are approved by the Information and Privacy Commissioner of Ontario ("IPC"). Subsection 55.12(1) requires the IPC to review the practices and procedures of the prescribed organization referred to in paragraph 14 of section 55.3 every three years after they are first approved to determine if the practices and procedures continue to meet the requirements.

Purpose of this Manual

The purpose of the Manual is to outline the process that will be followed by the IPC in reviewing the practices and procedures put in place by prescribed organizations to protect the privacy of individuals whose personal health information they receive for the purpose of developing and maintaining the electronic health record and to maintain the confidentiality of that information. The purpose is also to set out the obligations arising from the review process.

The Manual may be amended from time to time by the IPC. It is the responsibility of the prescribed organizations to ensure continued compliance with the Manual as amended from time to time.

Review Process for Prescribed Organizations

Each prescribed organization will be required to have in place practices and procedures to protect the privacy of individuals whose personal health information it receives for the purpose of developing and maintaining the electronic health record and to maintain the confidentiality of that information. At a minimum, these practices and procedures must include the policies, procedures, agreements and documentation set out in Appendix "A" and must contain the minimum content set out in Appendix "B" to the Manual. The policies, procedures, agreements and documentation set out in Appendix "A," containing the minimum content set out in Appendix "B," must either be developed and implemented or the policies, procedures, agreements and documentation previously developed and implemented under the Act must be amended to include the minimum content in Appendix "B."

The practices and procedures set out in Appendix "A" are based on an assessment of what would constitute a reasonable combination of practices and procedures given the nature of the functions performed by the prescribed organizations, the amount and sensitivity of the personal health information received for the purpose of developing and maintaining the electronic health record, the number and nature of the individuals with access to the personal health information, as well as the obligations and duties of the prescribed organizations under the Act and its regulation.

The process that will be followed by the IPC in conducting its review will depend on whether the review relates to the initial review of the practices and procedures put in place by the prescribed organization or the ongoing review of these practices and procedures, which is conducted every three years from the date of the initial approval.

Initial Review of the Prescribed Organization

In seeking the initial approval of the IPC, each prescribed organization must submit the applicable practices and procedures described in Appendix "A" to the Manual and containing the minimum content set out in Appendix "B" to the Manual, to the IPC. These practices and procedures must be submitted six months prior to the date that the approval of the IPC is requested.

Upon receipt, the IPC will review the practices and procedures implemented by the prescribed organization and will request any additional documentation and clarifications deemed necessary.

Once any additional documentation and necessary clarifications are received, an on-site meeting will be scheduled between the IPC and representatives of the prescribed organization. The purpose of the on-site meeting is to discuss the practices and procedures put in place by the prescribed organization and to provide the IPC with an opportunity to ask questions arising from the review of the practices and procedures and to review the physical security measures put in place to protect personal health information.

Following the on-site meeting, the prescribed organization will be informed of the actions that they are required to take prior to the approval of its practices and procedures. Once all necessary actions have been taken, the IPC will prepare a draft report and submit the draft report to the prescribed organization for review and comment prior to the report being finalized. Once the report is finalized, it will be posted on the website of the IPC, along with a letter of approval. The report and letter of approval will also be required to be posted on the website of the prescribed organization.

The final report and letter of approval may contain recommendations in respect of the practices and procedures put in place by the prescribed organization pursuant to paragraph 14 of section 55.3 of the *Act* and its regulations. The prescribed organization must comply with the recommendations on or before the date set out in the final report or letter of approval or, if no date is provided, one year prior to the date that the continued approval of their practices and procedures is required under the *Act*.

On or after the first anniversary of the day section 55.3 of the *Act* comes into force, a person or organization may not operate as a prescribed organization unless it has submitted its practices and procedures to the IPC and the IPC has reviewed and approved these practices and procedures and has issued a letter and accompanying report to this effect.

Three-Year Review of the Prescribed Organization

In seeking the continued approval of the IPC, which is required every three years from the date of the initial approval, each prescribed organization must submit a detailed written report, an

assessment of the privacy, security and other indicators and a sworn affidavit to the IPC. The written report, assessment of privacy, security and other indicators, and the sworn affidavit must be submitted to the IPC one year prior to the date that the continued approval is required pursuant to the *Act*.

The written report must demonstrate that the prescribed organization has put in place practices and procedures to protect the privacy of individuals whose personal health information it receives for the purpose of developing and maintaining the electronic health record and to maintain the confidentiality of that information, including the practices and procedures set out in Appendix "A." The written report must also demonstrate that the prescribed organization is adhering to the practices and procedures; that these practices and procedures, at a minimum, contain the content set out in Appendix "B" to this Manual; and that the prescribed organization complied with any recommendations made by the IPC during the prior review and approval of its practices and procedures.

If the prescribed organization has not complied with the requirements in Appendix "A" or Appendix "B" to the Manual or with the recommendations made by the IPC during the prior review and approval of its practices and procedures, the written report of the prescribed organization must provide a rationale for why compliance has not been achieved and must outline a strategy for achieving compliance. The strategy must set out the milestones for achieving compliance, the relevant time frames for achieving compliance and the individual(s) responsible for achieving compliance.

If, in the opinion of the prescribed organization, there is a clear rationale for not complying with one or more of the requirements in Appendix "A" or Appendix "B" to the Manual or one or more of the recommendations made by the IPC during the prior review and approval of its practices and procedures, this must be identified in the written report. The written report must also provide detailed information in support of this opinion.

The assessment of the privacy, security and other indicators must report on, provide information concerning, and assess the performance of the prescribed organization with respect to each of the privacy, security and other indicators set out in Appendix "C" to the Manual for the three-year period immediately before the assessment must be submitted to the IPC.

The sworn affidavit must be in the form set out in Appendix "D" to this Manual and must be executed by the Chief Executive Officer or the Executive Director, as the case may be, who is ultimately accountable for ensuring that the prescribed organization complies with the *Act*. The sworn affidavit requires the Chief Executive Officer or the Executive Director, among other things, to attest that the practices and procedures of the prescribed organization comply with the requirements in this Manual. The sworn affidavit also requires the Chief Executive Officer or Executive Director, as the case may be, to attest that the prescribed organization has taken steps that are reasonable in the circumstances to ensure compliance with the practices and procedures put in place.

Upon receipt, the IPC will review the written report, the assessment of the privacy, security and other indicators and the sworn affidavit and decide, in its sole and absolute discretion, whether

further action is required on the part of the prescribed organization prior to the continued approval of its practices and procedures. The further action may include one or more of the following:

- A full detailed review by the IPC of all the practices and procedures put in place by the prescribed organization;
- A partial detailed review by the IPC of one or more of the practices and procedures implemented by the prescribed organization;
- A request for further information from the prescribed organization with respect to one, more or all of its practices and procedures;
- An on-site meeting between the IPC and representatives of the prescribed organization;
- Requiring the prescribed organization to amend, put in place or adhere to one or more of its practices and procedures or to develop and put in place one or more additional practices and procedures;
- Requiring the prescribed organization to amend the written report, the assessment of the privacy, security and other indicators or sworn affidavit submitted; and/or
- Any other action by the prescribed organization deemed appropriate in the sole and absolute discretion of the IPC.

If further action is warranted, the prescribed organization will be informed of the further action(s) it is required to take prior to the continued approval of its practices and procedures. The prescribed organization must comply with such further action(s) as required by the IPC in order to obtain continued approval of its practices and procedures.

Provided all further actions have been taken in a timely manner and to the satisfaction of the IPC, or in the event that no further action is warranted, the IPC will advise the prescribed organization, in writing, that it continues to meet the requirements of the *Act* and its regulation.

The letter advising the prescribed organization that it continues to meet the requirements of the *Act* and its regulation may contain recommendations in respect of the practices and procedures put in place by the prescribe organization pursuant to the *Act* and its regulation. The prescribed organization must comply with the recommendations of the IPC on or before the date set out in the final report or letter of approval or, if no date is provided, one year prior to the date that continued approval of their practices and procedures is required under the *Act*.

The IPC will then make the letter advising the prescribed organization that it continues to meet the requirements of the Act and its regulation, and the detailed written report, the assessment of the privacy, security and other indicators and the sworn affidavit submitted by the prescribed organization, publicly available on its website at **www.ipc.on.ca**. The prescribed organization will also be required to make this documentation publicly available on its website.

A person or organization may not continue to operate as a prescribed organization unless it has submitted a detailed written report, an assessment of the privacy, security and other indicators and accompanying sworn affidavit to the IPC and the IPC has advised the prescribed organization, in writing, that it continues to meet the requirements of the *Act* and its regulation.

Appendix "A"
List of Required Documentation

Part 1 - Privacy Documentation

Categories	Required Documentation	Page No. Appendix "B"
General Privacy Policies, Procedures and Practices	1. Privacy Policy in Respect of its Status as a Prescribed Organization	12
	2. Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices	17
Transparency	3. Policy on the Transparency of Privacy Policies, Procedures and Practices	18
Receiving Personal Health Information	4. Policy and Procedures for Receiving Personal Health Information	20
	5. List of Types of Personal Health Information Received	22
	6. Policy and Procedures for Descriptions of Types of Personal Health Information Received	23
	7. Descriptions of Types of Personal Health Information Received	24
Managing Consent	8. Policy and Procedures for Managing Consent in the Electronic Health Record	24
	9. Log of Notices of Consent Directives	31
	10. Log of Notices of Consent Overrides	32
	11. Log of Reports of Consent Overrides to the IPC	32
	12. Log of Requests for Electronic Records from Health Information Custodians	32
	13. Log of Requests for Electronic Records from the IPC	33
	14. Log of Audits of the Electronic Records of Consent Directives and Consent Overrides	33
Viewing, Handling or Otherwise Dealing with Personal Health Information	15. Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization	33
	16. Log of Employees and Other Persons Acting on Behalf of the Prescribed Organization Granted Permission to View, Handle or Otherwise Deal with Personal Health Information	38

Categories	Required Documentation	Page No. Appendix "B"
Provision of Personal Health Information Pursuant to Direction	17. Policy and Procedures for the Provision of Personal Health Information Pursuant to a Direction Issued by a Member of a Data Integration Unit of the Minister or by the Minister	38
	18. Log of Directions Issued by a Member of the Data Integration Unit of the Minister or by the Minister	40
Requests for Access and Correction	19. Policy and Procedures for Responding to Requests for Access and Correction of Records of Personal Health Information	41
	20. Log of Access and Correction Requests	45
Agreements with Third Party Service Providers	21. Policy and Procedures for Executing Agreements with Third Party Service Providers	47
	22. Template Agreement for All Third Party Service Providers	49
	23. Log of Agreements with Third Party Service Providers	55
Privacy Impact Assessments	24. Privacy Impact Assessment Policy and Procedures	55
	25. Log of Privacy Impact Assessments	59
Privacy Audits	26. Policy and Procedures in Respect of Privacy Audits	60
	27. Log of Privacy Audits	61
Privacy Breaches, Inquires and Complaints	28. Policy and Procedures for Privacy Breach Management	62
	29. Log of Privacy Breaches	67
	30. Policy and Procedures for Privacy Complaints	69
	31. Log of Privacy Complaints	73
	32. Policy and Procedures for Privacy Inquiries	74

Part 2 - Security Documentation

Categories	Required Documentation	Page No. Appendix "B"
General Security Policies and Procedures	1. Information Security Policy	76
	2. Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices	78
Physical Security	3. Policy and Procedures for Ensuring Physical Security of Personal Health Information	80
	4. Log of Employees or Other Persons Acting on behalf of the Prescribed Organization with Access to the Premises of the Prescribed Organization	85
Retention, Transfer and Disposal	5. Policy and Procedures for Secure Retention of Records of Personal Health Information	85
	6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	87
	7. Policy and Procedures for Secure Transfer of Records of Personal Health Information	91
	8. Policy and Procedures for Secure Disposal of Records of Personal Health Information	93
Information Security	9. Policy and Procedures Relating to Passwords	96
	10. Policy and Procedures In Respect of Privacy Notices	97
	11. Policy and Procedures for Acceptable Use Agreements with Employees and Other Persons Acting On Behalf of the Prescribed Organization	98
	12. Template Acceptable Use Agreement with Employees and Other Persons Acting On Behalf of the Prescribed Organization	100
	13. Log of Acceptable Use Agreements	101
	14. Policy and Procedures for End User Agreements	102
	15. Template End User Agreements	103
	16. Log of End User Agreements	104
	17. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs	104
	18. Log of Requests for Electronic Records from Health Information Custodians	109
	19. Log of Requests for Electronic Records from the IPC	110
	20. Policy and Procedures for Patch Management	110

Categories	Required Documentation	Page No. Appendix "B"
Information Security (Cont'd)	21. Policy and Procedures Related to Change Management	112
	22. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information	114
	23. Policy and Procedures on the Acceptable Use of Technology	116
	24. Threat and Risk Assessment Policy and Procedures	117
	25. Log of Threat and Risk Assessments	119
Security Audits	26. Policy and Procedures In Respect of Security Audits	119
	27. Log of Security Audits	121
Information Security Breach Management	28. Policy and Procedures for Information Security Breach Management	121
	29. Log of Information Security Breaches	127

Part 3 - Human Resources Documentation

Categories	Required Documentation	Page No. Appendix "B"
Privacy Training and Awareness	1. Policy and Procedures for Privacy Training and Awareness	129
	2. Log of Attendance at Initial and Ongoing Privacy Training	133
Security Training Awareness	3. Policy and Procedures for Security Training and Awareness	133
	4. Log of Attendance at Initial and Ongoing Security Training	136
Confidentiality Agreements	5. Policy and Procedures for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on Behalf of the Prescribed Organization	137
	6. Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization	138
	7. Log of Executed Confidentiality Agreements with Employees and Other Persons Acting on Behalf of the Prescribed Organization	140
Responsibility for Privacy and Security	8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program	141
	9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program	142
Termination of Relationship	10. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship	143
Discipline	11. Policy and Procedures for Discipline and Corrective Action	144

Part 4 - Organizational and Other Documentation

Categories	Required Documentation	Page No. Appendix "B"
Governance	1. Privacy Governance and Accountability Framework	145
	2. Security Governance and Accountability Framework	146
	3. Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program	147
Risk Management	4. Corporate Risk Management Framework	147
	5. Corporate Risk Register	150
	6. Policy and Procedures for Maintaining a Consolidated Log of Recommendations	151
	7. Consolidated Log of Recommendations	151
Business Continuity and Disaster Recovery	8. Business Continuity and Disaster Recovery Plan	152

Appendix "B"
Minimum Content of Required Documentation[1]

Part 1 - Privacy Documentation

1. Privacy Policy in Respect of its Status As a Prescribed Organization

An overarching privacy policy must be developed and implemented in relation to personal health information received by the prescribed organization under Part V.1 of the *Act* ("the Privacy Policy"). At a minimum, the Privacy Policy must address the matters outlined below.

Status under the *Act*

The Privacy Policy must describe the status of the prescribed organization as defined in section 2 of the *Act* and the duties and responsibilities imposed on the prescribed organization pursuant to this status. The Privacy Policy must indicate that the prescribed organization has put in place policies, procedures and practices to protect the privacy of individuals whose personal health information it receives for the purpose of developing or maintaining the electronic health record pursuant to section 55.2 of the *Act*, and to maintain the confidentiality of that information. It must also provide that these policies, procedures and practices are subject to review by the IPC every three years.

If the prescribed organization engages in activities or roles that are otherwise regulated by the *Act* it should have appropriate policies and procedures in place that address the requirements of those other activities and roles. However, this *Manual for the Review and Approval of Prescribed Organizations* applies only to the prescribed organization's role as a "prescribed organization" as that term is defined in section 2 of the *Act*.

The Privacy Policy must also articulate a commitment on behalf of the prescribed organization to comply with the provisions of the *Act* and its regulations applicable to the prescribed organization.

Privacy and Security Accountability Framework

The accountability framework for ensuring compliance with the *Act* and its regulations and for ensuring compliance with the privacy and security policies, procedures and practices put in place by the prescribed organization must also be articulated. In particular, the Privacy Policy must indicate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring compliance with the *Act* and its regulations and for ensuring compliance with the policies, procedures and practices put in place.

The Privacy Policy must also identify the position(s) that have been delegated day-to-day authority to manage the privacy program and the security program and to whom these positions report. It must further identify the duties and responsibilities of the position(s) that have been

1 Note that policies, procedures, agreements and documentation containing the minimum content set out in this Appendix must either be developed and implemented or the policies, procedures, agreements and documentation previously implemented under the *Act* must be amended to include the minimum content in this Appendix.

delegated day-to-day authority to manage the privacy program and the security program and some of the key activities of these programs. The Privacy Policy should also identify other positions or committees that support the privacy program and/or the security program and their role in respect of these programs.

Authority to Receive Personal Health Information

The Privacy Policy must describe the authority by which the prescribed organization is permitted to receive personal health information from health information custodians for the purpose of developing and maintaining the electronic health record, pursuant to section 55.2 of the *Act*.

The Privacy Policy must state that the prescribed organization receives personal health information for the purpose of developing or maintaining the electronic health record. The Privacy Policy must describe the types of personal health information received for this purpose and the persons or organizations from which personal health information is typically received.

Consent Management

The Privacy Policy must set out the process for managing directives made by individuals to withhold or withdraw, in whole or part, the individual's consent to the collection, use and disclosure of his or her personal health information that is accessible by means of the electronic health record for the purpose of providing or assisting in the provision of health care to the individual. The information provided must include the name and/or title, mailing address and contact information for the employee(s) or other person(s) acting on behalf of the prescribed organization to whom directives may be submitted and the manner and format in which these directives may be submitted. The Privacy Policy must also set out the level of specificity as prescribed in the regulations at which personal health information may be made subject to a consent directive, including whose collection, use and disclosure of the information may be restricted. The Privacy Policy must also specify data elements that a health information custodian may collect, use or disclose for the purpose of uniquely identifying an individual in order to collect personal health information by means of the electronic health record that may not be made subject to a consent directive provided by the individual.

Minimizing the Personal Health Information Received

The Privacy Policy must articulate a commitment to and the reasonable steps taken by the prescribed organization to limit the personal health information it receives to that which is reasonably necessary for the purpose of developing or maintaining the electronic health record. In this regard, the Privacy Policy must outline the policies, procedures and practices put in place by the prescribed organization to ensure that both the amount and the type of personal health information received is limited to that which is reasonably necessary for its purpose.

The Privacy Policy must also contain a list of the types of personal health information maintained by the prescribed organization and must identify where an individual may obtain further information in relation to the types and sources of the personal health information received for the purpose of developing or maintaining the electronic health record.

Viewing, Handling or Otherwise Dealing with Personal Health Information

The purposes for which employees or any other persons acting on behalf of the prescribed organization, may view, handle, or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record must be identified. The Privacy Policy must specify that the prescribed organization does not permit its employees or any other person acting on its behalf to view, handle or otherwise deal with the personal health information received for the purpose of developing or maintaining the electronic health record, unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the prescribed organization.

The Privacy Policy must further articulate a commitment by the prescribed organization not to permit its employees or any other person acting on its behalf to view, handle or otherwise deal with personal health information if other information, such as de-identified or aggregate information, will serve the purposes identified. It must further articulate a commitment not to allow its employees and any other person acting on its behalf to view, handle or otherwise deal with more personal health information than is reasonably necessary to meet the purposes identified. The policies, procedures and practices put in place to support these commitments must also be outlined.

The Privacy Policy should also state that the prescribed organization remains responsible for personal health information viewed, handled or otherwise dealt with by its employees and any other persons acting on its behalf and should identify the policies, procedures and practices implemented to ensure that its employees and any other person acting on its behalf only view, handle or otherwise deal with personal health information in compliance with the *Act* and its regulations and in compliance with the privacy and security policies, procedures and practices put in place.

Providing Personal Health Information to Another Person

The Privacy Policy must state that the prescribed organization may not provide personal health information to any person, except as permitted or required by the *Act* and its regulations.

The Privacy Policy must specify that a member of a ministry data integration unit located within the Minister of Health ("the Minister") may issue a direction requiring the prescribed organization to provide to the member of the data integration unit personal health information that is accessible by means of the electronic health record that the member of the data integration unit is permitted to collect under subsection 55.9 (1) of the *Act* and that the prescribed organization must comply with such a direction. The Privacy Policy must state the limited purposes for which the member of the data integration unit is permitted to collect personal health information under subsection 55.9 (1) of the *Act*.

The Privacy Policy must specify that under subsection 55.10 (1) of the *Act* the Minister may direct the disclosure of personal health information that is accessible by means of the electronic health record, as if the Minister had custody and control of the information, in accordance with clause 39(1)(c), subsection 39(2), section 44 or 45 of the *Act* and the prescribed organization must comply with the direction.

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

Secure Retention, Transfer and Disposal

The Privacy Policy must address the secure retention of records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record in both paper and electronic format. This includes how long records of personal health information are retained, whether the records are retained in identifiable form and the secure manner in which they are retained.

It must also address the manner in which records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record, in both electronic and paper format, will be securely transferred and disposed of.

Implementation of Administrative, Technical and Physical Safeguards

The Privacy Policy must outline some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information it receives for the purpose of developing and maintaining the electronic health record and to maintain the confidentiality of that information. This shall include the steps taken to ensure that personal health information accessible by means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of the personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal.

Inquiries, Concerns or Complaints

The Privacy Policy is required to identify the employee(s) and other person(s) acting on behalf of the prescribed organization to whom and the manner in which individuals may direct inquiries, concerns or complaints related to the compliance of the prescribed organization with the *Act* and its regulations and the privacy policies, procedures and practices the prescribed organization has put in place pursuant thereto.

The Privacy Policy is also required to identify the employee(s) and other person(s) acting on behalf of the prescribed organization to whom and the manner in which individuals may direct inquiries, concerns and complaints related the privacy policies, procedures and practices of one or more health information custodians who collect, use or disclose personal health information by means of the electronic health record and related to the compliance of the health information custodians with the *Act* and its regulations.

The information provided must include the name and/or title, mailing address and contact information for the employees(s) and other persons acting on behalf of the prescribed organization to whom individuals may direct such inquiries, concerns or complaints.

It must also state that individuals may direct complaints regarding the compliance of the prescribed organization or one or more health information custodians who collect, use or

disclose personal health information by means of the electronic health record with the *Act* and its regulations to the IPC and provide the mailing address and contact information for the IPC.

Access and Correction

The Privacy Policy must set out the practices and procedures that enable the prescribed organization to respond to a request made by an individual under Part V of the *Act* to access or correct: a record of the individual's personal health information that is accessible by means of the electronic health record; or the electronic records kept by the prescribed organization under paragraphs 4, 5, and 6 of section 55.3 of the *Act*. The information provided must include the name and/or title, mailing address and contact information for the employee(s) or other person(s) acting on behalf of the prescribed organization to whom requests for access or correction may be made and the manner and format in which these requests may be made. It must also state that individuals may direct complaints related to access and correction to the IPC.

The Privacy Policy must also set out the practices and procedures that have been approved by the Minister for responding to or facilitating a response to a request made by an individual to a health information custodian under Part V of the *Act* to access or correct a record of the individual's personal health information that is accessible by means of the electronic health record.

Transparency of Practices

The Privacy Policy must state that the prescribed organization makes available to the public and to each health information custodian that provided personal health information to it for the purpose of developing or maintaining the electronic health record, a plain language description of the electronic health record, including a general description of the administrative, technical and physical safeguards in place, and any directives, guidelines and policies of the prescribed organization that apply to the personal health information that is accessible by means of the electronic health record.

The Privacy Policy must state that the prescribed organization makes available to each health information custodian that provided personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record, for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record, a written copy of the result of an assessment with respect to the threats, vulnerabilities and risks to the security and integrity of the personal health information that is accessible by means the electronic health record and how each system may affect the privacy of the individuals to whom the information relates.

The Privacy Policy must state that the prescribed organization makes available to the public, for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record, a summary of the result of an assessment with respect to the threats, vulnerabilities and risks to the security and integrity of the personal health information accessible by means of the electronic health record and how each system may affect the privacy of the individuals to whom the information relates.

The Privacy Policy must also identify where individuals may obtain further information in relation to the privacy policies, procedures and practices of the prescribed organization.

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

A policy and associated procedures must be developed and implemented to address the ongoing review of the privacy policies, procedures and practices put in place by the prescribed organization pursuant to the *Act* and its regulations. The purpose of the review is to determine whether amendments are needed and/or whether new privacy policies, procedures and practices are required.

The policy and procedures must identify the frequency of the review, the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for undertaking the review, the procedure to be followed in undertaking the review and the time frame in which the review will be undertaken. At a minimum, the privacy policies, procedures and practices put in place by the prescribed organization must be reviewed by the responsible person(s) at least once prior to each scheduled review of these policies, procedures and practices by the IPC pursuant to section 55.12 of the *Act* and whenever the Minister issues a directive to the prescribed organization with respect to the carrying out of its responsibilities and functions. The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the procedure to be followed in amending and/or drafting new privacy policies, procedures and practices deemed necessary as a result of the review, and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the procedure that must be followed in obtaining approval of any amended and/or newly developed privacy policies, procedures and practices.

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

- Any directives made to the prescribed organization by the Minister pursuant to section 55.4 of the *Act*;
- Any orders, decisions, guidelines, fact sheets and best practices issued by the IPC under the *Act* and its regulations;
- Evolving industry privacy standards and best practices;
- Amendments to the *Act* and its regulations relevant to the prescribed organization; and
- Recommendations arising from privacy and security audits, privacy impact assessments, and investigations into privacy complaints, privacy breaches and information security breaches.

It must also take into account whether the privacy policies, procedures and practices put in place continue to be consistent with actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices put in place.

The policy and its associated procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the procedure to be followed in communicating the amended or newly developed privacy policies, procedures and practices, including the method and nature of the communication. It shall also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the procedure to

be followed in reviewing and amending the communication materials available to the public, each health information custodian that provided the personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record and other stakeholders as a result of the amended or newly developed privacy policies, procedures and practices.

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

The policy and procedures must require employees and other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

A policy must be developed and implemented to address the information made available to the public and to each health information custodian that provided personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record relating to the privacy policies, procedures and practices put in place by the prescribed organization and that identifies the means by which such information is made available. At a minimum, the policy must require the following information be made available.

The following information must be made available to the public and each health information custodian that provided personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record:

- The Privacy Policy;
- Documentation related to the review by the IPC of the policies, procedures and practices put in place by the prescribed organization pursuant to the *Act* and its regulation.
- A list of each of the repositories that are accessible by means of the electronic health record and a description of the types of personal health information in each;

- A plain language description of the electronic health record including a general description of the administrative, technical and physical safeguards in place to:
    - protect the personal health information that is accessible by means of the electronic health record against theft, loss and unauthorized collection, use or disclosure;
    - protect the personal health information that is accessible by means of the electronic health record against unauthorized copying, modification or disposal; and
    - protect the integrity, security and confidentiality of the personal health information that is accessible by means of the electronic health record: and
- Any directives, guidelines and policies that apply to the personal health information that is accessible by means of the electronic health record, to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information.
- A description of the privacy policies, procedures and practices put in place in respect of personal health information, including:
    - the types of personal health information received and the persons or organizations from which this personal health information is typically received;
    - the purposes for which employee(s) or other person(s) acting on behalf of the prescribed organization may view, handle or otherwise deal with personal health information; and
    - the fact that the prescribed organization is required to comply with a directive issued by the Minister to provide personal health information to the Minister or to disclose personal health information to a person, in accordance with clause 39(1)(c), subsection 39(2) or section 44 or 45 of the *Act*.

The following information must be made available to the public:

- A summary of the results of the threat and risk assessments and privacy impact assessments that are performed for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record;
- The name and/or title, mailing address and contact information of the employee(s) or other person(s) acting on behalf of the prescribed organization to whom individuals may direct:
    - requests to make directives to withhold or withdraw, in whole or part, consent to the collection, use and disclosure of their personal health information by means of the electronic health record by a health information custodian for the purpose of providing or assisting in the provision of health care to the individual;
    - inquiries, concerns or complaints regarding compliance with *Act* and its regulation. and the privacy policies, procedures and practices put in place pursuant thereto; and
    - requests for access to or correct of their records of personal health information that are accessible by means of the electronic health record developed or maintained by the prescribed organization.

A written copy of the results of the threat and risk assessments and privacy impact assessments that relate to the personal health information the health information custodian provided to the prescribed organization must be made available to each health information custodian that provided personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record.

The policy and procedures must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

4. Policy and Procedures for Receiving Personal Health Information

A policy and procedures must be developed and implemented to identify the purpose for which personal health information will be received by the prescribed organization, the nature of the personal health information that will be received, from whom the personal health information will typically be received and the secure manner in which personal health information will be received.

The policy and procedures must require the prescribed organization to take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for developing and maintaining the electronic health record. The policy and procedures must also require the prescribed organization to receive the personal health information that classes of health information custodians or specific health information custodians are required to provide to the prescribed organization pursuant to the regulations.

Review and Approval Process

The policy and procedures must set out the process to be followed in reviewing and determining what personal health information the prescribed organization should receive for the purpose of developing and maintaining the electronic health record, other than the personal health information, if any, that classes of health information custodians or specific health information custodians are required to provide to the prescribed organization, pursuant to the regulations.

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for reviewing and determining whether to approve the receipt of personal health information for the purpose of developing or maintaining the electronic

health record. The policy and procedures must further set out the process that must be followed; the requirements, conditions or restrictions that must be considered in this regard; and the steps that must be taken to ensure that the personal health information is not received without authority.

The policy and procedures must further set out the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve the receipt of personal health information for the purposes of developing or maintaining the electronic health record.

At a minimum, the criteria must require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve the receipt of personal health information to ensure that the receipt is permitted by the *Act* and its regulations; and that any and all conditions or restrictions set out in the *Act* and its regulations or by the Minister have been satisfied. The criteria must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve the receipt of personal health information to ensure that the personal health information received by the prescribed organization is limited to that which is reasonably necessary for the purpose of developing or maintaining the electronic health record.

The policy and procedures should also set out the manner in which the decision approving or denying the receipt of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; and the required content of the documentation.

Conditions or Restrictions on the Approval

The policy and procedures must identify the conditions or restrictions that are required to be satisfied prior to the receipt of personal health information for the purpose of developing or maintaining the electronic health record, including any documentation and/or agreements that must be completed, provided or executed and the employee(s) or other person(s) acting on behalf of the prescribed organization and other persons or organizations responsible for completing, providing, executing or ensuring the execution of the documentation and/or agreements. The conditions or restrictions identified in the policy and procedures, including the documentation and/or agreements that must be completed, provided or executed, shall have regard to the requirements of the *Act* and its regulations and any directions issued by the Minister.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that any conditions or restrictions that must be satisfied prior to the receipt of personal health information for the purpose of developing or maintain the electronic health record have in fact been satisfied.

Secure Retention

The policy and procedures must require records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record to be retained in a secure manner in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

Secure Transfer

The policy and procedures must require records of personal health information received for the purpose of developing or maintaining the electronic health record to be transferred to the prescribed organization in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

Secure Disposal

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that the records of personal health information that have been received for the purpose of developing or maintaining the electronic health record are securely disposed of following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the receipt of the personal health information for the purpose of developing or maintaining the electronic health record.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employees(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

5. List of Types of Personal Health Information Received

The prescribed organization shall develop and retain an up-to-date list of each of the repositories that are accessible by means of the electronic health record and a description of the types of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record that are contained in each repository.

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

A policy and procedures must be developed and implemented with respect to the creation, review, amendment and approval of descriptions of types of personal health information received for the purpose of developing or maintaining the electronic health record. The policy and procedures shall require the descriptions to set out an up-to-date list of the types of personal health information received for the purpose of developing or maintaining the electronic health record (e.g., demographic, laboratory, drugs); a description of the personal health information (e.g., requisitions, orders, results); the source(s) of the personal health information (e.g., Minister, laboratories, hospitals); the repository in which the personal health information is contained; and whether or not the personal health information is received pursuant the regulations.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in completing the descriptions of types of personal health information received for the purpose of developing or maintaining the electronic health record, including the employee(s) or other person(s) acting on behalf of the prescribed organization and other persons or organizations that must be consulted in completing the descriptions of types of personal health information received and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for approving the descriptions of types of personal health information received. The role of the employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program in respect of the descriptions of types of personal health information received shall also be specified.

The persons and organizations that will be provided the descriptions of types of personal health information received shall also be identified. At a minimum, this should include the health information custodians or other persons or organizations from whom the personal health information is received.

The policy and procedures shall further require that the descriptions of types of personal health information received be reviewed on an ongoing basis in order to ensure their continued accuracy and in order to ensure that the personal health information received for the purpose of developing or maintaining the electronic health record is still necessary for the identified purpose. In this regard, the frequency with which and the circumstances in which the descriptions of types of personal health information received are required to be reviewed must be identified.

The employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in reviewing the descriptions of types of personal health information received and in amending the descriptions of types of personal health information received, if necessary, shall also be documented. This shall include the employee(s) or other person(s) acting on behalf of the prescribed organization or other persons or organizations that must be consulted in reviewing, and if necessary, amending the descriptions of types of personal health information received and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for approving the amended descriptions of types of personal health information received. The policy and procedures must further identify the persons and organizations that will be provided with amended descriptions of types of personal health

information received upon approval, including health information custodians or other persons or organizations from whom the personal health information is received.

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

7. Descriptions of Types of Personal Health Information Received

For each type of personal health information received for the purpose of developing or maintain the electronic health record, the prescribed organization must draft a description of the types of personal health information received (e.g., demographic, laboratory, drugs), a description of the personal health information (e.g., requisitions, orders, results); the source(s) of the personal health information (e.g., Minister, laboratories, hospitals); the repository in which the personal health information is contained; and whether or not the personal health information is received pursuant to the regulations.

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

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

The policy and procedures must require the prescribed organization to implement a consent directive when requested to do so by an individual. It must also require the prescribed organization to withdraw or modify a directive when requested to do so by the individual.

The policy and procedures must set out the level of specificity at which personal health information may be made subject to a consent directive, including whose collection, use and disclosure of the information may be restricted and, at a minimum, this must include the level of specificity prescribed in the regulations.

The policy and procedures must specify the data elements that may be collected, used or disclosed by a health information custodian for the purpose of uniquely identifying an individual in order to collect personal health information by means of the electronic health record that may not be made subject to a consent directive provided by the individual and this must be consistent with the data elements that may not be made subject to a consent directive prescribed in the regulations.

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

- The specificity at which personal health information may be made subject to a consent directive, including whose collection, use and disclosure of the information may be restricted;
- Any data elements that may not be made subject to a consent directive; and
- The name and/or title, mailing address and contact information of the employee(s) or other person(s) acting on behalf of the prescribed organization to whom such requests may be submitted and the manner and format in which individuals may submit requests to make, modify or withdraw consent directives.

Receiving Requests for Consent Directives

The policy and procedures shall establish the process to be followed in receiving requests to make, modify or withdraw consent directives in accordance with section 55.6 of the *Act*. This shall include the nature of the information to be requested from the individual submitting the request; any documentation that must be completed, provided and/or executed by the individual making the request; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving the request; any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the documentation must be completed and provided.

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

Implementing and Testing Consent Directives

The policy and procedures must establish the process to be followed in implementing an individual's request to make, modify or withhold a consent directive. In this regard, the policy must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the request; the manner in which the consent directive must

be implemented; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the request must be implemented and the documentation must be provided. The policy and procedures must require consent directives to be implemented in accordance with the requirements prescribed in the regulations, if any.

The policy and procedures must require the prescribed organization to take reasonable steps to test to ensure that requests to make, modify or withdraw a consent directive have been properly implemented. In this regard, the policy and procedures must establish the process to be followed in testing to ensure that requests have been properly implemented; identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing to ensure that the request has been properly implemented; the manner in which the testing must be done; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the testing must be completed and the documentation provided.

The policy and procedures must establish a process to be followed for notifying an individual that a consent directive has been implemented. In this regard, the policy must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying individuals; the manner in which the notice must be provided; the required content of the notice; the documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the notice must be provided and the documentation provided.

Keeping an Electronic Record of and Auditing and Monitoring Consent Directives

The policy and procedures must require the prescribed organization to keep an electronic record of all instances where a consent directive is made, modified or withdrawn, as required by paragraph 5 of section 55.3 of the *Act*. The electronic record shall identify the individual who made, withdrew or modified the consent directive, the instructions that the individual provided regarding the consent directive, the health information custodian, agent or other person to whom the directive was made, withdrawn or modified, and the date and time that the consent directive was made, withdrawn or modified.

The policy and procedures must require the prescribed organization, as required by paragraph 7 of section 55.3 of the *Act,* to continuously audit and monitor the electronic record of all instances where a consent directive is made, withdrawn or modified to ensure that the consent

directive continues to apply as requested. The policy and procedures must establish the process for continuously auditing and monitoring the electronic record to ensure that the consent directive continues to apply. In this regard, the policy must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for continuously auditing and monitoring to ensure that consent directives continue to apply; the manner in which this continuous auditing and monitoring shall be done; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the documentation must be provided.

Providing Notice of Consent Directives

If a health information custodian seeks to collect personal health information that is subject to a consent directive, the policy and procedures must require the prescribed organization to notify the health information custodian that an individual has made a directive without providing any personal health information that is subject to the directive, in accordance with subsection 55.6 (7) of the *Act*. The policy and procedures must establish a process to be followed in notifying a health information custodian that an individual has made a consent directive. In this regard, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that a custodian has been notified of a consent directive; the manner in which the notice must be provided; the required content of the notice; any documentation that must be completed, provided or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring that execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the documentation must be provided.

Overrides of Consent Directives

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

- Obtains the express consent of the individual to whom the information relates;
- Believes, on reasonable grounds, that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom it relates and it is not reasonably possible for the health information custodian that is seeking to collect the personal health information to obtain the individual's consent in a timely manner; or

- Believes, on reasonable grounds, that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom it relates or a group of persons.

The policy and procedures must set out the process to be followed in overriding a consent directive. In this regard, the policy must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the health information custodians are able to override a consent directive; the manner in which a consent directive may be overridden; the documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that consent directives can be overridden and/or by the custodian that overrides the consent directive; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensure the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization or other persons to whom this documentation must be provided, and the time frame within which the documentation must be provided. At a minimum, the policy and procedures must require the prescribed organization to notify the custodian in the event that the custodian overrides a consent directive.

Keeping an Electronic Record of and Auditing and Monitoring Consent Overrides

The policy and procedures must require the prescribed organization to keep an electronic record of all instances where a consent directive is overridden by a health information custodian, as required by paragraph 6 of section 55.3 of the *Act*. The electronic record shall identify the health information custodian that disclosed the information, the health information custodian that collected the information, any agent of the health information custodian who collected the information, the individual to whom the information relates, the type of information that was disclosed, the date and time of the disclosure and the purpose of the disclosure (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to another person or group of persons).

The policies and procedures must require the prescribed organization, as required by paragraph 7 of section 55.3 of the *Act,* to audit and monitor the electronic record of all instances where a consent directive is overridden by a health information custodian. In this regard, the policy must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for auditing and monitoring the consent override; the manner in which this auditing and monitoring shall be done; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing or ensuring the execution of the documentation; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided, and the time frame within which the documentation must be provided.

Providing Notice of Consent Overrides

The policy and procedures must set out the process that must be followed in notifying health information custodians about consent overrides, as required by subsection 55.7 (6) of the *Act*. At a minimum, where personal health information that has been made subject to a consent directive has been collected by a health information custodian pursuant to a consent override, the policy and procedures must require the prescribed organization to immediately provide written notice, in accordance with the requirements prescribed in the regulations, to the health information custodian that collected the information. The policy and procedures must set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying consent overrides and for notifying health information custodians about consent overrides; and the form, manner and time frame within which the notice must be provided which must be in accordance with the requirements in the regulations.

The policy and procedures must set out the information that must be contained in the notice. At a minimum, the notice must set out the name of the individual to whom the information relates; the name of any agent of the health information custodian who collected the information, if available; a general description of the type of personal health information that was collected; the reason or reasons for the consent override as described in the *Act* (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to another person or group of persons); and the date and time of the collection.

Reporting Consent Overrides to the IPC

The policy and procedures must require the prescribed organization to submit to the IPC, at least annually, a report based on or containing any information, other than personal health information, that is kept in the electronic record that the prescribed organization is required to keep of every instance where personal health information that is accessible by means of the electronic health record that is the subject of a consent directive is disclosed pursuant to a consent override since the time of the last report, as required by paragraph 16 of section 55.3 of the *Act*. The policy and procedures must set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for preparing the report; the form and manner of the report which must be in accordance with that specified by the IPC; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the report must be provided; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for approving the report; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for providing the report to the IPC; and the time frame within which the report must be provided to the IPC.

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

The policy and procedures shall set out the process that must be followed in responding to requests from health information custodians pursuant to paragraph 9 of section 55.3 of the *Act* for the electronic records of consent directives and consent overrides that the prescribed organization is required to keep pursuant to paragraphs 5 and 6 of section 55.3 of the *Act*. At a

minimum, the policy and procedures shall indicate that the prescribed organization must provide, upon the request of a health information custodian that requires the records to audit and monitor its compliance with the *Act*, the electronic records that the prescribed organization is required to keep under the *Act*. The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving requests for electronic records from health information custodians; for preparing the electronic records requested by health information custodians and for providing the requested information to health information custodians; any documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization and/or the health information custodian requesting the electronic records; the employee(s) or other person acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. In setting out the process for responding to requests, the policy and procedures must specify the form, manner and time frame within which the electronic records requested by health information custodians must be provided.

The policy and procedures shall also set out the process that must be followed in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of the *Act* for the electronic records that the prescribed organization is required to keep pursuant to paragraphs 5 and 6 of section 55.3 of the *Act*. At a minimum, the policy and procedures shall indicate that the prescribed organization must provide, upon the request of the IPC, the electronic records that the prescribed organization is required to keep under the *Act* to the IPC for the purposes of Part VI of the *Act*. The policy and procedures must set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving requests for electronic records from the IPC; for preparing the electronic records requested by the IPC and for providing the requested information to the IPC; any documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization and/or the IPC; the employee(s) or other person acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. In setting out the process for responding to requests, the policy and procedures must specify the form, manner and time frame within which the electronic records requested by the IPC must be provided.

Logging

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

- All instances where a notice of a consent directive is provided to a health information custodian pursuant to subsection 55.6 (7) of the *Act*;
- All instances where a notice of a consent override is provided to a health information custodian pursuant to subsection 55.7 (6) of the *Act*;

- All instances where a report of consent overrides is provided to the IPC pursuant to paragraph 16 of section 55.3 of the *Act*;
- All requests from the IPC, made pursuant to paragraph 8 of section 55.3 of the *Act*, for the electronic records the prescribed organization is required to maintain pursuant to paragraphs 5 and 6 of section 55.3 of the *Act*;
- All requests from health information custodians, made pursuant to paragraph 9 of section 55.3 of the *Act*, for the electronic records the prescribed organization is required to maintain pursuant to paragraphs 5 and 6 of section 55.3 of the *Act*; and
- The audits, required by paragraph 7 of section 55.3 of the *Act*, of the electronic records that the prescribed organization is required to keep under paragraphs 5 and 6 of section 55.3 of the *Act*.

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining each log and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for auditing and monitoring the log to ensure that notices of consent overrides are provided to individuals and reports of consent overrides are provided to the IPC.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

9. Log of Notices of Consent Directives

The prescribed organization shall maintain a log of notices of consent directives that have been provided to a health information custodian pursuant to subsection 55.6 (7) of the *Act*. At a minimum, the log must set out the employee(s) or other person(s) acting on behalf of the prescribed organization who sent the notice; the health information custodian to whom the notice was sent; the date the notice was sent; the individual to whom the personal health information relates; and the type of personal health information subject to the consent directive.

If an override of the consent directive is made pursuant to section 55.7 of the *Act,* the log must set out the health information custodian that disclosed the personal health information as a result of the override; the name of any agent who collected the personal health information on a custodian's behalf; the date and time of the collection; and the purpose of the collection (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to a person other than the individual to whom the information relates or to a group of persons).

10. Log of Notices of Consent Overrides

The prescribed organization shall maintain a log of notices of consent overrides that have been sent to health information custodians pursuant to subsection 55.7 (6) of the *Act*. At a minimum, the log must set out the employee(s) or other person(s) acting on behalf of the prescribed organization who sent the notice; the health information custodian to whom the notice was sent; the date the notice was sent; the health information custodian that disclosed the personal health information as a result of the override; the name of any agent who collected the personal health information on a custodian's behalf; the individual to whom the personal health information relates; the type of personal health information that was collected; the date and time of the collection; and the purpose of the collection (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to a person other than the individual to whom the information relates or to a group of persons).

11. Log of Reports of Consent Overrides to the IPC

The prescribed organization shall maintain a log of annual reports provided to the IPC based on or containing any information, other than personal health information, that is kept in the electronic record that the prescribed organization is required to keep of every instance where personal health information that is accessible by means of the electronic health record that is the subject of a consent directive is disclosed since the time of the last report pursuant to paragraph 16 of subsection 55.3 of the *Act*. At a minimum, for each annual report, the log must set out the employee(s) or other person(s) acting on behalf of the prescribed organization who sent the report to the IPC; the employee(s) or other person(s) acting on behalf of the IPC to whom the report was sent; the date the report was sent; and the date by which the next annual report must be sent to the IPC.

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

The prescribed organization shall maintain a log of the electronic records that are provided to health information custodians, pursuant to paragraph 9 of section 55.3 of the *Act*. At a minimum, for each request for electronic records received from a health information custodian, the log shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization who received the request for electronic records; the date the request for electronic records was received by the prescribed organization, the health information custodian who made the request for electronic records; the types of electronic records that were requested by the health

information custodian; the employee(s) or other person(s) acting on behalf of the prescribed organization who responded to the request; the types of electronic records that were provided to the health information custodian; the agent of the health information custodian to whom the electronic records were provided; and the form, manner and date the electronic records were provided to the health information custodian.

13. Log of Requests for Electronic Records from the IPC

The prescribed organization shall maintain a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of section 55.3 of the *Act*. At a minimum, for each request for electronic records received from the IPC, the log shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization who received the request for electronic records; the date the request was received, the employee(s) or other person(s) acting on behalf of the IPC who submitted the request; the types of electronic records that were requested by the IPC; the employee(s) or other person(s) acting on behalf of the prescribed organization who responded to the request; the types of electronic records that were provided to the IPC; the employee(s) or other person(s) acting on behalf of the IPC to whom the electronic records were provided; the form, manner and date when the electronic records were provided to the IPC.

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

The prescribed organization shall maintain a log of all audits conducted on the electronic records the prescribed organization is required to maintain of consent directives and consent overrides pursuant to paragraphs 5 and 6 of section 55.3 of the *Act*. At a minimum, for each audit conducted, the log shall set out the nature and scope of the audit; the employee(s) or other person(s) acting on behalf of the prescribed organization who conducted the audit; the date the audit was conducted; the results of the audit; any follow-up action that is required to be taken as a result of the audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for taking the follow-up action; the date the follow-up action was completed; the employee(s) or other person(s) acting on behalf of the prescribed organization or other third parties to whom the results of the audit must be communicated; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the results of the audit.

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

A policy and procedures must be developed and implemented to identify the purposes for which and the circumstances in which personal health information received for the purpose of creating or maintaining the electronic health record may be viewed, handled or otherwise dealt with by employees and other persons acting on behalf of the prescribe organization and the secure manner in which it must be viewed, handled or otherwise dealt with.

The purpose of this policy and its procedures is to ensure that employees and other persons acting on behalf of the prescribed organization view, handle or otherwise deal with the least

identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.

The policy and procedures must identify the limited and narrowly defined purposes for which and circumstances in which employees and other persons acting on behalf of the prescribed organization are permitted to view, handle or otherwise deal with personal health information and the levels of access to personal health information that may be granted.

In this regard, the policy and procedures must explicitly prohibit the viewing, handling or otherwise dealing with personal health information received for the purpose of developing or maintaining the electronic health record if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit the viewing, handling or otherwise dealing with more personal health information received for the purpose of developing or maintaining the electronic health record than is reasonably necessary to meet the identified purpose.

Levels of Access

The policy and procedures must identify the levels of use that may be granted to employees and other persons acting on behalf of the prescribed organization. The policy and procedures must further require the duties of these employees and other persons acting on behalf of the prescribed organization who are permitted to view, handle or otherwise deal with personal health information be segregated in order to avoid a concentration of privileges that would enable a single employee or other person acting on behalf of the prescribed organization to compromise the personal health information.

The policy and procedures must also prohibit employee(s) or other person(s) acting on behalf of the prescribed organization from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

Review and Approval Process

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in determining whether an employee or other person acting on behalf of the prescribed organization will be permitted to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record, along with the various level(s) of access that may be granted.

In outlining the process to be followed, the policy and procedures must set out the requirements to be satisfied; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executed and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also set out the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether an employee or other person acting on behalf of the prescribed organization will be permitted to view, handle or otherwise deal with personal health information and the criteria that must be considered in determining the appropriate level of access. At a minimum, the employee(s) or other person(s) acting on behalf of the prescribed organization must be satisfied that:

- The employee or other person acting on behalf of the prescribed organization is required to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record on an ongoing basis or for a specified period in order to perform his or her employment, contractual or other responsibilities;
- The identified purpose for the viewing, handling or otherwise dealing with personal health information is required or is permitted by the *Act* and its regulations;
- The identified purpose for the viewing, handling or otherwise dealing with personal health information cannot reasonably be accomplished without personal health information;
- De-identified and/or aggregate information will not serve the identified purpose; and
- No more personal health information will be viewed, handled or otherwise dealt with than is reasonably necessary to meet the identified purpose.

The policy and procedures should further set out any documentation that must be completed, provided and/or executed upon making the determination, if any; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation. the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; to whom the determination will be communicated; the method by which and the format in which the determination will be communicated and the required content of the documentation.

Conditions or Restrictions on Approval

The policy and procedures must identify the conditions or restrictions that will be imposed on an employee or other person acting on behalf of the prescribed organization who has been permitted to view, handle or otherwise deal personal health information received for the purpose developing or maintaining the electronic health record.

In the event that an employee or other person acting on behalf of the prescribed organizatio. is only required to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining an electronic health record for a specified period, the policy and procedures must set out the process to be followed in ensuring that the viewing, handling or otherwise dealing with the personal health information is permitted only for that specified time period.

It is recommended that all permissions granted to employees and other persons acting on behalf of the prescribed organization to view, handle or otherwise deal with personal health information

received for the purpose of developing or maintaining the electronic health record be subject to an automatic expiry. Following the automatic expiry, it is recommended that the responsible employee(s) or person(s) be required to determine whether to continue to permit the employee or other person acting on behalf of the prescribed organization to view, handle or otherwise deal with the personal health information. At a minimum, it is recommended that the expiry date be one year from the date that permission is granted.

Further, the policy and procedures must impose conditions or restrictions on the purposes for which and the circumstances in which an employee or other person acting on behalf of the prescribed organization permitted to view, handle or otherwise deal with personal health information received for the purpose of developing or maintain the electronic health record is permitted to provide or disclose the information. In particular, the policy and procedures must state that personal health information may only be provided to the Minister or disclosed to another person pursuant to a direction issued by the Minister.

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

The policy and procedures must require an employee or other person acting on behalf of the prescribed organization who has been permitted to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record, as well as his or her supervisor, to provide notification when the employee or other person acting on behalf of the prescribe. organization is no longer employed by, contracted or otherwise engaged by the prescribed organization or no longer needs to view, handle or otherwise deal with personal health information.

The procedure to be followed in providing the notification must also be identified. In particular, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this notification must be provided; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for terminating the viewing, handling or otherwise dealing with personal health information, the procedure to be followed in terminating the viewing, handling or otherwise dealing with personal health information, and the time frame within which the viewing, handling or otherwise dealing with personal health information must be terminated.

The procedures implemented in this regard must be consistent with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

Secure Retention

The policy and procedures must require an employee or other person acting on behalf of the prescribed organization who has been permitted to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record to retain the records of personal health information in a secure manner in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

Secure Disposal

The policy and procedures must require an employee or other person acting on behalf of the prescribed organization granted approval to view, handle or otherwise deal with personal health information to dispose of the records of personal health information in a secure manner in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.

Tracking Approval to View, Handle or Otherwise Deal with Personal Health Information

The policy and procedures must require that a log be maintained of employees or other persons acting on behalf of the prescribed organization who have been permitted to view, handle or otherwise deal with personal health information and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log. It is also recommended that the policy and procedures address where documentation related to the permission or termination of permission to view, handle or otherwise deal with personal health information is to be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.

In the event that there is no automatic expiry date on the permission to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record, regular audits must be conducted in accordance with the *Policy and Procedures In Respect of Privacy Audits*. The purpose of the audit is to ensure that these employees and other persons acting on behalf of the prescribed organization continue to be:

- Employed, contracted or otherwise engage to provide services in or for the prescribed organization; and
- Required to view, handle or otherwise deal with the same amount and type of personal health information.

In this regard, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, audits must be conducted on an annual basis.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

A log of employees and other persons acting on behalf of the prescribed organization permitted to view, handle or otherwise deal with personal health information must be maintained. At a minimum, the log must include the name of the employee or other person acting on behalf of the prescribed organization permitted to view, handle or otherwise deal with personal health information; the types of personal health information to which the employee or other person acting on behalf of the prescribed organization is permitted to view, handle or otherwise deal with; the level or type of viewing, handling or otherwise dealing with personal health information permitted; the date the permission was granted; and the termination date of the permission or the date of the next audit of the viewing, handling or otherwise dealing with personal health information.

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

A policy and procedures must be developed and implemented for the provision or disclosure of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization to a member of a data integration unit of the Minister or another person pursuant to a direction issued under subsections 55.9 (3) or 55.10 (1) of the *Act*.

The policy and procedures must stipulate that the Minister or a member of a data integration unit of the Minister may issue a direction requiring the prescribed organization to provide or disclose personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization to the member of a data integration unit for the purposes of subsection 55.9 (1) of the *Act* or to another person for the purposes of subsection 55.10 (1) of the *Act*.

The policy and procedures must stipulate that the direction issued by the Minister or the member of the data integration unit of the Minister under subsection 55.9 (3) or 55.10 (1) of the *Act* may specify the form, manner and time frame in which the personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization that is the subject of the direction must be provided to the member of the data integration unit or other person. The policy and procedures must also stipulate that, pursuant to subsections 55.9 (3) and 55.10 (3) of the *Act*, the prescribed organization is required to comply with a direction issued under subsection 55.9 (3) or 55.10 (1) of the *Act*.

Receiving the Direction

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving a direction issued by the member of the data integration unit of the Minister or by the Minister under subsections 55.9 (3) or 55.10 (1) of the *Act* for the provision or disclosure of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization. This shall include a discussion of the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Implementing the Direction

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing a direction issued by the member of the data integration unit of the Minister or by the Minister for the provision or disclosure of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization under subsections 55.9 (3) or 55.10 (1) of the *Act*. The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the direction to ensure that the personal health information that is accessible by means of the electronic health record that is the subject of a direction is provided in the form, manner and time frame specified in the direction. The policy and procedures shall also include a discussion of the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Secure Transfer

The policy and procedures shall require personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization that is subject to a direction by the member of the data integration unit of the Minister or by the Minister under subsections 55.9 (3) or 55.10 (1) of the *Act* to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

Logging

The policy and procedures must require that a log be maintained of all directions issued by the member of the data integration unit of the Minister or by the Minister and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log. In addition, it is recommended that the policy and procedures address where documentation related to the log of directions will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Auditing and Enforcement

The policy and procedures must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

A prescribed organization must maintain a log of directions issued by a member of the data integration unit of the Minister or by the Minister under subsections 55.9 (3) or 55.10 (1) of the *Act*. At a minimum, the log must include:

- The date the direction was issued;
- The date the direction was received;
- Whether the direction was issued under subsection 55.9(3) or 55.10(1) of the *Act*;
- For a direction issued under subsection 55.10(1) of the *Act*, whether the information that is the subject of the direction was requested in accordance with clause 39(1)(c), subsection 39(2), section 44 or 45 of the *Act*;
- A description of the personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization that is the subject of the direction;
- The form, manner and time frame in which the personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization that is the subject of the direction must be provided;
- The name of the person or organization to whom the personal health information from the electronic health record developed or maintained by the prescribed organization that is the subject of the direction must be provided;
- The name of the employee(s) or other person(s) acting on behalf of the prescribed organization who received the direction;

- The name of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing the required documentation, if any, relating to the direction;
- The name of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the direction and ensuring the personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization that is the subject of a direction is provided in the form, manner and time frame specified in the direction; and
- The date the personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization that is the subject of a direction was provided.

19. Policy and Procedures for Responding to Requests for Access and Correction of Records of Personal Health Information

Pursuant to subsection 51(5) of the *Act,* the prescribed organization must develop and implement a policy and procedures that that sets out the practices and procedures that enable the prescribed organization to respond to a request made by an individual under Part V of the *Act* to access or correct: a record of the individual's personal health information that is accessible by means of the electronic health record; or the electronic records kept by the prescribed organization under paragraphs 4, 5, and 6 of section 55.3 of the *Act*. The policies and procedures must enable the prescribed organization to respond to an individual's request in accordance with Part V of the *Act* as though the prescribed organization were a custodian and as though the prescribed organization has custody or control of the records.

NOTE: At the time of initial publication of this *Manual for the Review and Approval of Prescribed Organizations*, subsection 51(5) of the *Act* had not yet been proclaimed in force. The requirements set out below that pertain to the prescribed organization's obligations pursuant to subsection 51(5) of the *Act* shall not apply until such time as that subsection is proclaimed in force.

The prescribed organization must also develop and implement a policy and procedures that sets out the practices and procedures that have been approved by the Minister for responding to or facilitating a response to a request made by an individual to a health information custodian under Part V of the *Act* to access or correct a record of the individual's personal health information that is accessible by means of the electronic health record.

Receiving and Reviewing Requests

The policy and procedures should identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed for receiving and reviewing requests to access or correct records of personal health information that are accessible by means of the electronic health record.

In outlining the process to be followed, the policy and procedures must set out the documentation that must be completed, provided and/or executed; the employee(s) or

other person(s) acting on behalf of the prescribed organization or other person responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of this documentation.

Responding to Requests

Access Requests

The policy and procedures must set out practices and procedures that enable the prescribed organization to respond to an individual's access request in accordance with the provisions of Part V of the *Act*. In particular the policy and procedures must address the prescribed organization's obligations with respect to each of the following, as applicable:

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

- Determining whether to charge the requester a fee and the quantum of any such fee, providing an estimate of the fee to the requester, and determining whether to waive any such fee.

The policy and procedures must set out the process to be followed with respect to each of the above obligations, including, as applicable: the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making a decision or implementing an action; the process to be followed with respect to making a decision or implementing an action; the requirements that must be satisfied and the criteria that must be considered with respect to any decision or action; any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of this documentation.

Correction Requests

The policy and procedures must set out practices and procedures that enable the prescribed organization to respond to an individual's correction request in accordance with the provisions of Part V of the *Act*. In particular the policy and procedures must address the prescribed organization's obligations with respect to each of the following, as applicable:

- Making a determination as to whether the prescribed organization is required to correct the record;
- Correcting the record;
- Providing a response to the requester, including, as applicable:
    - giving written notice that the prescribed organization made the requested correction;
    - giving written notice that the prescribed organization refused to make the requested correction, and the reasons for the refusal;
    - giving written notice regarding the requester's rights with respect to a statement of disagreement; or
    - giving written notice that the requester may make a complaint to the IPC;
- Applying a statement of disagreement;
- Giving written notice to any required person regarding the correction or statement of disagreement; and
- Providing a response within the timeframe required by the *Act*, including, as applicable, making a decision to extend the time limit and providing notice of such decision to the requester.

The policy and procedures must set out the process to be followed with respect to each of the above obligations, including, as applicable: the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making a decision or implementing an action;

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

Facilitating a Response to Requests

The policy and procedures must enable the prescribed organization to comply with the practices and procedures that have been approved by the Minister for responding to or facilitating a response to a request made by an individual to a health information custodian under Part V in respect of the individual's record of personal health information that is accessible by means of the electronic health record. Where the prescribed organization must respond to or facilitate a response to such a request, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for responding to or facilitating a response; the process to be followed in responding to or facilitating a response; any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of this documentation. With regard to the process for responding to or facilitating a response, the policy and procedures should specify the format, manner and time frame with which a response must be facilitated.

Where the prescribed organization must respond to or facilitate a response to a request made by an individual to a health information custodian, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying the individual that the prescribed organization will be responding to or facilitating a response to the request; the process for notifying the individual; any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of this documentation. With regard to the process for notifying the individual that the prescribed organization will be responding to or facilitating a response to the request, the policy and procedures must specify the format, manner and time frame within which the individual must be notified.

Notice to the Public

The policy and procedures must set out the information that must be provided to the public with respect to the individual's right to access and request correction of their records of personal health information that are accessible by means of the electronic health record. The information must include the name and/or title, mailing address and contact information for the employee(s)

or other person(s) acting on behalf of the prescribed organization to whom requests for access or correction may be made and the manner and format in which these requests may be made.

Tracking Requests

The policy and procedures must require that a log be maintained of all requests to access and correct records of personal health information that are accessible by means of the electronic health record developed and maintained by the prescribed organization. The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log. In addition, it is recommended that the policy and procedures address where documentation relating to requests for access and correction will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The prescribed organization must also require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Breach Notification

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

20. Log of Access and Correction Requests

The prescribed organization must maintain a log of all requests for access and correction of records of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization. At a minimum, the log must include each of the following, as applicable.

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

- The date the request was received;
- The name and contact information for the individual to whom the information relates;
- The type of request (i.e., access or correction);

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

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

- The name and contact information for the health information custodian to whom the request was made; and
- A description of each decision that was made or action that was taken by the prescribed organization in responding to or facilitating the response.

21. Policy and Procedures for Executing Agreements with Third Party Service Providers

A policy and procedures must be developed and implemented requiring written agreements to be entered into with third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization prior to permitting third party service providers to view, handle or otherwise deal with the personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record. The policy and procedures must further require the written agreements to contain the relevant language from the *Template Agreement for All Third Party Service Providers*.

The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that an agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of such an agreement, must also be identified in the policy and procedures.

Limitations on Provision and the Viewing, Handling and Otherwise Dealing with Personal Health Information

The policy and procedures must state that only third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization may be provided and are permitted to view, handle or otherwise deal with the personal health information received for the purpose of developing or maintaining the electronic health record.

The policy and procedures must state that the prescribed organization shall not provide personal health information to a third party service provider if other information, such as de-identified and/or aggregate information, will serve the purpose and shall not provide more personal health information than is reasonably necessary to meet the purpose. The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making this determination must also be identified in the policy and procedures.

The policy and procedures must require the prescribed organization to ensure that any third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization agree to comply with the restrictions and conditions that are necessary to enable the prescribed organization to comply with all of the requirements in section 55.3 of the *Act*. This includes the requirement that the prescribed organization not permit any third party service providers to view, handle or otherwise deal with the personal health information received from health information custodians, unless the third party service provider agrees to comply with the restrictions that apply to the prescribed organization.

Where retention or disposal of records of personal health information outside the premises of the prescribed organization is the primary service provided by a third party service provider the prescribed organization must maintain a detailed inventory of the records transferred to the service provider.

Secure Transfer

The policy and procedures must also identify the purposes for which and the circumstances in which, if any, records of personal health information received by the prescribed organization

for the purpose of developing or maintaining the electronic health record may be transferred to third party service providers contracted or otherwise engaged to provide service in or for the prescribed organization. For those purposes and in those circumstances, the policy and procedures must require the records to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*. The policy and procedures must further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that, if the records are transferred, they are either securely returned or are securely disposed of, as the case may be, following the termination of the agreement. They must further address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received following the termination of the agreement, including the employee(s) or other person(s) responsible for implementing this process and the time frame following termination within which this process must be implemented.

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

The policy and procedures must require the prescribed organization to prohibit third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization from disclosing personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record. The policy and procedures must further set out the processes and safeguards that have been put in place to prevent disclosure by third party service providers contracted or otherwise engage to provide services in or for the prescribed organization and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the processes and safeguards.

Tracking Agreements

The policy and procedures shall require that a log be maintained of all agreements executed with third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization and who are permitted to view, handle or otherwise deal with personal health information. The policy and procedures must further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log and for tracking the agreements with third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization who are permitted to use personal health information.

The process to be followed in tracking all third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization who are permitted to view, handle or otherwise deal with the personal health information shall also be outlined. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed to verify that the agreements have been executed; the employee(s) or other person(s) acting on behalf of the prescribe organization responsible for completing, providing, executing and ensuring the execution of the documentation; the

employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying third party service providers contracted or otherwise engaged to provide services in or for the prescribed organization who have not executed the agreement and for ensuring that these third party service providers do so, including the timeframe within which the procedure must be implemented.

It is also recommended that the policy and procedures address where documentation related to the execution of agreements with these third party service providers will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if there has been a breach or the employee or other person believes there may have been a breach of this policy or its procedures.

22. Template Agreement for All Third Party Service Providers

A written agreement must be entered into with third party service providers contracted or otherwise engaged to provide services to the prescribed organization who will be permitted to view, handle or otherwise deal with personal health information provided to the prescribed organization for the purpose of developing or maintaining the electronic health record. This includes third party service providers contracted or otherwise engaged to retain, transfer or dispose of the records of personal health information and third party service providers contracted or otherwise engaged to provide services for the purpose of enabling the use of electronic means to collect, use, modify, disclose, retain or dispose of records of personal health information (“Electronic Service Providers”). At a minimum, the written agreement must address the matters set out below.

General Provisions

The agreement must describe the status of the prescribed organization under the *Act* and the duties and responsibilities arising from this status. The agreement must also describe the authority under the *Act* and its regulation pursuant to which the prescribed organization is permitted to view, handle or otherwise deal with personal health information for the purpose of developing or maintaining the electronic health record and the duties and responsibilities imposed on the prescribed organization in this regard.

The agreement must require the third party service provider contracted or otherwise engaged to assist in providing services in or for the prescribed organization to agree to comply with the restrictions and conditions that are necessary to enable the prescribed organization to comply with all of the requirements set out in section 55.3 of the *Act*. This includes the requirement that the third party service provider be prohibited from viewing, handling or otherwise dealing with personal health information, unless the third party service provider agrees to comply with all of the restrictions that apply to the prescribed organization, and comply with the privacy and security policies and procedures implemented by the prescribed organization.

The agreement must also provide a definition of personal health information that is consistent with the *Act* and its regulations and must describe the nature of the personal health information that the third party service provider will be permitted to view, handle or otherwise deal with in the course of providing services pursuant to the agreement.

The agreement must also require that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained employees or other persons acting on behalf of the third party service provider.

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

The agreement shall identify the purposes for which the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization is permitted to view, handle or otherwise deal with the personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record and any limitations, conditions or restrictions imposed thereon. In identifying the limited and narrowly defined purposes for which the third party service provider is permitted to view, handle or otherwise deal with personal health information, it must ensure that each instance of viewing, handling or otherwise dealing with personal health information identified in the agreement is consistent with and necessary for the purposes of the *Act* and its regulations and is not contrary to the *Act*, its regulations or another law. The agreement must also prohibit the third party service provider from viewing, handling or otherwise dealing with personal health information except as permitted in the agreement.

The agreement must further prohibit the third party service provider from viewing, handling, or otherwise dealing with personal health information if other information, such as de-identified

and/or aggregate information, will serve the purposes identified in the agreement and from using more personal health information than is reasonably necessary to meet the purposes identified.

Prohibition on Disclosure

The agreement must prohibit the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization from disclosing personal health information provided to the prescribed organization by health information custodians.

Secure Transfer

The agreement must identify the purposes for which and the circumstances in which, if any, records of personal health information received by the prescribed organization may be transferred to the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization.

For those purposes and in those circumstances, the agreement must require the records to be transferred in a secure manner. The agreement must specify the secure manner in which the records will be transferred, the conditions pursuant to which the records will be transferred, to whom the records will be transferred and the procedure that must be followed in ensuring that the records are transferred in a secure manner. In identifying the secure manner in which records of personal health information must be transferred, the agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

In addition, where retention or disposal of records of personal health information outside the premises of the prescribed organization is the primary service provided by the third party service provider, the agreement shall require the third party service provider to provide to the prescribed organization documentation setting out the date, time and mode of transfer of the records and with written confirmation evidencing receipt of the records by the third party service provider. In these circumstances, the agreement must also obligate the third party service provider to maintain a general description of the records transferred.

Secure Retention

For those purposes and in those circumstances where records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record may be transferred to a third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization, the agreement shall require the third party service provider to retain the records in a secure manner. The agreement must identify the precise methods by which records of personal health information, in both paper and electronic format, will be securely retained by the third party service provider, including records of personal health information retained on various media.

The agreement must further outline the responsibilities of the third party service provider in securely retaining the records of personal health information provided to the prescribed organization for the purpose of developing or maintaining the electronic health record. In identifying the secure manner in which records of personal health information must be retained,

the agreement shall have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

Where the retention of records of personal health information is the primary service provided to the prescribed organization by the third party service provider, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records being retained, as well as a method to track the records being retained.

Secure Return or Disposal Following Termination of the Agreement

For those purposes and in those circumstances where records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record may be transferred to the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization, the agreement must address whether records will be securely returned or securely disposed of following the termination of the agreement.

If the records are required to be returned in a secure manner, the agreement must stipulate the time frame following the date of termination of the agreement within which the third party service provider must securely return the records, the secure manner in which the records must be returned and the employee or other person acting on behalf of the prescribed organization to whom the records must be securely returned. In identifying the secure manner in which records of personal health information will be returned, the agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

If the records of personal health information are required to be securely disposed of, the agreement must provide a definition of secure disposal that is consistent with the Act and its regulations and must identify the precise manner in which the records are to be securely disposed of by the third party service provider. In identifying the secure manner in which the records of personal health information will be disposed of, it must ensure that the method of secure disposal identified is consistent with:

- The *Act* and its regulations;
- Orders and decisions issued by the IPC under the *Act* and its regulation, including Order HO-001 and Order HO-006;
- Guidelines, fact sheets and best practices issued by the IPC, including *Fact Sheet 10: Secure Destruction of Personal Information;* and
- The *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.

The agreement must also stipulate the time frame following termination of the agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided by the third party service provider. The agreement must further identify the employee or other person acting on behalf of the prescribed organization to whom the certificate of destruction must be provided and must identify the required content of the certificate of destruction. At a minimum, the certificate of destruction must be required to identify the records of personal health information securely disposed of; to

stipulate the date, time and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

Secure Disposal as a Contracted Service

Where the disposal of records of personal health information received for the purpose of developing or maintaining the electronic health record is the primary service provided to the prescribed organization by the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization, in addition to the requirements set out above in relation to secure disposal, the agreement must further set out the responsibilities of the third party service provider in securely disposing of the records, including:

- The time frame within which the records are required to be securely disposed of;
- The precise method by which records, in both paper and electronic format, must be securely disposed of, including records retained on various media;
- The conditions pursuant to which the records will be securely disposed of; and
- The person(s) responsible for ensuring the secure disposal of the records.

The agreement should also enable the prescribed organization, at its discretion, to witness the secure disposal of the records by the third party service provider, subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

The agreement shall require the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization to take steps that are reasonable in the circumstances to ensure that the personal health information viewed, handled or otherwise dealt with in the course of providing services pursuant to the agreement is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be implemented by the third party service provider must be detailed in the agreement.

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

The agreement shall require the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization to provide training to its employees and other persons acting on behalf of the third party service provider on the importance of protecting the privacy of individuals whose personal health information is viewed, handled or otherwise dealt with in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

The agreement must also require the third party service provider to ensure that its employees and any person acting on behalf of the third party service provider who will view, handle or otherwise deal with records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to viewing, handling or otherwise dealing with

personal health information. The agreement must also set out the method by which this will be ensured. This may include requiring employees and other persons acting on behalf of the third party service provider to sign an acknowledgement, prior to being permitted to view, handle or otherwise deal with the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.

Subcontracting of the Services

In the event that the agreement permits the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization to subcontract the services provided under the agreement, the third party service provider must be required to acknowledge and agree that it will provide the prescribed organization with advance notice of its intention to do so, will enter into a written agreement with the subcontractor on terms consistent with its obligations to the prescribed organization, and will provide a copy of the written agreement to the prescribed organization.

Notification

At a minimum, the agreement must require the third party service provider contracted or otherwise engaged to provide services in or for the prescribed organization to notify the prescribed organization at the first reasonable opportunity if:

- There has been a breach or suspected breach of the agreement;
- Personal health information viewed, handled or otherwise dealt with by the third party service provider on behalf of the prescribed organization is collected without authority or is stolen, lost or subject to unauthorized use or disclosure; or
- Personal health information viewed, handled or otherwise dealt with by the third party service provider on behalf of the prescribed organization is believed to have been collected without authority or is believed to have been stolen, lost or subject to unauthorized use or disclosure.

The agreement should also identify whether the notification must be verbal, written or both and to whom the notification must be provided. The third party service provider must also be required to take steps that are reasonable in the circumstances to contain the breach and to contain the unauthorized collection or theft, loss or any unauthorized use or disclosure.

Consequences of Breach and Monitoring Compliance

The agreement must outline the consequences of breach of the agreement. The agreement must require that the third party service provider's compliance with the agreement will be audited and the manner in which compliance will be audited and the notice, if any, that will be provided to the third party service provider of the audit.

23. Log of Agreements with Third Party Service Providers

A log of executed agreements with third party service providers that are permitted to view, handle or otherwise deal with personal health information must be maintained. At a minimum, the log must include:

- The name of the third party service provider;
- The date that the agreement with the third party service provider was executed;
- The date of termination of the agreement with the third party service provider;
- The nature of the services provided by the third party service provider;
- The nature of the personal health information that the third party service provider is permitted to view, handle or otherwise deal with in the course of providing the services;
- The date the third party service provider began to view, handle or otherwise deal with the personal health information;
- The date the third party service provider's viewing, handling or otherwise dealing with records of personal health information was terminated;
- Whether the records of personal health information were transferred to the third party service provider, and if so the nature of the records transferred and the dates(s) of transfer;
- Whether the records of personal health information, if any, will be securely returned or securely disposed of following the date of termination of the agreement; and
- The date the records of personal health information were returned or a certificate of destruction was provided or the date by which the records must be returned or disposed of.

24. Privacy Impact Assessment Policy and Procedures

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

In identifying the circumstances in which privacy impact assessments are required to be conducted, the policy and procedures must, at a minimum, require a privacy impact assessment be conducted for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization. Further, the policy and procedures must require the prescribed organization to conduct privacy impact assessments on existing and proposed systems that retrieve, process or integrate personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization and on changes or proposed changes to existing information systems that retrieve, process or integrate personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization.

The policy and procedures must also specify that a privacy impact assessment must be conducted for each type of personal health information that is currently being provided and for each type of personal health information that is proposed to be requested or required

by regulation to be provided to the prescribed organization for the purpose of developing or maintaining the electronic health record.

If there are limited and specific circumstances in which privacy impact assessments are not required to be conducted on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated, these shall be outlined in the policy and procedures along with a rationale for why privacy impact assessments are not required. The policy and procedures must further identify the employee(s) responsible for making this determination and must require the determination and the reasons for the determination to be documented.

The policy and procedures must also address the timing of privacy impact assessments. With respect to proposed systems that retrieve, process or integrate personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization and proposed changes to existing systems that retrieve, process or integrate personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization, the policy and procedures must require that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to any new types of personal health information that is proposed to be requested or required to be provided to the prescribed organization for the purpose of developing or maintaining the electronic health record, the policy and procedures must require that the privacy impact assessment be conducted before the personal health information is requested or required to be provided to the prescribed organization.

With respect to existing systems that retrieve, process or integrate personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization and the types of personal health information that are currently being provided to the prescribed organization, the policy and procedures must require that a timetable be developed to ensure privacy impact assessments are conducted and the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for developing the timetable.

Once privacy impact assessments have been completed, the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the privacy and security policies, procedures and practices put in place by the prescribed organization. The policy and procedures must also identify the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact

assessments are reviewed and amended, if necessary. The role of employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified in respect of privacy impact assessments.

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

For existing or proposed systems that retrieve, process or integrate personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization, the privacy impact assessment must describe:

- The system that is currently or will be retrieving, processing or integrating personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization;
- The types of the personal health information that are or will be retrieved, processed or integrated by the existing or proposed system;
- The sources of the personal health information that is or will be retrieved, processed or integrated by the existing or proposed system;
- The reason why the system is necessary for developing or maintaining the electronic health record;
- The flows of the personal health information that currently is or will be retrieved, processed or integrated by the existing or proposed system;
- The statutory authority relating to the system that is or will be retrieving, processing or integrating personal health information accessible by means of the electronic health record, if any;
- The limitations imposed on the collection, use and disclosure of and/or the viewing, handling or otherwise dealing with the personal health information in the system that is or will be retrieving, processing or integrating personal health information accessible by means of the electronic health record, if any;
- The secure manner in which the personal health information that is or will be retrieved, processed or integrated by the existing or proposed system is or will be retained, transferred and disposed of;
- The functionality for logging access, collection, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized collection, use or disclosure;
- The risks to the privacy of individuals whose personal health information will be retrieved, processed or integrated by the existing or proposed system and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and

- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.

For types of personal health information that are or will be provided to the prescribed organization, the privacy impact assessment must describe:

- The types of personal health information that are or will be provided to the prescribed organization for the purpose of developing or maintaining the electronic health record;
- The sources of the personal health information that are or will be provided to the prescribed organization for the purpose of developing or maintaining the electronic health record;
- The statutory authority for the provision of the personal health information to the prescribed organization, if any;
- The retention period for the types of personal health information provided to the prescribed organization;
- The secure manner in which the records of personal health information that are being provided to the prescribed organization are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized collection, use or disclosure;
- The risks to the privacy of individuals whose personal health information is or will be accessible by means of the electronic health record developed or maintained by the prescribed organization and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the personal health information.

The process for addressing the recommendations arising from privacy impact assessments, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning another employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations, is also required to be outlined.

The policy and procedures must require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log.

The policy and procedures must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and

procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

In developing the policy and procedures, it is recommended that regard be had to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, issued by the IPC.

25. Log of Privacy Impact Assessments

A log shall be maintained of privacy impact assessments that have been completed and that have been undertaken but not completed in respect of all systems that retrieve, process or integrate personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization and for each type of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record. The log shall describe the systems that retrieve, process or integrate personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization or the type(s) of personal health information at issue; the date that the privacy impact assessment was completed or is expected to be completed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

The prescribed organization shall also maintain a log of systems that retrieve, process or integrate personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization or for types of personal health information received by the prescribed organization for which privacy impact assessments have not been undertaken. The log shall describe the systems that retrieve, process or integrate personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization or the types of personal health information received by the prescribed organization at issue. For each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization and each type of personal health information received by the prescribed organization, the log shall either set out the reason that a privacy impact assessment will not be undertaken and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making this determination or set out the date that the privacy impact assessment is expected to be completed and the employee(s) or

other person(s) acting on behalf of the prescribed organization responsible for completing or ensuring the completion of the privacy impact assessment.

26. Policy and Procedures in Respect of Privacy Audits

A policy and procedures must be developed and implemented that sets out the types of privacy audits that are required to be conducted in respect of personal health information received by the prescribed organization for the purpose of developing and maintaining the electronic health record. At a minimum, the audits required to be conducted shall include audits:

- To assess compliance with the privacy policies, procedures and practices put in place by the prescribed organization;
- Of the employee(s) and other person(s) acting on behalf of the prescribed organization permitted to view, handle or otherwise deal with personal health information; and
- Of the employee(s) and other person(s) acting on behalf of the prescribed organization permitted to view, handle or otherwise deal with personal health information that has been de-identified or aggregated.

With respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures shall require a privacy audit schedule to be developed and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for developing the privacy audit schedule. Where there is no automatic expiry on the permission granted to an employee or other person acting on behalf of the prescribed organization to view, handle or otherwise deal with personal health information, at a minimum, audits of these employees and other persons must be conducted on an annual basis in accordance with the *Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization*.

For each type of privacy audit that is required to be conducted, the policy and procedures shall also set out the process to be followed in conducting the audit. In outlining the process to be followed, the policy and procedures shall set out the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures must further set out the documentation that must be completed, provided and/or executed in undertaking each privacy audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. The role of the employee(s) or other person(s) acting on

behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from privacy audits, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations within the identified timelines.

The policy and procedures must also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the privacy audit, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation, the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided and the required content of the documentation.

The policy and procedures must also address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit must be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures must further require that a log be maintained of privacy audits and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log. They should further address where documentation related to privacy audits will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the privacy audit to notify the prescribed organization, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Management* and of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management*.

27. Log of Privacy Audits

A log of all privacy audits that have been completed must be maintained. The log shall set out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing the privacy audit; the recommendations arising from the privacy audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for

addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

28. Policy and Procedures for Privacy Breach Management

A policy and procedures must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches in respect of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record. In developing the policy and procedures, it is recommended that regard be had to guidelines issued by the IPC entitled *Responding to a Health Privacy Breach: Guidelines for the Health Sector* and any directions issued by the Minister.

The policy and procedures must provide a definition of the term "privacy breach." At a minimum, a privacy breach shall be defined to include:

- The collection, use and disclosure of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization that is not in compliance with the *Act* and its regulations;
- The viewing, handling or otherwise dealing with personal health information provided to the prescribed organization for the purpose of developing or maintaining the electronic health record that is not in compliance with the *Act* or its regulations;
- A contravention of the privacy policies, procedures or practices put in place by the prescribed organization pursuant to the *Act* and its regulations;
- A contravention of Confidentiality Agreements and Agreements with Third Party Service Providers including written acknowledgements acknowledging and agreeing not to use personal health information which has been de-identified and/or aggregated, to identify an individual;
- Circumstances where personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization is collected without authority or is stolen, lost or subject to unauthorized use or disclosure; and
- Circumstances where records of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization are subject to unauthorized copying, modification or disposal.

Identification of Privacy Breaches

The policy and procedures must set out the manner in which privacy breaches or suspected privacy breaches will be identified by the prescribed organization. At a minimum, the policy and procedures must indicate that privacy breaches or suspected privacy breaches will be identified through reports by employees or other persons acting on behalf of the prescribed organization; reports by health information custodians that collect, use and disclose the personal health information that is accessible by means of the electronic health record; privacy audits, privacy complaints and inquiries; and the auditing and monitoring of the electronic records the prescribed organization is required to maintain.

The policy and procedures shall impose a mandatory requirement on employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity after they become aware of a privacy breach or suspected privacy breach through any manner including those noted above. In this regard, the policy and procedures shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization who must be notified of the privacy breach or suspected privacy breach and shall provide contact information for the employee(s) or other person(s) acting on behalf of the prescribed organization who must be notified. The policy and procedures shall further stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification.

The policy and procedures shall also address the documentation that must be completed, provided and/or executed with respect to notification; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Privacy Breaches Caused by One or More Health Information Custodians

The policy and procedures must specify that where the prescribed organization identifies a privacy breach or suspected privacy breach that was caused by one or more health information custodians, the prescribed organization must report the privacy breach or suspected privacy breach to the health information custodians.

The policy and procedures must specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall cooperate with health information custodians in developing a policy and procedures to make a determination of whether a privacy breach has in fact occurred and if so, to contain, investigate and remediate the privacy breach and to notify individuals in circumstances where the privacy breach or suspected privacy breach was caused by one or more health information custodians.

The policy and procedures must also specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in making a determination of whether a privacy breach has in fact occurred and if so, assist in containing, investigating and remediating the privacy breach and notifying individuals in circumstances where the privacy breach or suspected privacy breach was caused by one or more health information custodians.

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

Privacy Breaches Caused by the Prescribed Organization or an Unauthorized Person

The policy and procedures shall require the prescribed organization to take the following steps in any instance in which a privacy breach or suspected privacy breach is caused by: an employee(s) or other person(s) acting on behalf of the prescribed organization; a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; or an unauthorized person who is not an employee or other person acting on behalf of the prescribed organization or an agent of a health information custodian.

Determination of Whether a Privacy Breach Occurred

The policy and procedures shall require the prescribed organization to make a determination of whether a privacy breach has in fact occurred and if so what, if any, personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization has been breached. The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making this determination must also be identified.

The policy and procedures must further address when senior management, including the Chief Executive Officer or Executive Director, will be notified of a privacy breach. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

Containment

The policy and procedures shall require the prescribed organization to immediately initiate containment and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for containment and the procedure that must be followed in this regard. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for containing the breach; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

In undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to protect personal health information accessible by means of the electronic health record from further unauthorized collection, from further theft, loss or unauthorized use, or disclosure, and from being further viewed, handled or otherwise dealt with without authority, and to protect records of personal health information accessible by means of the electronic health record from further unauthorized copying, modification or disposal. At a minimum, these steps shall include ensuring that no copies of the records of personal health information have been made and ensuring that the records are either retrieved or disposed of in a secure manner. Where the records of personal health information are securely disposed of, written confirmation should be obtained in respect of the date, time and method of secure

disposal. These steps shall also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to other personal health information and, if necessary, taking further action to prevent additional privacy breaches.

The employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether further containment measures are necessary, must be identified in the policy and procedures. The policy and procedures shall also address the documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for reviewing the containment measures; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Notification

The policy and procedures must require the health information custodian(s) that provided the personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record to be notified at the first reasonable opportunity.

In particular, the policy and procedures shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying the health information custodians, the format of the notification and the nature of the information that must be provided upon notification. At a minimum, the policy and procedures must require the health information custodian to be advised of the extent of the privacy breach, the nature of the personal health information at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation.

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

The policy and procedures shall also set out whether any other persons or organizations must be notified of the privacy breach and shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification. At a minimum, the policy and procedures must require the prescribed organization to notify the IPC, in writing, immediately after becoming aware that personal health information that is accessible by means of the electronic health record:

- Has been viewed, handled or otherwise dealt with by the prescribed organization or a third party contracted or otherwise engaged by the prescribed organization other than in accordance with the *Act* or its regulations; or
- Has been made available or released by the prescribed organization or a third party contracted or otherwise engaged by the prescribed organization, other than in accordance with the *Act* and its regulations.

Investigation and Recommendations

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in this regard. In outlining the process to followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed in undertaking the investigation; the employee(s) responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. The role of employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from the investigation of the privacy breach including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations; for establishing timelines to address the recommendations; and for monitoring and ensuring the implementation of the recommendations within the stated timelines.

The policy and procedures shall also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the privacy breach, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

Communication of Findings of Investigation and Recommendations

The policy and procedures must also address the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or Executive Director.

Tracking Privacy Breaches

The policy and procedures shall require that a log be maintained of all privacy breaches and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log. The policy and procedures should further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Relationship to Policy and Procedures for Information Security Breach Management

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

Compliance, Audit and Enforcement

The policy and procedures must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

29. Log of Privacy Breaches

A log of all privacy breaches in respect of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization shall be maintained. At a minimum, the log shall set out each of the following, to the extent that they are known to the prescribed organization:

- The date notification of the privacy breach was received;
- The date of the privacy breach;
- The date the privacy breach was identified or suspected;
- A description of the manner in which the privacy breach was identified and by whom;
- The date that the Chief Executive Officer or Executive Director, and senior management were notified of the privacy breach;
- The cause of the privacy breach;
- That the privacy breach was caused by one or more health information custodians and the name of each health information custodian or each health information custodian whose agents or Electronic Service Providers caused the privacy breach and the name of each agent and electronic service provider of the health information custodian that caused the privacy breach, if applicable;

- That the breach was caused by the prescribed organization and the system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization or the name of each employee and other person acting on behalf of the prescribed organization that caused the privacy breach, if applicable;
- That an unauthorized person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian caused the breach and the name or a description of the unauthorized person, if applicable;
- The name of each health information custodian that provided the personal health information to the prescribed organization;
- The date(s) notification was provided to the affected custodian(s), where applicable;
- The date(s) notification was provided to the individual(s) to whom the personal health information relates, where applicable;
- The nature and extent of the privacy breach;
- The nature of the information that is accessible by means of the electronic health record that was subject to the privacy breach, without disclosing any personal health information;
- The date the privacy breach was contained, the name of the employee(s) or other person(s) acting on behalf of he prescribed organization or the name of the agent(s) of a health information custodian(s) responsible for containing the privacy breach; and the nature of the containment measures;
- The employee(s) or other person(s) acting on behalf of the prescribed organization or the agent(s) of a health information custodian(s) responsible for conducting the investigation;
- The date the investigation of the privacy breach was commenced;
- The date the investigation of the privacy breach was completed;
- The findings and recommendations arising from the investigation;
- The employee(s) or other person(s) acting on behalf of the prescribed organization or the agent(s) of a health information custodian(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed;
- The date notification was provided to the IPC, if applicable; and
- The date(s) that the findings of the investigation and the measures taken, if any, in response to the privacy breach were provided to the individual(s) to whom the information relates.

30. Policy and Procedures for Privacy Complaints

A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints in respect of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization. This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Privacy Inquiries*.

The policy and procedure must provide a definition of the term "privacy complaint" that includes concerns or complaints related to compliance of a health information custodian or the prescribed organization with the *Act* and its regulations in respect of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization.

The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy complaints shall also be identified. At a minimum, the information communicated to the public shall include the name and/or title, mailing address and contact information of the employee(s) or other person(s) acting on behalf of the prescribed organization to whom individuals may direct privacy complaints and the manner in which privacy complaints may be made. It must also state that individuals may direct a privacy complaint related to compliance with the *Act* and its regulations to the IPC and must provide the mailing address and contact information for the IPC.

Process for Receiving Complaints

The policy and procedures must establish the process to be followed in receiving privacy complaints. This shall include the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for receiving the privacy complaint and the nature of the information to be requested from the individual making the privacy complaint.

Complaint Relates to One or More Health Information Custodians

The policy and procedures must specify that where the prescribed organization receives a privacy complaint related to one or more health information custodians or to an agent(s) or electronic service provider(s) of one or more health information custodians, the prescribed organization must forward the privacy complaint to the health information custodian(s).

Where the prescribed organization forwards the privacy complaint to one or more health information custodians, the policy and procedures must require the prescribed organization to respond in writing to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that the privacy complaint has been forwarded to one or more health information custodians; and providing contact information for the health information custodian(s) to whom the complaint was forwarded.

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for sending the above noted written communication to the individuals making privacy complaints and the time frame within which the communication will be sent to the individuals.

The policy and procedures must specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in developing a policy and procedures to make a determination of whether to investigate a privacy complaint and if so, to investigate and remediate the privacy complaint in circumstances where the privacy complaint relates to more than one health information custodian or to an agent(s) or electronic service provider(s) of more than one health information custodian.

The policy and procedures must also specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in making a determination of whether to investigate a privacy complaint and if so, to assist in investigating and remediating the privacy complaint in circumstances where the privacy complaint relates to one or more health information custodians or to an agent(s) or electronic service provider(s) of one or more health information custodians.

Complaint Relates to the Prescribed Organization or an Unauthorized Person

The policy and procedures shall require the prescribed organization to take the following steps in any instance in which a privacy complaint is received relating to: an employee(s) or other person(s) acting on behalf of the prescribed organization; a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; or an unauthorized third party who is not an employee or other person acting on behalf of the prescribed organization or an agent of a health information custodian.

Determination of Whether to Investigate a Complaint

The policy and procedures shall require the prescribed organization to make a determination of whether the privacy complaint will be investigated. In this regard, the policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation.

Where Complaint Will Not be Investigated

In the event that it is determined that an investigation will not be undertaken, the policy and procedures must require the prescribed organization to respond in writing to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken and the reason an investigation will not be undertaken; advising the individual that he or she may make a complaint to the IPC if there are reasonable grounds to believe that the prescribed organization has contravened or is about to contravene the *Act* or its regulations; and providing contact information for the IPC.

Where Complaint Will be Investigated

In the event that it is determined that an investigation will be undertaken, the policy and procedures must require the prescribed organization to respond in writing to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation process; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation. The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for sending the written communication and the time frame within which the communication will be sent.

Where an investigation of a privacy complaint will be undertaken, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed in undertaking the investigation; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. The role of the employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed for addressing the recommendations arising from the investigation of privacy complaints, including the employee(s) responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations within the stated timelines shall also be addressed in the policy and procedures.

The policy and procedures must also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuing the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

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

a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures shall further require the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. The individual making the privacy complaint shall also be advised that he or she may make a complaint to the IPC if there are reasonable grounds to believe that the *Act* or its regulations has been or is about to be contravened. The contact information for the IPC shall also be provided. The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, shall also be addressed.

The policy and procedures should also identify whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying these other persons or organizations; the form and the manner of the notification; the nature of the information that must be provided upon notification and the time frame within which the notification must be provided.

Tracking Privacy Complaints

The policy and procedures must require that a log be maintained of all privacy complaints and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log. The policy and procedures should further address where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Relationship to Policy and Procedures for Privacy Breach Management

The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Breach Management* shall also be addressed.

Compliance, Audit and Enforcement

The policy and procedures must require employees or other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

31. Log of Privacy Complaints

A log of privacy complaints in respect of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization must be maintained. At a minimum, the log shall set out each of the following, to the extent that they are known to the prescribed organization:

- The date that the privacy complaint was received;
- The nature of the privacy complaint;
- The health information custodian(s) to whom the privacy complaint was forwarded and the date the privacy complaint was forwarded, if applicable;
- The date the individual was advised that the privacy complaint was forwarded to one or more health information custodians, if applicable;
- The determination as to whether or not the privacy complaint will be investigated by the prescribed organization;
- The employee(s) or other person(s) acting on behalf of the prescribed organization and/or the agent(s) of a health information custodian who made the determination as to whether the privacy complaint would be investigated;
- Where the determination was made that the privacy complaint will not be investigated, the date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint; and
- Where the determination is made that the privacy complaint will be investigated:
    - the date that the individual making the complaint was advised that the complaint will be investigated;
    - the date that the investigation was commenced;
    - the date that the investigation was completed;
    - the employee(s) or other person(s) acting on behalf of the prescribed organization and/or the agent(s) of a health information custodian responsible for conducting the investigation;
    - the findings and recommendations arising from the investigation;
    - the employee(s) or other person(s) acting on behalf of the prescribed organization and/or agent(s) of a health information custodian responsible for addressing each recommendation;

- the date each recommendation was or is expected to be addressed;
- the manner in which each recommendation was or is expected to be addressed; and
- the date that the individual making the privacy complaint was advised of the findings of the investigation.

32. Policy and Procedures for Privacy Inquiries

A policy and procedures must be developed and implemented to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries in respect of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization. This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Privacy Complaints*.

The policy and procedures must provide a definition of the term "privacy inquiry" that includes inquiries related to compliance of a health information custodian or the prescribed organization with the *Act* and its regulations in respect of personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization and the privacy policies, procedures and practices put in place by health information custodians or the prescribed organization in relation to personal health information that is accessible by means of the electronic health record developed or maintained by the prescribed organization.

The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries shall also be identified. At a minimum, the information communicated to the public shall include the name and/or title, mailing address and contact information of the employee(s) or other person(s) acting on behalf of the prescribed organization to whom privacy inquiries may be directed; the manner in which privacy inquiries may be made; and information as to where individuals may obtain further information about the privacy policies, procedures and practices put in place by health information custodians or the prescribed organization.

Inquiry Relates to One or More Health Information Custodians

The policy and procedures must specify that where the prescribed organization receives a privacy inquiry related to one or more health information custodians, the prescribed organization must forward the privacy inquiry to the health information custodian(s) to whom the inquiry relates.

Where the prescribed organization forwards the privacy inquiry to one or more health information custodians, the policy and procedures must require the prescribed organization to respond in writing to the individual making the privacy inquiry acknowledging receipt of the privacy inquiry; advising that the privacy inquiry has been forwarded to one or more health information custodians; and providing contact information for the health information custodian(s) to whom the inquiry was forwarded.

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for sending written communication to individuals making privacy inquiries and the time frame within which the communication will be sent to the individuals.

The policy and procedures must specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in developing a policy and procedures to respond to inquiries in circumstances where the privacy inquiries relate to one or more health information custodians.

The policy and procedures must also specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in responding to privacy inquiries related to personal health information that is accessible by means of the electronic health record.

Inquiry Relates to the Prescribed Organization or an Unauthorized Person

The policy and procedures must further establish the process to be followed in receiving and responding to privacy inquiries that relate to an employee(s) or other person(s) acting on behalf of the prescribed organization; a system that retrieves, processes or integrates personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization; or an unauthorized third party who is not an employee or other person acting on behalf of the prescribed organization or an agent of a health information custodian.

In outlining the process to be followed, the policy and procedures shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving and responding to privacy inquiries; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing executing and ensuring the execution of documentation; the required content of the documentation; and the format and content of the response to the individual making the privacy inquiry. The role of the employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

Compliance, Audit and Enforcement

The policy and procedures must require employees or other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

Part 2 - Security Documentation

1. Information Security Policy

An overarching information security policy must be developed and implemented in relation to personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record under the *Act* and its regulation.

The information security policy must require steps to be taken that are reasonable in the circumstances to ensure that personal health information accessible by means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of the personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal.

Threat and Risk Assessment

The information security policy must require the prescribed organization to undertake comprehensive and organization-wide threat and risk assessments for all information systems, technologies, equipment, resources, applications and programs used for the purpose of developing or maintaining the electronic health record, including for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record, as well as appropriate project specific threat and risk assessments involving such personal health information. It must also establish and document a methodology for identifying, assessing and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

Information Security Program

The information security policy must further require a comprehensive information security program to be developed and implemented consisting of administrative, technical and physical safeguards that are consistent with established industry standards and practices. The information security program must be required to effectively address the threats and risks identified, must be amenable to independent verification, and must be consistent with established security frameworks and control objectives. The duties and responsibilities of employees and other persons acting on behalf of the prescribed organization in respect of the information security program and in respect of implementation of the administrative, technical and physical safeguards shall also be addressed.

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

- A security governance framework for the implementation of the information security program, including security training and awareness;
- Policies and procedures for the ongoing review of the security policies, procedures and practices implemented;

- Policies and procedures for ensuring the physical security of the premises and the locations within the premises where records of personal health information received for the purpose of developing or maintaining the electronic health record are retained, viewed, handled or otherwise dealt with by the prescribed organization;
- Policies and procedures for the secure retention, transfer and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of data at rest;
- Policies and procedures to establish access control and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control;
- Policies and procedures for information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Policies and procedures for logging, auditing and monitoring, including policies and procedures for maintaining and reviewing system control and audit logs;
- Policies and procedures for security audits;
- Policies and procedures for network security management, including patch management and change management;
- Policies and procedures related to the acceptable use of information technology;
- Policies and procedures for back-up and recovery;
- Policies and procedures for information security breach management; and
- Policies and procedures to establish protection against malicious and mobile code.

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

Information Security Infrastructure

The information security policy shall also outline the information security infrastructure implemented by the prescribed organization including the transmission of personal health information over authenticated, encrypted and secure connections; the establishment of hardened servers, firewalls, demilitarized zones and other perimeter defences; anti-virus, anti-spam and anti-spyware measures; intrusion detection and prevention systems; privacy and security enhancing technologies; and mandatory system-wide password-protected screen savers after a defined period of inactivity.

Continuous Assessment and Verification of the Security Program

The information security policy must require a credible program to be implemented for continuous assessment and verification of the effectiveness of the security program in order to deal with threats and risks to the personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with this policy and with all other security policies, procedures and practices implemented by the prescribed organization and must address how and by whom compliance will be enforced and the consequences of breach. The information security policy 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 will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy.

Notification of Breach

The information security policy must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or any of the security policies, procedures and practices implemented.

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

A policy and associated procedures must be developed and implemented for the ongoing review of the security policies, procedures and practices put in place by the prescribed organization pursuant to the *Act* and its regulation. The purpose of the review is to determine whether amendments are needed and/or whether new security policies, procedures and practices are required.

The policy and procedures must identify the frequency of the review, the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for undertaking the review, the procedure to be followed in undertaking the review and the time frame in which the review will be undertaken. At a minimum, the security policies, procedures and practices implemented by the prescribed organization must be reviewed at least once prior to each scheduled review of these policies, procedures and practices by the IPC pursuant to section 55.12 of the *Act* and whenever the Minister issues a directive to the prescribed organization with respect to the carrying out of its responsibilities and functions. The policy and procedures must also identify the employee(s) and other persons acting on behalf of the prescribed organization responsible and the procedure to be followed in amending and/or drafting new security policies, procedures and practices if deemed necessary as a result of the review, and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the procedure that must be

followed in obtaining approval of any amended and/or newly developed security policies, procedures and practices.

In undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, regard must be had to:

- Any directives issued by the Minister with respect to the carrying out of its responsibilities and functions;
- Any orders, decisions, guidelines, fact sheets and best practices issued by the IPC under the *Act* and its regulation;
- Evolving industry security standards and best practices;
- Technological advancements;
- Amendments to the *Act* and its regulation relevant to the prescribed organization; and
- Recommendations arising from privacy and security audits, privacy impact assessments, and investigations into privacy complaints, privacy breaches and information security breaches.

It must also take into account whether the security policies, procedures and practices of the prescribed organization continue to be consistent with its actual practices and whether there is consistency between and among the security and privacy policies, procedures and practices implemented.

The policy and associated procedures must also identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible and the procedure to be followed in communicating the amended and/or newly developed security policies, procedures and practices, including the method and nature of the communication. It shall also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for and the procedure to be followed in reviewing and amending the communication materials available to the public, each health information custodian that provided personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record, and other stakeholders as a result of the amended or newly developed security policies, procedures and practices.

This policy and its associated procedures may either be a stand-alone document or may be combined with the *Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices.*

The policy and procedures must require employees or other persons acting on its behalf to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes that there may have been a breach of this policy or its associated procedures.

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

A policy and associated procedures must be developed and implemented to address the physical safeguards put in place by the prescribed organization to ensure personal health information accessible my means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of the personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal.

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

The policies and procedures must also require that the premises of the prescribed organization be divided into varying levels of security with each successive level being more secure and restricted to fewer individuals and that in order to access locations within the premises where records of personal health information are retained, individuals be required to pass through multiple levels of security.

Policy, Procedures and Practices with Respect to Access by Employees and Other Persons Acting on Behalf of Prescribed Organization

The various levels of access that may be granted to the premises and to locations within the premises where records of personal health information are retained shall be set out in the policy and procedures.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in approving and terminating access by employees or other persons acting on behalf of the prescribed organization to the premises and to locations within the premises where records of personal health information are retained, including the levels of access that may be granted. In outlining the process to be followed, the policy and procedures shall set out the requirements that must be satisfied; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must further set out the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for approving and determining the appropriate level of access. The criteria must be based on the

"need to know" principle and must ensure that access is only provided to employees or other persons acting on behalf of the prescribed organization who routinely require such access for their employment, contractual or other responsibilities. At a minimum, the criteria considered by the employees(s) or other person(s) acting on behalf of the prescribed organization must ensure that access is only provided to employee(s) or other person(s) acting on behalf of the prescribed organization:

- Employed, contracted or otherwise engaged to provide services in or for the prescribed organization;
- Who are routinely required to use personal health information received by the prescribed organization for the purpose of developing and maintaining the electronic health record; and
- Whose use of the personal health information is permitted by the *Act* and by the *Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization*.

In the event that an employee or other person acting on behalf of the prescribed organization only requires such access for a specified period, the policy and procedures must set out the process to be followed for ensuring that access is permitted only for that specified period.

The policy and procedures should also set out the manner in which the determination relating to access and the level of access is documented; to whom this determination will be communicated; any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

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

The policy and procedures shall require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys and shall set out the process that must be followed in this regard. In outlining the process to be followed, the policy and procedures shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the notification must be provided; the nature and format

of the notification; the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee or other person acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures shall also outline the safeguards that are required to be implemented as a result of the theft, loss or misplacement of identification cards, access cards and/or keys and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing these safeguards.

The policy and procedures must also address the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for their issuance. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing executing and ensuring the execution of the documentation; the employee or other person acting on behalf of the prescribed organization to whom the documentation must be provided; the required content of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom temporary identification cards, access cards and/or keys shall be returned; and the time frame for return.

The process to be followed in the event that temporary identification cards, access cards and/or keys are not returned, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the process and the time frame within which the process must be implemented, shall also be addressed.

Termination or Cessation of the Employment, Contractual or Other Relationship

The policy and procedures shall require employees and other persons acting on behalf of the prescribed organization, as well as their supervisors, to notify the prescribed organization of the termination or cessation of their employment, contractual or other relationship with the prescribed organization and to return their identification cards, access cards and/or keys to the prescribed organization on or before the date of termination or cessation of their employment, contractual or other relationship in accordance with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

The policy and procedures must also require that access to the premises be terminated upon the cessation of the employment, contractual or other relationship in accordance with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

Notification When Access is No Longer Required

The policy and procedures must require an employee or other person acting on behalf of the prescribed organization granted approval to access location(s) where records of personal health information are retained, as well as his or her supervisor, to notify the prescribed organization when the employee or other person acting on behalf of the prescribed organization no longer requires such access.

The policy and procedures shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the notification must be provided; the nature and format of the notification; the time frame within which the notification must be provided; the process that must be followed in providing the notification; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for terminating access; the procedure to be followed in terminating access; the method by which access will be terminated; and the time frame within which access must be terminated.

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

The policy and procedures must require audits to be conducted of employees or other persons acting on behalf of the prescribed organization with access to the premises of the prescribed organization and to locations within the premises where records of personal health information are retained in accordance with the *Policy and Procedures In Respect of Security Audits*.
The purpose of the audit is to ensure that employees or other persons acting on behalf of the prescribed organization granted access to the premises and to locations within the premises where records of personal health information are retained continue to:

- Be employed, contracted or otherwise engaged to provide services in or for the prescribed organization;
- Be routinely required to use personal health information received by the prescribed organization for the purpose of developing and maintaining the electronic health record; and
- Require the same level of access to the personal health information.

In this regard, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, these audits must be conducted on an annual basis.

Tracking and Retention of Documentation Related to Access to the Premises

The policy and procedures shall require that a log be maintained of employees or other persons acting on behalf of the prescribed organization granted approval to access the premises of the prescribed organization and to locations within the premises where records of personal health information are retained and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log. It is also recommended that the policy and procedures address where documentation related to the receipt, review, approval and termination of access to the premises and to locations within the premises where personal

health information is retained will be maintained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining this documentation.

Policy, Procedures and Practices with Respect to Access by Visitors

The policy and procedures must address the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in identifying, screening and supervising visitors to the premises of the prescribed organization. At a minimum, the policy and procedures shall set out the identification that is required to be worn by visitors; any documentation that must be completed, provided and/or executed by employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying, screening and supervising visitors; and the documentation that must be completed, provided and executed by visitors. At a minimum, visitors shall be required to record their name, date and time of arrival, time of departure and the name of the employee(s) or other person(s) acting on behalf of the prescribed organization with whom the visitors are meeting.

The duties of employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying, screening and supervising visitors shall also be addressed. These duties shall include ensuring that visitors are accompanied at all times; ensuring that visitors are wearing the identification issued by the prescribed organization; ensuring that the identification is returned prior to departure; and ensuring that visitors complete the appropriate documentation upon arrival and departure.

The policy and procedures should also address the process to be followed when the visitor does not return the identification provided or does not document his or her date and time of departure and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the identified process.

It is also recommended that the policy and procedures address where documentation related to the identification, screening and supervision of visitors will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The policy and procedures must require employees or other persons acting on behalf of the prescribed organization to comply with this policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity,

in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes that there may have been a breach of this policy or its associated procedures.

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

A log must be maintained of employees or other persons acting on behalf of the prescribed organization granted approval to access the premises of the prescribed organization and the level of access granted. At a minimum, the log must include the name of the employee or other person acting on behalf of the prescribed organization granted approval to access the premises, and for each employee or other person acting on behalf of the prescribed organization:

- The level and nature of the access granted;
- The locations within the premises to which access is granted;
- The date that the access was granted;
- The date(s) that identification cards, access cards and/or keys were provided to the employee or other person acting on behalf of the prescribed organization;
- The identification numbers on the identification cards, access cards and/or keys, if any;
- The date of the next audit of access; and
- The date that the identification cards, access cards and/or keys were returned to the prescribed organization, if applicable.

5. Policy and Procedures for Secure Retention of Records of Personal Health Information

A policy and procedures must be developed and implemented with respect to the secure retention of records of personal health information accessible by means of the electronic health record developed or maintained by the prescribed organization, in paper and electronic format.

Retention Period

The policy and procedures must identify the retention period for records of personal health information in both paper and electronic format, including various categories thereof. The policy and procedures must mandate that records of personal health information be retained for only as long as necessary for the purpose of developing or maintaining the electronic health record.

Secure Retention

The policy and procedures must also require the records of personal health information to be retained in a secure manner and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure retention of these records. In this regard, the policy and procedures must identify the precise methods by which records of personal health information in paper and electronic format are to be securely retained, including records retained on various media.

Further, the policy and procedures must require employees or other persons acting on behalf of the prescribed organization to take steps that are reasonable in the circumstances to ensure that personal health information accessible by means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of the personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal. The reasonable steps that must be taken by employees or other persons acting on behalf of the prescribed organization shall also be outlined in the policy and procedures.

Third Party Service Providers

If a third party service provider is contracted or otherwise engaged to retain records of personal health information on behalf of the prescribed organization, the policy and procedures must also address the following additional matters.

The policy and procedures must identify the purposes for which and the circumstances in which records of personal health information will be transferred to the third party service provider for secure retention. The policy and procedures must detail the process to be followed in securely transferring the records of personal health information to and in securely retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and retrieved, the conditions pursuant to which the records will be transferred and retrieved, and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer and retrieval of the records. In this regard, the procedures shall comply with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

The policy and procedures must address the documentation that is required to be maintained in relation to the transfer of records of personal health information to the third party service provider for secure retention. In particular, the policy and procedures must require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer to document the date, time and mode of transfer and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information.

The policy and procedures must also require a detailed inventory to be maintained of records of personal health information being securely retained by the third party service provider and of records of personal health information retrieved by the prescribed organization and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the detailed inventory.

Further, the policy and procedures must require that a written agreement be executed with the third party service provider in accordance with the *Policy and Procedures for Executing Agreements with Third Party Service Providers* and containing the relevant language from the *Template Agreement For All Third Party Service Providers*. The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that the agreement has been executed prior to transferring the records of personal health information for secure retention.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, the prescribed organization permits personal health information received for the purpose of developing or maintaining the electronic health record to be retained on a mobile device. In this regard, the policy and procedures shall provide a definition of "mobile device."

In drafting this policy and its procedures, the prescribed organization must be consistent with:

- The *Act* and its regulation;
- Any directives made by the Minister with respect to the carrying out of its responsibilities and functions under the *Act* and its regulation;
- Orders and decisions issued by the IPC under the *Act* and its regulation, including Order HO-004, Order HO-007 and Order HO-008;
- Guidelines, fact sheets and best practices issued by the IPC pursuant to the *Act* and its regulation, including *Safeguarding Privacy on Mobile Devices*; and
- Evolving privacy and security standards and best practice.

Where Personal Health Information is Permitted to be Retained on a Mobile Device

If the prescribed organization permits personal health information received for the purpose of developing or maintaining the electronic health record to be retained on a mobile device, the policy and procedures must set out the purposes for which and the circumstances in which this is permitted.

Approval Process

The policy and procedures must state whether approval is required prior to retaining personal health information on a mobile device.

If approval is required, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization and the process that must be followed in determining whether to approve or deny the retention of personal health information on a mobile device. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must further set out the requirements that must be satisfied and the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device.

At a minimum, prior to any approval of a request to retain personal health information on a mobile device, the policy and procedures must require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose. The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to the *Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization*.

The policy and procedures should also set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device

The policy and procedures must require mobile devices containing personal health information to be encrypted as well as password-protected using strong and complex passwords that are in compliance with the *Policy and Procedures Relating to Passwords*. Where mobile devices have display screens, the policy and procedures must further require that a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity. The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled shall also be identified.

The policy and procedures must also identify the conditions or restrictions with which employees or other persons acting on behalf of the prescribed organization granted approval to retain personal health information on a mobile device must comply. At a minimum, the employees or other persons acting on behalf of the prescribed organization must:

- Be prohibited from retaining personal health information on a mobile device if other information, such as de-identified and/or aggregate information, will serve the purpose;
- De-identify the personal health information to the fullest extent possible;
- Be prohibited from retaining more personal health information on a mobile device than is reasonably necessary for the identified purpose;
- Be prohibited from retaining personal health information on a mobile device for longer than necessary to meet the identified purpose; and
- Ensure that the strong and complex password for the mobile device is different from the strong and complex passwords for the files containing the personal health information and that the password is supported by "defence in depth" measures.

The policy and procedures must also detail the steps that must be taken by employees or other persons acting on behalf of the prescribed organization to ensure that personal health information retained on a mobile device is protected against theft, loss and unauthorized use or disclosure and that records of the personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to retain the personal health information on a mobile device in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information* and to securely delete personal health information retained on a mobile device in accordance with the process and in compliance with the time frame outlined in the policy and procedures.

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

If the prescribed organization does not permit personal health information to be retained on a mobile device, the policy and procedures must expressly prohibit the retention of personal health information on a mobile device and must indicate whether or not personal health information received for the purpose of developing or maintaining the electronic health record may be accessed remotely through a secure connection or virtual private network.

If the prescribed organization permits personal health information to be accessed remotely, the policy and procedures must set out the purposes for which and the circumstances in which this is permitted.

Approval Process

The policy and procedures must identify whether approval is required prior to accessing personal health information remotely through a secure connection or virtual private network.

If approval is required, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in determining whether to approve or deny a request for remote access to personal health information. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must further set out the requirements that must be satisfied and the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve remote access to the personal health information.

At a minimum, prior to any approval, the policy and procedures must require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny the request to ensure that other information, such as de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information will be accessed than is reasonably necessary to meet the identified purpose.

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny the request to ensure that the viewing, handling or otherwise dealing with the personal health information has been approved pursuant to the *Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization*.

The policy and procedures should also set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Remote Access to Personal Health Information

The policy and procedures must identify the conditions or restrictions with which employees or other persons acting on behalf of the prescribed organization granted approval to access personal health information remotely must comply. At a minimum, the employees or other persons acting on behalf of the prescribed organization must be prohibited from remotely accessing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more personal health information than is reasonably necessary for the identified purpose. The policy and procedures must also set out the administrative, technical and physical safeguards that must be implemented by employees or other persons acting on behalf of the prescribed organization in remotely accessing personal health information.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information

A policy and procedures must be developed and implemented with respect to the secure transfer of records of personal health information received for the purpose of developing or maintaining the electronic health record in paper and electronic format.

Approved Methods of Secure Transfer

The policy and procedures shall require records of personal health information to be transferred in a secure manner and shall set out the secure methods of transferring records of personal health information in paper and electronic format that have been approved by the prescribed organization. The policy and procedures shall require employees or other persons acting on behalf of the prescribed organization to use the approved methods of transferring records of personal health information and shall prohibit all other methods.

Process of Secure Transfer

The procedures that must be followed in securely transferring records of personal health information through each of the approved methods must also be outlined. In outlining the process to be followed, the policy and procedures shall set out the conditions pursuant to which records of personal health information will be transferred; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer; any documentation that is required to be completed, provided and/or executed in relation to the secure transfer; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address whether and in what circumstances the employee or other person acting on behalf of the prescribed organization transferring records of personal health information is required to document the date, time and mode of transfer; the recipient of the records of personal health information; and the nature of the records of personal health information transferred. Further, the policy and procedures must address whether and in what circumstances confirmation of receipt of the records of personal health information is required from the recipient, and if so, the manner of obtaining and recording acknowledgement of receipt of the records of personal health information and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for doing so. In addressing whether and in what circumstances an employee or other person acting on behalf of the prescribed organization is required to document the transfer and whether and in what circumstances confirmation of receipt is required, regard must be had to the other privacy and security policies put in place[2].

Administrative, Technical and Physical Safeguards to Ensure Secure Transfer

The policy and procedures must set out the administrative, technical and physical safeguards that must be implemented by employees or other persons acting on behalf of the prescribed organization in transferring records of personal health information through each of the approved methods in order to ensure that the records of personal health information are transferred in a secure manner.

The approved methods of securely transferring records of personal health information and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of personal health information must be consistent with:

- The *Act* and its regulation;
- Any directives made by the Minister with respect to the carrying out of its responsibilities and functions under the *Act* and its regulation;
- Orders issued by the IPC under the *Act* and its regulation, including but not limited to Order HO-004, Order HO-007, Order HO-008 and Order HO-011;
- Guidelines, fact sheets and best practices issued by the IPC, including *Fact Sheet: Communicating Personal Health Information by Email, Fact Sheet 18: The Secure Transfer of Personal Health Information, and Guidelines on Facsimile Transmission Security*; and
- Evolving privacy and security standards and best practices.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and

2 For example, the *Policy and Procedures for Secure Retention of Records of Personal Health Information, Policy and Procedures for Secure Disposal of Records of Personal Health Information, Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information* and *Policy and Procedures for Executing Agreements with Third Party Service Providers.*

procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information

A policy and procedures must be developed and implemented with respect to the secure disposal of records of personal health information received for the purpose of developing or maintaining the electronic health record in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

The policy and procedures must require records of personal health information to be disposed of in a secure manner and must provide a definition of secure disposal that is consistent with the *Act* and its regulation.

Methods of Secure Disposal

The policy and procedures must identify the precise method by which records of personal health information in paper format are required to be securely disposed of and the precise method by which records of personal health information in electronic format, including records retained on various media, are required to be securely disposed of.

In addressing the precise method by which records of personal health information must be securely disposed of, the prescribed organization must ensure that the method of secure disposal adopted is consistent with:

- The *Act* and its regulation;
- Any directives made by the Minister with respect to the carrying out of its responsibilities and functions under the *Act* and its regulation;
- Orders and decisions issued by the IPC under the *Act* and its regulation, including Order HO-001 and Order HO-006;
- Guidelines, fact sheets and best practices issued by the IPC, including *Fact Sheet 10: Secure Destruction of Personal Information*; and
- Evolving privacy and security standards and best practices.

Secure Retention Pending Disposal

The policy and procedures must further address the secure retention of records of personal health information pending their secure disposal. At a minimum, the policy and procedures must require the physical segregation of records of personal health information intended for secure disposal from other records intended for recycling, must require that an area be designated for the secure retention of records of personal health information pending their secure disposal and must require the records of personal health information to be retained in a clearly marked and locked container pending their secure disposal. The policy and procedures shall comply with the *Policy and Procedures for Secure Retention of Records of Personal Health Information* The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure retention of records of personal health information pending their secure disposal.

Process of Secure Disposal

In the event that records of personal health information or certain categories of records of personal health information will be securely disposed of by a designated employee or other person acting on behalf of the prescribed organization, who is not a third party service provider, the policy and procedures must identify the designated employee or other person acting on behalf of the prescribed organization responsible for securely disposing of the records of personal health information; the responsibilities of the designated employee or other person acting on behalf of the prescribed organization in securely disposing of the records; and the time frame within which, the circumstances in which and the conditions pursuant to which the records of personal health information must be securely disposed of. The policy and procedures must also require the designated employee or other person acting on behalf of the prescribed organization to provide a certificate of destruction:

- Identifying the records of personal health information to be securely disposed of;
- Confirming the secure disposal of the records of personal health information;
- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the employee(s) or other person(s) acting on behalf of the prescribed organization who performed the secure disposal.

The time frame within which and the employee(s) or other person(s) acting on behalf of the prescribed organization to whom certificates of destruction must be provided following the secure disposal of the records of personal health information must also be addressed in the policy and procedures.

In the event that records of personal health information or certain categories of records of personal health information will be securely disposed of by a person that is a third party service provider, the policy and procedures must address the following additional matters.

The policy and procedures must detail the procedure to be followed by the prescribed organization in securely transferring the records of personal health information to the third party service provider for secure disposal. At a minimum, the policy and procedures must identify

the secure manner in which the records of personal health information will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer of the records. In this regard, the policy and procedures shall comply with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer of records of personal health information to document the date, time and mode of transfer, and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information. A detailed inventory related to the records of personal health information transferred to the third party service provider for secure disposal must also be maintained and the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining this inventory.

Further, the policy and procedures must require that a written agreement be executed with the third party service provider in accordance with the *Policy and Procedures for Executing Agreements with Third Party Service Providers* and containing the relevant language from the *Template Agreement For All Third Party Service Providers*. The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.

The policy and procedures must also outline the procedure to be followed in tracking the dates that records of personal health information are transferred for secure disposal and the dates that certificates of destruction are received from the third party service provider or from the designated employee or other person acting on behalf of the prescribed organization that is not a third party service provider, and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting such tracking. Further, the policy and procedures must outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the time set out in the agreement with the third party service provider, and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing this process.

It is also recommended that the policy and procedures address where certificates of destruction will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining the certificates of destruction.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and

procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

9. Policy and Procedures Relating to Passwords

A policy and procedures must be developed and implemented with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs used to create or maintain the electronic health record regardless of whether they are owned, leased or operated by the prescribed organization.

The policy and procedures must be based on an assessment of risks, and form part of a comprehensive policy regarding identification, authentication and authorization ("access control") that is consistent with evolving industry best practices. The policy and procedures must:

- establish rules for password strength and composition, protection, use, confidentiality and change requirements;
- establish a process for handling repeated failed access attempts, including the number of failed attempts that will result in a denial of access;
- establish a process for handling idle sessions, including the length of time that will require re-authentication and the imposition of a mandatory system-wide password-protected lock screen after a defined period of inactivity;

The policy and procedures shall further identify the administrative, technical and physical safeguards that must be implemented by employees or other persons acting on behalf of the prescribed organization in respect of passwords in order to ensure that the personal health information received for the purpose of developing or maintaining the electronic health record is protected against theft, loss and unauthorized use or disclosure and that the records of personal health information are protected against unauthorized copying, modification or disposal. At a minimum, employees or other persons acting on behalf of the prescribed organization must be required to keep their passwords private and secure and to change their passwords immediately if they suspect that their password has become known to any other individual, including another employee or other person acting on behalf of the prescribed organization. Employees or other persons acting on behalf of the prescribed organization must also be prohibited from writing down, displaying, revealing, hinting at, providing, sharing or otherwise making their password known to any other individual, including another employee or other person acting on behalf of the prescribed organization.

The prescribed organization must ensure that the policy and procedures it has developed in this regard, are consistent with any directives made by the Minister with respect to the carrying out of its responsibilities and functions under the *Act* and its regulation; any orders and decisions issued by the IPC under the *Act* and its regulation; with any guidelines, fact sheets and best practices issued by the IPC; and with evolving privacy and security standards and best practices.

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

10. Policy and Procedures In Respect of Privacy Notices

A policy and procedures must be developed and implemented requiring privacy notices to be displayed on all information systems and technologies involving personal health information.

The policy and procedures must set out the required content of the privacy notice, must require the privacy notice to be prominently displayed on all information systems and technologies involving personal health information, and must require employees and other persons acting on behalf of the prescribed organization to acknowledge and agree to certain statements prior to accessing the personal health information. At a minimum, the privacy notice must:

- Indicate that all viewing, handling and otherwise dealing with of personal health information will be logged, audited and monitored;
- Require employees and other persons acting on behalf of the prescribed organization to acknowledge and agree that they:
    - will only view, handle or otherwise deal with the personal health information for the purpose of developing and maintaining the electronic health record;
    - will comply with the *Act* and its regulations;
    - have read, understood and agree to comply with the privacy and security policies, procedures put in place; and

- Set out the consequences for viewing, handling or otherwise dealing with the personal health information for other purposes and for failing to comply with the *Act* and its regulations and with the privacy and security policies, procedures and practices put in place.

The policy and procedures and the privacy notice developed in this regard must be consistent with orders and decisions issued by the IPC under the *Act* and its regulations, including Order HO-013; and with guidelines, fact sheets and best practices issued by the IPC, including *Detecting and Deterring Unauthorized Access to Personal Health Information*.

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

A policy and procedures must be developed and implemented requiring employees or other persons acting on behalf of the prescribed organization to acknowledge and agree to comply with the Acceptable Use Agreement. The policy and procedures must further require the Acceptable Use Agreement to contain the language from the *Template Acceptable Use Agreement*.

Timing of Acceptable Use Agreements

The policy and procedures shall set out the timeframe within which employees or other persons acting on behalf of the prescribed organization must acknowledge and agree to comply with the Acceptable Use Agreement. At a minimum, the policy and procedures shall require these employees or other persons acting on behalf of the prescribed organization acknowledge and agree to comply with the Acceptable Use Agreement prior to accessing information systems and technologies involving personal health information, including personal health information that has been de-identified and/or aggregated, for the first time and on an annual basis thereafter. The policy and procedures shall further identify the timeframe each year in which employees and other persons acting on behalf of the prescribed organization are required to acknowledge and agree to comply with the Acceptable Use Agreement on an ongoing basis.

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

The policy and procedures must identify the employees(s) and other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in ensuring that employee(s) and other person(s) acting on behalf of the prescribed organization acknowledges and agrees to comply with the Acceptable Use Agreement.

Tracking Acceptable Use Agreements

The policy and procedures shall require that a log be maintained of all Acceptable Use Agreements acknowledged and agreed to by employees or other persons acting on behalf of the prescribed organization. The policy and procedures must further identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for maintaining the log and for tracking that Acceptable Use Agreements have been acknowledged and agreed to.

The process to be followed in tracking that all employees or other persons acting on behalf of the prescribed organization have acknowledged and agreed to comply with the Acceptable Use Agreement shall also be outlined. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed to verify that Acceptable Use Agreements have been acknowledged and agreed to; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for identifying employee(s) and other person(s) acting on behalf of the prescribed organization who have not acknowledged and agreed to comply with the Acceptable Use Agreement and for ensuring that they do so, including the timeframe within which the procedure must be implemented.

It is also recommended that the policy and procedures address where documentation related to the Acceptable Agreements will be retained and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

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

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

Where employees or other persons acting on behalf of the prescribed organization are being provided access to information systems and technologies involving personal health information, the Acceptable Use Agreement must identify the purposes for which these employees or other persons are permitted to view, handle or otherwise deal with the personal health information.

Where employees or other persons acting on behalf of the prescribed organization are being provided access to information systems and technologies involving personal health information has been de-identified and/or aggregated, the Acceptable Use Agreement must identify the purposes for which these employees or other persons are permitted to use and disclose the de-identified or aggregated information.

Administrative, Technical and Physical Safeguards

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

With respect to personal health information, this includes requiring employees or other persons acting on behalf of the prescribed organization to only view, handle or otherwise deal with the personal health information if other information, such as de-identified and/or aggregate information, will not serve the purposes and not view, handle or otherwise deal with more of the personal health information than is reasonably necessary.

With respect to personal health information that has been de-identified and/or aggregated, this includes requiring employees or other persons acting on behalf of the prescribed organization not to use the de-identified or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

Consequences of Breach and Monitoring Compliance

The Acceptable Use Agreement must outline the consequences of breach of the agreement and must address the manner in which compliance with the Acceptable Use Agreement will be enforced. The Acceptable Use Agreement must further stipulate that compliance with the Acceptable Use Agreement will be audited and must address the manner in which compliance will be audited.

Required Acknowledgements and Agreements

The Acceptable Use Agreement must require employees and other persons acting on behalf of the prescribed organization to acknowledge and agree:

- Not to view, handle or otherwise deal with personal health information, including personal health information that has been de-identified and/or aggregated, except as permitted by the Acceptable Use Agreement and by the privacy policies, procedures and practices put in place by the prescribed organization;
- To implement the administrative, technical and physical safeguards set out in the Acceptable Use Agreement;
- To comply with the *Act* and its regulations and the terms of the Acceptable Use Agreement;
- That they have read, understood and agree to comply with the privacy and security policies, procedures and practices put in place pursuant to the *Act* and its regulations; and
- To provide notification at the first reasonable opportunity of a privacy breach, information security breach, suspected privacy breach or suspected information security breach in accordance with the *Policy and Procedures for Privacy Breach Management* and/or *Policy and Procedures for Information Security Breach Management*, as the case may be.

13. Log of Acceptable Use Agreements

A log of all Acceptable Use Agreements acknowledged and agreed to by employees or other persons acting on behalf of the prescribed organization must be maintained. At a minimum, the log must set out the name of the employee or other person acting on behalf of the prescribed organization, and for each employee or other person:

- The date of commencement of his or her employment, contractual or other relationship with the prescribed organization; and
- The dates that the Acceptable Use Agreement was acknowledged and agreed to.

14. Policy and Procedures for End User Agreements

A policy and procedures must be developed and implemented requiring each end user (including an end user who is a health information custodian or an agent of a health information custodian), who provides personal health information to or collects personal health information by means of the electronic health record to acknowledge and agree to comply with the End User Agreement. The policies and procedures must further require the End User Agreement to contain the language from the *Template End User Agreement*.

Timing of End User Agreement

The policies and procedures shall set out the timeframe within which end users must acknowledge and agree to comply with the End User Agreement. At a minimum, the policy and procedures shall require those end users to acknowledge and agree to comply with the End User Agreement prior to providing personal health information to or collecting personal health information via the electronic health record for the first time, and on an annual basis thereafter. The policy and procedures shall further identify the timeframe each year in which end users are required to acknowledge and agree to comply with the End User Agreement on an ongoing basis.

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

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

Tracking End User Agreements

The policy and procedures shall require that a log be maintained of all End User agreements acknowledged and agreed to by end users. The policy and procedures must further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log and for tracking that End User Agreements have been acknowledged and agreed to.

The process to be followed in tracking that all end users have acknowledged and agreed to comply with the End User Agreement shall also be outlined. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed to verify that End User Agreements have been acknowledged and agreed to; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying end users who have not acknowledged and agreed to comply with the End User Agreement and

for ensuring that these custodians and agents do so, including the timeframe within which the procedure must be implemented.

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

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

15. Template End User Agreements

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

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

The End User Agreement must identify the purposes for which the end user is permitted to provide personal health information to or to collect, use or disclose personal health information by means of the electronic health record. Each provision, collection, use or disclosure identified in the End User Agreement must be permitted by the *Act* and its regulations.

Administrative, Technical and Physical Safeguards

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

Consequences of Breach and Monitoring Compliance

The End User Agreement must outline the consequences of breach of the agreement and must address the manner in which compliance with the End User Agreement will be enforced. The End User Agreement must further stipulate that compliance with the End User Agreement will be audited and must address the manner in which compliance will be audited.

Required Acknowledgements and Agreements

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

- To provide, collect, use, disclose, view, handle or otherwise deal with personal health information via the electronic health record only in accordance with the terms of the End User Agreement and the *Act* and regulations;
- To implement and comply with the administrative, technical and physical safeguards set out in the End User Agreement;
- To provide the notifications required by the End User Agreement and the *Act* and its regulations; and
- To comply with the *Act* and its regulations and the terms of the End User Agreement.

16. Log of End User Agreements

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

- The name of each health information custodian or agent;
- For each agent, the name of the health information custodian on whose behalf the agent is acting; and
- The dates that the End User Agreement was acknowledged and agreed to.

17. Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

A policy and procedures must be developed and implemented for the creation, maintenance and ongoing review of system control and audit logs involving personal health information that is accessible by means of the electronic health record. At a minimum, the system control and audit logs that must be created, maintained and reviewed must include the electronic records the prescribed organization is required to keep under paragraph 4 of section 55.3 of the *Act*.

The policy and procedures must be consistent with evolving industry standards and best practices and must be commensurate with the amount and sensitivity of the personal health information maintained; with the number and nature of employees or other persons acting on behalf of the prescribed organization with access to the personal health information; with the number and nature of persons acting on behalf of health information custodians with access to the personal health information; and with the threats and risks associated with the personal health information.

In drafting the policy and its procedures, regard must be had to orders and decisions issued by the IPC under the Act and its regulations, including Order HO-010 and Order HO-013, to guidelines, fact sheets and best practices issued by the IPC, including *Detecting and Deterring Unauthorized Access to Personal Health Information* and to the requirements of the *Act* and its regulation, including paragraphs 4 and 7 through 9 of section 55.3 of the *Act*; and evolving privacy and security standards and best practices.

Logging Functionality

The policy and procedures shall require the prescribed organization to ensure that all information systems, technologies, applications and programs used to develop and maintain the electronic health record involving personal health information have logging functionality.

The policy and procedures shall further set out the types of events that are required to be logged and the types of logs that are required to be created and maintained. At a minimum, as required under paragraph 4 of section 55.3 of the *Act*, the policy and procedures must require the prescribed organization to keep an electronic record of all instances where:

- All or part of the personal health information that is accessible by means of the electronic health record is viewed, handled or otherwise dealt with by employees or other persons acting on behalf of the prescribed organization or by health information custodians or their agents;
- Personal health information is transmitted to a custodian by means of the electronic health record, where the custodian has requested the transmission;

Content of Logs

The policy and procedures must set out the nature and scope of the information that must be contained in each type of system control and audit log.

At a minimum, the electronic records the prescribed organization is required to keep must contain the following:

Where all or part of the personal health information that is accessible by means of the electronic health record is viewed, handled or otherwise dealt with by employees or other persons acting on behalf of the prescribed organization or by health information custodians or their agents:

- The individual to whom the information relates;
- The type of information that is viewed, handled or otherwise dealt with;
- All persons who have viewed, handled or otherwise dealt with the information; and
- The date, time and location that the personal health information was viewed, handled, or otherwise dealt with;

Where the prescribed organization transmits personal health information to a health information custodian by means of the electronic health record, upon the request of the custodian:

- The individual to whom the information relates;
- The type of information that is transmitted;
- The custodian requesting the information;
- The date and time that the information was transmitted; and
- The location to which the information was transmitted.

Retention of Logs

The policy and procedures shall identify, for each type of system control and audit log that is required to be created and maintained, the length of time that system control and audit logs are required to be retained, the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining the system control and audit logs and where the system control and audit logs will be retained.

The policy and procedures shall further require the system control and audit logs, to be immutable, that is, the prescribed organization must be required to ensure that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way. They must also set out the procedures that must be implemented in this regard and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing these procedures.

Auditing and Monitoring

With respect to system control and audit logs created and maintained by the prescribed organization, the policy and procedures shall set out the types of events that are required to be audited and monitored. This shall include, at a minimum, the electronic records required to be kept pursuant to paragraph 4 of section 55.3 of the *Act* and to be audited and monitored pursuant to paragraph 7 of section 55.3 of the *Act*. The policy and procedures shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that the types of events that are required to be audited are in fact audited and monitored. It is recommended that new automated tools be explored to assist in auditing and monitoring information systems, technologies, applications and programs used to develop and maintain the electronic health record.

The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for auditing and monitoring system control and audit logs, and the types of auditing and monitoring that must be conducted. For each type of auditing and monitoring required to be conducted, the policy and procedures shall set out the frequency with which and the circumstances in which the auditing and monitoring must be conducted, the criteria that must be used, and process that must be followed. In this regard, the policy and procedures shall require an auditing and monitoring schedule to be developed and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for developing the auditing and monitoring schedule.

At a minimum, the policies and procedures must require auditing and monitoring:

- in response to inquiries and complaints from individuals regarding the collection, use of disclosure of their personal health information and whenever a privacy breach or suspected privacy breach is identified; and
- of all instances where personal health information that is accessible by means of the electronic health record is viewed, handled or otherwise dealt with by someone acting for or on behalf of the prescribed organization or by a custodian or an agent of a custodian.

In auditing and monitoring all instances in which personal health information is viewed, handled or otherwise dealt with, the policy and procedures must require a reasonable combination of proactive (e.g., to identify potential privacy breaches) and reactive (e.g., in response to a privacy complaint) auditing and monitoring, as well as targeted (e.g., activities of a specific agent or activities of all agents in relation to the personal health information of a specific individual) and random (e.g., activities of a randomly selected agent or activities of all agents in respect of the personal health information of a randomly selected individual). The policy and procedures must also set out the circumstances where auditing and monitoring must be conducted on a continuous basis (e.g., every instance where a consent directive is overridden).

For each type of system control and audit log that is required to be audited and monitored, the policy and procedures shall set out the process to be followed in conducting the auditing and monitoring.

The policy and procedures shall also set out the nature of the documentation that must be completed, provided and/or executed following the auditing and monitoring; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; the required content of the documentation; and the frequency with which this documentation must be provided.

Further, the policy and procedures must address the findings arising from the auditing and monitoring of system control and audit logs, and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the findings, for establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed.

The manner and format for communicating the findings of the auditing and monitoring and how the findings have been or are being addressed must also be outlined. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the auditing and monitoring of system control and audit logs. The policy and procedures must identify the mechanism and format for communicating the findings of the auditing and monitoring; the time frame within which the findings of the auditing and monitoring must be communicated; and to whom the findings of the auditing and monitoring must be communicated.

Further, the policy and procedures must set out the process to be followed in tracking the findings of the auditing and monitoring of system control and audit logs. The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for tracking that the findings have been addressed within the identified timelines.

Responding to Requests for Electronic Records

The policy and procedures shall set out the process that must be followed in responding to requests from health information custodians pursuant to paragraph 9 of section 55.3 of the *Act* for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the *Act*. At a minimum, the policy and procedures shall indicate that the prescribed organization must provide, upon the request of a health information custodian that requires the records to audit and monitor its compliance with the *Act*, the electronic records that the prescribed organization is required to keep under the *Act*. The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving requests for electronic records from health information custodians; for preparing the electronic records requested by health information custodians and for providing the requested information to health information custodians; any documentation that must be completed, provided, and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization and/or the health information custodian requesting the electronic records; the employee(s) or other person acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. In setting out the process for responding to requests, the policy and procedures must specify the form, manner and time frame within which the electronic records requested by health information custodians must be provided.

The policy and procedures shall also set out the process that must be followed in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of the *Act* for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the *Act*. At a minimum, the policy and procedures shall indicate that the prescribed organization must provide, upon the request of the IPC, the electronic records that the prescribed organization is required to keep under the *Act* to the IPC for the purposes of Part VI of the *Act*. The policy and procedures must set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for receiving requests for electronic records from the IPC; for preparing the electronic records requested by the IPC and for providing the requested information to the IPC; any documentation that must be completed, provided and/or executed by the employee(s) or other person(s) acting on behalf of the prescribed organization and/or the IPC; the employee(s) or other person acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. In setting out the process for responding to requests, the policy and procedures must specify the form, manner and time frame within which the electronic records requested by the IPC must be provided.

Logging

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

- All requests from health information custodians, made pursuant to paragraph 9 of section 55.3 of the *Act*, for the electronic records the prescribed organization is required to maintain pursuant to paragraph 4 of section 55.3 of the *Act*;
- All requests from the IPC, made pursuant to paragraph 8 of section 55.3 of the *Act*, for the electronic records the prescribed organization is required to maintain pursuant to paragraph 4 of section 55.3 of the *Act*;

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining each log and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for tracking requests for electronic records to ensure that they are responded to or provided within the identified time frame. The policy and procedures should further address where documentation related to auditing and monitoring will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the auditing and monitoring to notify the prescribed organization, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Managemen*t and of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management*.

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

The prescribed organization shall maintain a log of the electronic records that are provided to health information custodians, pursuant to paragraph 9 of section 55.3 of the *Act*. At a minimum, for each request for electronic records received from a health information custodian, the log shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization who received the request for electronic records; the date the request for electronic records was received by the prescribed organization, the health information custodian who made the

request for electronic records; the types of electronic records that were requested by the health information custodian; the employee(s) or other person(s) acting on behalf of the prescribed organization who responded to the request; the types of electronic records that were provided to the health information custodian; the agent of the health information custodian to whom the electronic records were provided; and the form, manner and date the electronic records were provided to the health information custodian.

19. Log of Requests for Electronic Records from the IPC

The prescribed organization shall maintain a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of section 55.3 of the *Act*. At a minimum, for each request for electronic records received from the IPC, the log shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization who received the request for electronic records; the date the request was received, the employee(s) or other person(s) acting on behalf of the IPC who submitted the request; the types of electronic records that were requested by the IPC; the employee(s) or other person(s) acting on behalf of the prescribed organization who responded to the request; the types of electronic records that were provided to the IPC; the employee(s) or other person(s) acting on behalf of the IPC to whom the electronic records were provided; the form, manner and date when the electronic records were provided to the IPC.

20. Policy and Procedures for Patch Management

A policy and procedures must be developed and implemented for patch management for all information systems, technologies, equipment, resources, applications and programs used to create and maintain the electronic health record.

Patch Monitoring

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for monitoring the availability of patches, the frequency with which such monitoring must be conducted and the procedure that must be followed in this regard.

Patch Analysis

The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for analyzing the patch and making a determination as to whether or not the patch should be implemented must also be identified. The policy and procedures shall further discuss the process that must be followed and the criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for undertaking this analysis and making this determination, as well as the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

In circumstances where a determination is made that the patch should not be implemented, the policy and procedures shall require the responsible employee(s) or other person(s) acting on behalf of the prescribed organization to document the description of the patch; the date that the patch became available; the severity level of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; and the rationale for the determination that the patch should not be implemented.

In circumstances where a determination is made that the patch should be implemented, the policy and procedures shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining the time frame for implementation of the patch and the priority of the patch.

Patch Implementation

The policy and procedures shall also set out the process for patch implementation, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for patch implementation and any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The circumstances in which patches must be tested, the time frame within which patches must be tested, the procedure for testing and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing shall also be addressed, including the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also require documentation to be maintained in respect of patches that have been implemented and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining this documentation. At a minimum, the documentation must include a description of the patch; the date that the patch became available; the severity level and priority of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; the date that the patch was implemented; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the patch; the date, if any, when the patch was tested; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing; and whether or not the testing was successful.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

21. Policy and Procedures Related to Change Management

A policy and procedures must be developed and implemented for reviewing and determining whether to approve a change to the operational environment of the prescribed organization in creating or maintaining the electronic health record.

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for reviewing and determining whether to approve a change to the operational environment and the process that must be followed and the requirements that must be satisfied in this regard. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. At a minimum, the documentation shall describe the change requested why the change is necessary and the impact of executing or not executing the change to the operational environment.

The criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny a request for a change to the operational environment shall also be identified.

The policy and procedures shall also set out the manner in which the decision approving or denying the request for a change to the operational environment and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

If the request for a change to the operational environment is not approved, the policy and procedures shall require the responsible employee(s) or other person(s) acting on behalf of the prescribed organization to document the change to the operational environment requested, the name of the employee or other person acting on behalf of the prescribed organization requesting the change, the date that the change was requested and the rationale for the determination that the change should not be implemented.

If the request for a change to the operational environment is approved, the policy and procedures shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining the time frame for implementation of the change and the priority assigned to the change requested.

The policy and procedures shall also set out the process for implementation of the change to the operational environment, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementation and any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The circumstances in which changes to the operational environment must be tested, the time frame within which changes must be tested, the procedure for testing and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing shall also be addressed in the policy and procedures, including the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also require documentation to be maintained of changes that have been implemented and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining this documentation. At a minimum, the documentation must include a description of the change requested; the name of the employee or other person acting on behalf of the prescribed organization requesting the change; the date that the change was requested; the priority assigned to the change; the date that the change was implemented; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for implementing the change; the date, if any, when the change was tested; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing; and whether or not the testing was successful.

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and*

Procedures In Respect of Security Audits, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

22. Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

A policy and procedures must be developed and implemented for the back-up and recovery of records of personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record.

The policy and procedures shall identify the nature and types of back-up storage devices maintained by the prescribed organization; the frequency with which records of personal health information are backed-up; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for the back-up and recovery of records of personal health information; and the process that must be followed and the requirements that must be satisfied in this regard. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Testing the Procedure for Back-Up and Recovery

The policy and procedures shall also address testing the procedure for back-up and recovery of records of personal health information, the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for testing, the frequency with which the procedure is tested and the process that must be followed in conducting such testing. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) and other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures shall further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that back-up storage devices containing records of personal health information are retained in a secure manner. The policy and procedures must also identify the location where they are required to be retained and the

length of time that they are required to be retained. In this regard, the policy and procedures shall require the backed-up records of personal health information to be retained in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information* and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that they are retained in a secure manner.

Third Party Service Providers

If a third party service provider is contracted or otherwise engaged to retain backed-up records of personal health information, the policy and associated procedures must also address the following additional matters.

The policy and procedures must require the backed-up records of personal health information to be transferred to and from the third party service provider in a secure manner. They must also detail the procedure to be followed in securely transferring the backed-up records of personal health information to the third party service provider and in securely retrieving the backed-up records from the third party service provider, including the secure manner in which they will be transferred and retrieved, the conditions pursuant to which they will be transferred and retrieved and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer and retrieval of the backed-up records. In this regard, the procedures shall comply with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

Further, the policy and procedures must address the documentation that is required to be maintained in relation to the transfer of backed-up records of personal health information to the third party service provider for secure retention. In particular, the policy and procedures must require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring the secure transfer to document the date, time and mode of transfer and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the backed-up records of personal health information. A detailed inventory of the backed-up records that are being securely retained by, and that are being retrieved from, the third party service provider must also be maintained, and the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the detailed inventory.

Further, the policy and procedures must require that a written agreement be executed with the third party service provider in accordance with the *Policy and Procedures for Executing Agreements with Third Party Service Providers* and containing the relevant language from the *Template Agreement For All Third Party Service Providers*. The policy and procedures must further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for ensuring that the agreement has been executed prior to transferring the backed-up records of personal health information to the third party service provider for retention.

Availability of Backed-Up Records

The policy and procedures should further address the need for the availability of backed-up records of personal health information, including the circumstances in which the backed-up records are required to be made available.

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Managemen*t, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

23. Policy and Procedures on the Acceptable Use of Technology

A policy and procedures must be developed and implemented outlining the acceptable use of information systems, technologies, equipment, resources, applications and programs used for the purpose of developing or maintaining the electronic health record regardless of whether they are owned, leased or operated by the prescribed organization.

The policy and procedures shall set out the uses that are prohibited without exception, the uses that are permitted without exception and the uses that are permitted only with prior approval.

For those uses that are permitted only with prior approval, the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for reviewing and determining the request and the process that must be followed and the requirements that must be satisfied in this regard. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. The criteria that must be considered by the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for determining whether to approve or deny the request shall also be identified.

The policy and procedures should also set out the manner in which the decision approving or denying the request and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

24. Threat and Risk Assessment Policy and Procedures

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

In identifying the circumstances in which threat and risk assessments are required to be conducted, at a minimum the policy and procedures must specify that a threat and risk assessment must be conducted for all information systems, technologies, equipment, resources, applications and programs used for the purpose of developing or maintaining the electronic health record, including each system that retrieves, processes or integrates personal health information in the electronic health record (each, for the purposes of this section of this Manual, a “system”). The policy and procedures must ensure that the prescribed organization conducts threat and risk assessments on existing and proposed systems, as well as whenever changes to existing systems are contemplated.

The policy and procedures must also address the timing of threat and risk assessments. With respect to proposed systems, and proposed changes to existing systems, the policy and procedures must require that threat and risk assessments be conducted at the earliest possible stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing systems, the policy and procedures must require that a timetable be developed to ensure threat and risk assessments are conducted and the policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for developing the timetable.

Once threat and risk assessments have been completed, the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the prescribed organization's security practices. The policy and procedures must also identify the circumstances in which and the frequency with which the threat and risk assessments are required to be reviewed.

The policy and procedures must also identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in identifying when threat and risk assessments are required; in identifying when threat and risk assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that threat and risk assessments are conducted and completed; and in ensuring that threat and risk assessments are reviewed and amended, if necessary. The role of employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the security program shall also be identified in respect of threat and risk assessments.

The policy and procedures must also stipulate the required threat and risk assessment methodology. At a minimum, the threat and risk assessment methodology should include:

- Scope of the threat and risk assessment, including risk tolerance level;
- Asset identification;
- Asset valuation;
- Identification of safeguards (both existing and those pending implementation);
- Identification of threats and vulnerabilities;
- Assessment of the likelihood of threats;
- Assessment of the potential impact of threats;
- Risk analysis, based on both threat likelihood and size of impact, including prioritized list of threats;
- Risk treatment, including recommendations to mitigate, transfer or avoid risk; and
- Residual risk analysis and acceptance.

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

The process for addressing the recommendations arising from threat and risk assessments, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations, is also required to be outlined.

The policy and procedures must require that a log be maintained of threat and risk assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures must also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log.

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization 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.

25. Log of Threat and Risk Assessments

The prescribed organization shall maintain a log of threat and risk assessments that have been completed and of threat and risk assessments that have been undertaken but that have not been completed. The log shall describe the system that is at issue; the date the threat and risk assessment was completed or is expected to be completed; the employee(s) and other persons acting on behalf of the prescribed organization responsible for completing or ensuring the completion of the threat and risk assessment; the recommendations arising from the threat and risk assessment; the employee(s) and other persons acting on behalf of the prescribed organization responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

The prescribed organization shall also maintain a log of new and proposed changes to existing systems for which threat and risk assessments have not been undertaken. For each such system, the log shall set out the date that the threat and risk assessment is expected to be completed and the employee(s) and other persons acting on behalf of the prescribed organization responsible for completing or ensuring the completion of the threat and risk assessment.

26. Policy and Procedures In Respect of Security Audits

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

- Audits to assess compliance with the security policies, procedures and practices implemented by the prescribed organization;
- Threat and risk assessments;
- Security reviews or assessments;
- Vulnerability assessments;
- Penetration testing;
- Ethical hacks; and
- Reviews of system control and audit logs, including the electronic records required to be kept pursuant to paragraph 4 of section 55.3 of the *Act* and to be audited and monitored pursuant to paragraph 7 of section 55.3 of the *Act*.

With respect to each security audit that is required to be conducted, the policy and procedures must set out the purposes of the security audit; the nature and scope of the security audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the security audit; and the frequency with which and the circumstances in which each security audit is required to be conducted. In this regard, the policy and procedures shall require a security audit schedule to be developed and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for developing the security audit schedule.

For each type of security audit that is required to be conducted, the policy and procedures shall also set out the process to be followed in conducting the audit. This shall include the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures must further discuss the documentation that must be completed, provided and/or executed in undertaking each security audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The role of the employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from security audits, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations within the identified timelines.

The policy and procedures must also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the security audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the manner and format in which the findings of security audits, including the recommendations arising from the security audits and the status of addressing the recommendations, are communicated. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the security audit; the mechanism and format for communicating the findings of the security audit; the time frame within which the findings of the security audit must be communicated; and to whom the findings of the security audit will be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures must further require that a log be maintained of security audits and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log and for tracking that the recommendations arising from the security audits are addressed within the identified time frame. They should further address where documentation related to security audits will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

The policy and procedures must also require the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the security audit to notify the prescribed organization, at the first reasonable opportunity, of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management* and of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Management*.

27. Log of Security Audits

The prescribed organization shall maintain a log of all security audits that have been completed. The log shall set out the nature and type of the security audit conducted; the date that the security audit was completed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing the security audit; the recommendations arising from the security audit; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

28. Policy and Procedures for Information Security Breach Management

A policy and procedures must be developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of information security

breaches. The policy and procedures must provide a definition of the term "information security breach." At a minimum, an information security breach shall be defined to include:

- A contravention of the security policies, procedures or practices implemented by the prescribed organization;
- A contravention of the Acceptable Use Agreement;
- A contravention of the End User Agreement; and
- An event that compromises or threatens the security of information systems, technologies, equipment, resources, applications and programs involving personal health information.

Identification of Information Security Breaches

The policy and procedures must set out the manner in which information security breaches or suspected information security breaches will be identified by the prescribed organization. At a minimum, the policy and procedures must indicate that information security breaches or suspected information security breaches will be identified through reports by employees or other persons acting on behalf of the prescribed organization, reports by health information custodians, security audits, privacy complaints and inquiries, and the auditing and monitoring of the electronic records the prescribed organization is required to keep.

The policy and procedures shall impose a mandatory requirement on employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization of an information security breach or suspected information security breach.

In this regard, the policy and procedures shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization who must be notified of the information security breach or suspected information security breach and shall provide contact information for the employee(s) or other person(s) acting on behalf of the prescribed organization who must be notified. The policy and procedures shall further stipulate the time frame within which notification must be provided, whether the notification must be provided verbally and/or in writing and the nature of the information that must be provided upon notification.

The policy and procedures shall also address the documentation that must be completed, provided and/or executed with respect to notification; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Information Security Breaches Caused by One or More Health Information Custodians

The policy and procedures must specify that where the prescribed organization identifies an information security breach or suspected information security breach that was caused by one or more health information custodians, the prescribed organization must report the information security breach or suspected information security breach to the health information custodian(s).

The policy and procedures must specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall cooperate with health information custodians in developing a policy and procedures to make a determination of whether an information security breach has in fact occurred and if so, to contain, investigate and remediate the information security breach in circumstances where the information security breach or suspected information security breach was caused by one or more information custodians.

The policy and procedures must also specify that, when requested to do so or directed to do so by the Minister, the prescribed organization shall assist health information custodians in making a determination of whether an information security breach has in fact occurred and if so, assist in containing, investigating and remediating the information security breach where the information security breach or suspected information security breach was caused by one or more health information custodians.

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

The privacy policy and procedures shall require the prescribed organization to take the following steps in any instance in which a information security breach or suspected information security breach is caused by: an employee(s) or other person(s) acting on behalf of the prescribed organization; a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; or an unauthorized person who is not an employee or other person acting on behalf of the prescribed organization nor an agent of a health information custodian.

Determination of Whether a Security Breach Occurred

The policy and procedures shall require the prescribed organization to make a determination of whether an information security breach has in fact occurred and if so what, if any, personal health information has been breached. A determination shall further be made of the extent of the information security breach and whether the breach is an information security breach or privacy breach or both. The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for making these determinations must also be identified.

The policy and procedures must further address when senior management, including the Chief Executive Officer, will be notified. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

Containment

The policy and procedures shall require the prescribed organization to immediately initiate containment and shall identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for containment and the procedure that must be followed in this regard. In outlining the process to be followed, the policy and procedures shall set out

the documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation;; the employee(s) or other person(s) acting on behalf of the prescribed organization to which the notification must be provided; and the required content of the documentation.

In undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to ensure that additional information security beaches cannot occur through the same means.

The employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in reviewing the containment measures implemented and determining whether the information security breach has been effectively contained or whether further containment measures are necessary, must be identified in the policy and procedures. The policy and procedures shall also address any documentation that must be completed, provided and/or executed; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation;; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Notification

The policy and procedures must require the health information custodian that provided the personal health information to the prescribed organization for the purpose of developing or maintaining the electronic health record to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons.

The prescribed organization should not directly notify the individual to whom the personal health information relates of a security breach. The required notification shall be provided by the health information custodian. However, the policy and procedures must specify that the prescribed organization is required to assist health information custodians in fulfilling their obligations to notify individuals under the *Act* to the greatest extent possible, when requested to do so or directed by the Minister to do so.

In particular, the policy and procedures shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying the health information custodian, the format of the notification and the nature of the information that will be provided upon notification. At a minimum, the policy and procedures must require the health information custodian to be advised of the extent of the information security breach; the nature of the personal health information at issue, if any; the measures implemented to contain the information security breach; and further actions that will be undertaken with respect to the information security breach, including investigation and remediation.

The policy and procedures shall also set out whether any other persons or organizations must be notified of the information security breach and shall set out the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification. At a minimum, the policy and procedures must require the prescribed organization to notify the IPC, in writing, immediately after becoming aware that personal health information in the electronic health record:

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

Investigation and Recommendations

The policy and procedures must further identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for investigating the information security breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the information security breach. In outlining the process to be followed, the policy an procedures shall set out the documentation that must be completed, provided and/or executed in undertaking the investigation; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation. The role of the employee(s) or other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for assigning other employee(s) or other person(s) acting on behalf of the prescribed organization to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines.

The policy and procedures shall also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the information security breach; the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee(s) or other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the required content of the documentation.

Communication of Findings of Investigation and Recommendations

The policy and procedures must also address the manner and format in which the findings of the investigation of the information security breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This shall include a discussion of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer.

Tracking Information Security Breaches

The policy and procedures must require that a log be maintained of all information security breaches and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for maintaining the log and for tracking that the recommendations arising from the investigation of information security breaches are addressed within the identified timelines. They should further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of information security breaches will be retained and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Relationship to Policy and Procedures for Privacy Breach Management

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

Compliance, Audit and Enforcement

The prescribed organization must require employees or other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees or other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes that there may have been a breach of this policy or its associated procedures.

29. Log of Information Security Breaches

The prescribed organization shall maintain a log of information security breaches setting out:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- That the information security breach was caused by one or more health information custodians or an agent or electronic service provider of a health information and the name of each health information custodian and the name of each agent and electronic service provider of the health information custodian that caused the information security breach, if applicable;
- That the information security breach was caused by an employee(s) or other person(s) acting on behalf of the prescribed organization and the name of each employee and other person acting on behalf of the prescribed organization that caused the information security breach, if applicable;
- That the information security breach was caused by a system that retrieves, processes or integrates personal health information in the electronic health record created or maintained by the prescribed organization or the name of each system that caused the information security breach, if applicable;
- That an unauthorized person who is not an employee or other person acting on behalf of the prescribed organization and is not a health information custodian or an agent or electronic service provider of a health information custodian caused the information security breach and the name or a description of the unauthorized person, if applicable;
- The nature of the personal health information, if any, that was the subject matter of the information security breach and the nature and extent of the information security breach;
- The name of each health information custodian that provided the personal health information to the prescribed organization, if applicable;
- The date the health information custodian(s) that caused the information security breach was notified of the breach, if applicable;
- The date that the health information custodian that provided the personal health information to the prescribed organization was notified, if applicable;
- The name of any other organization or person that was notified and the date of notification, if applicable;
- The date that the information security breach was contained, the name of the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for containing the information security breach; and the nature of the containment measures;
- The date the investigation of the information security breach was commenced;
- The date that the investigation of the information security breach was completed;

- The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the investigation;
- The findings and recommendations arising from the investigation to remediate the information security breach and to prevent similar breaches in the future;
- The employee(s) or other person(s) acting on behalf of the prescribed organization responsible for addressing each recommendation;
- The manner in which each recommendation was or is expected to be addressed; and
- The status of the implementation of each recommendation.

Part 3 - Human Resources Documentation

1. Policy and Procedures for Privacy Training and Awareness

A policy and procedures must be developed and implemented requiring employees and other persons acting on behalf of the prescribed organization to attend initial privacy training as well as ongoing privacy training.

Timing and Method of Initial and Ongoing Privacy Training

The policy and procedures shall set out the time frame within which employees and other persons acting on behalf of the prescribed organization must complete the initial privacy training as well as address the frequency of ongoing privacy training. At a minimum, the policy and procedures shall require an employee or other person acting on behalf of the prescribed organization to complete the initial privacy training prior to viewing, handling or otherwise dealing with personal health information received for the purpose of developing or maintaining the electronic health record, including personal health information that has been de-identified and/or aggregated and to attend ongoing privacy training provided by the prescribed organization on an annual basis thereafter. The policy and procedures must also address the method(s) by which the initial and ongoing privacy training will be provided.

Process for Preparing the Content and Delivering Privacy Training

The policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for preparing the content of the initial and ongoing privacy training. The policy and procedures must also require the content of the initial and ongoing privacy training to be reviewed and updated on a regular basis and must set out the frequency with which the training will be reviewed and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for reviewing and updating the training. It is recommended that the initial and ongoing privacy training be reviewed and updated, if necessary, on an annual basis.

The policy and procedures shall further set out the process that must be followed in notifying the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for delivering the initial privacy training when an employee or other person acting on behalf of the prescribed organization has commenced or will commence an employment, contractual or other relationship with the prescribed organization. This shall include a discussion of the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

Content of Initial Privacy Training

The policy and procedures shall identify the content of the initial privacy training to ensure that it is formalized and standardized. At a minimum, the policy and procedures shall require that the initial privacy training include:

- A description of the prescribed organization's role pursuant to Part V.1 of the *Act* and the duties and responsibilities that arise as a result;

- A description of the purposes for which personal health information is provided to the prescribed organization by health information custodians;
- The purposes for which employees and any other person acting on behalf of the prescribed organization may view, handle, or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record;
- Limitations placed on the viewing, handling or otherwise dealing with personal health information by employees and other persons acting on behalf of the prescribed organization;
- Notice that all instances in which personal health information in the electronic health record is viewed, handled or otherwise dealt with by any person will be logged, audited and monitored;
- Limitations, conditions or restrictions placed on the personal health information, including a prohibition on viewing, handling or otherwise dealing with personal health information if other information such as de-identified and/or aggregate information, will serve the purpose of developing or maintaining the electronic health record and on viewing, handling or otherwise dealing with more of the personal health information that is necessary;
- A description of the procedure that must be followed in the event that an employee or other person acting on behalf of the prescribed organization is requested to apply a consent directive to personal health information in the electronic health record developed or maintained by the prescribed organization;
- A description of the procedure that must be followed in the event that an employee or other person acting on behalf of the prescribed organization is requested to provide personal health information to the Minister or another person as directed by the Minister;
- An overview of the privacy policies, procedures and practices that have been implemented by the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the privacy program;
- The administrative, technical and physical safeguards implemented by the prescribed organization to ensure that personal health information accessible by means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal;
- The duties and responsibilities of employees and other persons acting on behalf of the prescribed organization in implementing the administrative, technical and physical safeguards put in place by the prescribed organization;

- The purposes for which personal health information received by the prescribed organization for the purpose of developing or maintaining the electronic health record, which has been de-identified or aggregated, may be viewed, handled or otherwise dealt with by employees or other persons acting on behalf of the prescribed organization;
- A prohibition on using de-identified or aggregate information, either alone or with other information, to identify an individual;
- Notice that compliance with the prohibition on using de-identified or aggregated information to identify an individual will be audited an monitored;
- A discussion of the nature and purpose of the Privacy Notices, Confidentiality Agreements and End User Agreements that employees and other persons acting on behalf of the prescribed organization must execute and the key provisions of these notices and agreements; and
- An explanation of the *Policy and Procedures for Privacy Breach Management* and the duties and responsibilities imposed on employees and other persons acting on behalf of the prescribed organization in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches, including the duty to provide notice at the first reasonable opportunity of a privacy breach or suspected privacy breach.

Content of Ongoing Privacy Training

The policy and procedures shall also require the ongoing privacy training in respect of personal health information to be formalized and standardized and be based on evolving industry privacy standards and best practices. At a minimum, the policy and procedures shall require that ongoing privacy training:

- Include role-based training in order to ensure that employees and other persons acting on behalf of the prescribed organization understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities;
- Address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices;
- Take into account any:
    - recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints;
    - orders, decisions, guidelines, fact sheets and best practices issued by the IPC under the *Act* and its regulations; and
    - amendments to the *Act* and its regulations relevant to the prescribed organization.

Tracking, Auditing and Monitoring Privacy Training

The policy and procedures must require that a log be maintained to track attendance at the initial and ongoing privacy training and must identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial privacy training as well as the ongoing privacy training shall also be outlined. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed to verify attendance; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employee or other person acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for identifying employees and other persons acting on behalf of the prescribed organization who do not attend the initial or ongoing privacy training and for ensuring that such employees and other persons acting on behalf of the prescribed organization attend the initial and the ongoing privacy training, including the time frame following the date of the initial or ongoing privacy training within which this procedure must be implemented.

It is also recommended that the policy and procedures address where documentation related to attendance at the initial and the ongoing privacy training is to be retained and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Other Mechanisms to Foster a Privacy Culture

The policy and procedures shall also discuss the other mechanisms implemented by the prescribed organization to foster a culture of privacy and to raise awareness of the *Act*, the privacy program and the privacy policies, procedures and practices implemented. The policy and procedures shall also identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for fostering a culture of privacy and for raising privacy awareness as well as the frequency, method and nature of the communications that employees and other persons acting on behalf of the prescribed organization will receive in relation to privacy.

Relationship to Policy and Procedures for Security Training and Awareness

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*.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures*

*In Respect of Privacy Audit*s, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

2. Log of Attendance at Initial and Ongoing Privacy Training

The prescribed organization shall maintain a log of the attendance of employees and other persons acting on behalf of the prescribed organization at the initial and ongoing privacy training. At a minimum, the log must set out the name of the employee or other person acting on behalf of the prescribed organization, and for each such employee or person:

- The date that the employee or person acting on behalf of the prescribed organization commenced his or her employment, contractual or other relationship with the prescribed organization; and
- The date that the employee or other person acting on behalf of the prescribed organization attended the initial and ongoing privacy training.

3. Policy and Procedures for Security Training and Awareness

A policy and procedures must be developed and implemented requiring employees and other persons acting on behalf of the prescribed organization to attend initial and ongoing security training.

Timing and Method of Initial and Ongoing Security Training

The policy and procedures shall set out the time frame within which employees and other persons acting on behalf of the prescribed organization must complete the initial security training as well as address the frequency of ongoing security training. At a minimum, the policy and procedures shall require an employee or other person acting on behalf of the prescribed organization to complete the initial security training prior to viewing, handling, or otherwise dealing with personal health information received for the purpose of developing or maintaining the electronic health record, including personal health information that has been de-identified and/or aggregated and to attend ongoing security training provided by the prescribed organization on an annual basis thereafter. The policy and procedures must also address the method(s) by which the initial and ongoing security training will be provided.

Process for Preparing and Delivering Security Training

The policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for preparing and delivering the initial security training and ongoing security training. The policy and procedures must also require the content of the initial and ongoing security training to be reviewed and updated on a regular basis and must set out the frequency with which the training will be reviewed and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for reviewing and updating the training. It is recommended that the initial and ongoing security training be reviewed and updated, if necessary, on an annual basis.

The policy and procedures shall further set out the process that must be followed in notifying the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for delivering the initial security training when an employee or other person acting on behalf of the prescribed organization has commenced or will commence an employment, contractual or other relationship with the prescribed organization. This shall include a discussion of the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

Content of Initial Security Training

The policy and procedures shall also identify the content of the initial security training to ensure that it is formalized and standardized. At a minimum, the policy and procedures shall require that the initial security training include:

- An overview of the security policies, procedures and practices that have been implemented by the prescribed organization and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the security policies, procedures and practices implemented;
- An explanation of the security program, including the key activities of the program and the employee(s) and other person(s) acting on behalf of the prescribed organization that have been delegated day-to-day authority to manage the security program;
- The administrative, technical and physical safeguards implemented by the prescribed organization to ensure that personal health information accessible by means of the electronic health record is not collected without authority and is protected against theft, loss and unauthorized use or disclosure and that records of personal health information accessible by means of the electronic health record are protected against unauthorized copying, modification or disposal;
- The duties and responsibilities of employees and other persons acting on behalf of the prescribed organization in implementing the administrative, technical and physical safeguards put in place by the prescribed organization; and

- An explanation of the *Policy and Procedures for Information Security Breach Management* and the duties and responsibilities imposed on employees and other persons acting on behalf of the prescribed organization in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

Content of Ongoing Security Training

The policy and procedures shall also require the ongoing security training to be formalized and standardized and be based on evolving industry standards and best practices. At a minimum, the policy and procedures shall require that ongoing security training:

- Include role-based training in order to ensure that employees and other persons acting on behalf of the prescribed organization understand how to apply the security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities;
- Address any new security policies, procedures and practices and significant amendments to existing security policies, procedures and practices; and
- Take into account any:
    - recommendations with respect to security training made in security audits, privacy impact assessments and the investigation of information security breaches;
    - orders, decisions, guidelines, fact sheets and best practices issued by the IPC under the *Act* and its regulations; and
    - amendments to the *Act* and its regulations relevant to the Minister and the prescribed organization.

Tracking, Auditing and Monitoring Security Training

The policy and procedures must require that a log be maintained to track attendance at the initial security training as well as the ongoing security training and the policy and procedures must identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial security training as well as the ongoing security training shall also be outlined, including the documentation that must be completed, provided and/or executed to verify attendance; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation; the employee or other person acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for identifying employees and other persons acting on behalf of the prescribed organization who do not attend the initial or ongoing security training and for ensuring that such employees and other persons acting on behalf

of the prescribed organization attend the initial and ongoing security training, including the time frame following the date of the initial or ongoing security training within which this procedure must be implemented.

It is also recommended that the policy and procedures address where documentation related to attendance at the initial security training and the ongoing security training will be retained and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for retaining this documentation.

Other Mechanisms to Raise Security Awareness

The policy and procedures shall also discuss the other mechanisms implemented by the prescribed organization to raise awareness of the security program and the security policies, procedures and practices implemented. The policy and procedures shall also identify the employees and other persons acting on behalf of the prescribed organization responsible for raising security awareness as well as the frequency, method and nature of the communications that employees and other persons acting on behalf of the prescribed organization will receive in relation to information security.

Relationship to Policy and Procedures for Privacy Training and Awareness

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*.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

4. Log of Attendance at Initial and Ongoing Security Training

The prescribed organization shall maintain a log of the attendance of employees and other persons acting on behalf of the prescribed organization at the initial and ongoing security training. At a minimum, the log must set out the name of the employee or other person acting on behalf of the prescribed organization, and for each such employee or person,

- The date of commencement of his or her employment, contractual or other relationship with the prescribed organization; and
- The date that the employee or other person acting on behalf of the prescribed organization attended the initial and ongoing security training.

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

A policy and procedures must be developed and implemented requiring employees and other persons acting on behalf of the prescribed organization to execute a Confidentiality Agreement that contains the language from the *Template Confidentiality Agreement with Employees and Other Persons Acting on Behalf of the Prescribed Organization*.

Timing of Confidentiality Agreements

The policy and procedures shall set out the timeframe within which employees and other persons acting on behalf of the prescribed organization must execute the Confidentiality Agreement. At a minimum, the policy and procedures shall require these employees or other persons acting on behalf of the prescribed organization to execute a Confidentiality Agreement prior to viewing, handling or otherwise dealing with personal health information for the first time, including personal health information that has been de-identified and/or aggregated, and on an annual basis thereafter. The policy and procedures shall further identify the timeframe each year in which these employees or other persons acting on behalf of the prescribed organization are required to execute the Confidentiality Agreement on an ongoing basis.

Process for Executing Confidentiality Agreements

The policy and procedures must identify the employee(s) or other person(s) acting on behalf of the prescribed organization responsible and the process to be followed in ensuring that each employee or other person acting on behalf of the prescribed organization executes a Confidentiality Agreement in compliance with this policy and its procedures.

The policy and procedures shall set out the process that must be followed in notifying the responsible employee(s) or other person(s) acting on behalf of the prescribed organization each time an employee or other person acting on behalf of the prescribed organization has commenced or will commence an employment, contractual or other relationship with the prescribed organization. This shall include a discussion of the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

Tracking Execution of Confidentiality Agreements

The policy and procedures shall require that a log be maintained of all Confidentiality Agreements executed by employees and other persons acting on behalf of the prescribed organization. The policy and procedures must further identify the employee(s) or other persons acting on behalf of the prescribed organization responsible for maintaining the log and for tracking that Confidentiality Agreements have been executed.

The process to the followed in tracking that all employees or other persons acting on behalf of the prescribed organization have executed the Confidentiality Agreement shall also be outlined. In outlining the process to be followed, the policy and procedures shall set out the documentation that must be completed, provided and/or executed to verify that Confidentiality Agreements have been executed; the employees or other persons acting on behalf of the prescribed organization responsible for completing, providing, executing and ensuring the execution of the documentation; the employees or other persons acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall further set out the process to be followed and the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for identifying the employees or other persons acting on behalf of the prescribed organization who have not executed Confidentiality Agreements and for ensuring these employees or persons do so, including the timeframe within which the process must be implemented.

It is also recommended that the policy and procedures address where documentation related to the Confidentiality Agreements will be retained and the employees or other persons acting on behalf of the prescribed organization responsible for retaining this documentation.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance 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 employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

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

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

General Provisions

The Confidentiality Agreement must describe the status of the prescribed organization as defined in section 2 of the *Act* and the duties and responsibilities imposed on the prescribed organization pursuant to this status. It must also state that individuals executing the agreement are acting on behalf of the prescribed organization in respect of personal health information and must outline the responsibilities associated with this status. The Confidentiality Agreement must also provide a definition of personal health information and the definition provided must be consistent with the *Act* and its regulation.

Required Compliance

The Confidentiality Agreement must also require employees and other persons acting on behalf of the prescribed organization to comply with the provisions of the *Act* and its regulation relating to the role of the prescribed organization and with the terms of the Confidentiality Agreement as may be amended from time to time.

Employees and other persons acting on behalf of the prescribed organization 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 organization 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.

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

The Confidentiality Agreement shall identify the purposes for which employees and other persons acting on behalf of the prescribed organization are permitted to view, handle or otherwise deal with personal health information received for the purpose of developing or maintaining the electronic health record and any limitations, conditions or restrictions imposed thereon. In identifying these purposes, it must be ensured that each instance of viewing, handling or otherwise dealing with personal health information identified in the Confidentiality Agreement is permitted by the *Act* and its regulations and by the policies, procedures and practices put in place pursuant thereto.

In this regard, the Confidentiality Agreement must prohibit employees and other persons acting on behalf of the prescribed organization from viewing, handling or otherwise dealing with personal health information except as permitted in the Confidentiality Agreement.

The Confidentiality Agreement must also require employees and other persons acting on behalf of the prescribed organization to limit the personal health information received to that which is reasonably necessary for the purpose of developing or maintaining the electronic health record. Further, the Confidentiality Agreement must prohibit employees and other persons acting on behalf of the prescribed organization from viewing, handling or otherwise dealing with personal health information if other information will serve the purpose and from viewing, handling or otherwise dealing with more personal health information than is reasonably necessary to meet the purpose.

Obligations with Respect to De-Identified and Aggregate Information

The Confidentiality Agreement shall identify the purposes for which employees or other persons acting on behalf of the prescribed organization are permitted to use and disclose personal health information which has been de-identified or aggregated.

The Confidentiality Agreement must further prohibit employees and other persons acting on behalf of the prescribed organization from using the de-identified or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information, and attempting to identify an individual based on prior knowledge.

Termination of the Contractual, Employment or Other Relationship

The Confidentiality Agreement shall require employees and other persons acting on behalf of the prescribed organization to securely return all property of the prescribed organization, including records of personal health information, de-identified and aggregate information and all identification cards, access cards and/or keys, on or before the date of termination or cessation of the employment, contractual or other relationship in accordance with the *Policy and Procedures For Termination or Cessation of the Employment or Contractual Relationship*.

Notification

At a minimum, the Confidentiality Agreement shall require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization 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 employee or other person acting on behalf of the prescribed organization breaches or believes that there may have been a breach of the Confidentiality Agreement or if the employee or other person acting on behalf of the prescribed organization breaches or believes that there may have been a breach of the privacy or security policies, procedures and practices implemented by the prescribed organization.

Consequences of Breach and Monitoring Compliance

The Confidentiality Agreement must outline the consequences of breach of the agreement and must address the manner in which compliance with the Confidentiality Agreement will be enforced. The Confidentiality Agreement must further stipulate that compliance with the Confidentiality Agreement will be audited and must address the manner in which compliance will be audited.

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

A log of Confidentiality Agreements executed by employees and other persons acting on behalf of the prescribed organization must be maintained. At a minimum, the log must set out the name of the employee or other person acting on behalf of the prescribed organization, and for each such employee or person: the date of commencement of the employment, contractual or other relationship with the prescribed organization and the dates that the Confidentiality Agreement was executed.

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 organization must be developed.

The job description 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. The job description must also 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 employees and other persons acting on behalf of the prescribed organization are aware of the *Act* and its regulation and their duties thereunder;
- Ensuring employees and other persons acting on behalf of the prescribed organization are aware of the privacy policies, procedures and practices implemented by the prescribed organization and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial and ongoing privacy training and fostering a culture of privacy;
- Receiving and responding to requests to make, withdraw or modify a consent directive in relation to personal health information accessible by means of the electronic health record pursuant to the *Policy and Procedures for Managing Consent in the Electronic Health Record*;
- Receiving and responding to directions from the Minister for the provision of personal health information accessible by means of the electronic health record pursuant to the *Policy and Procedures for the Provision of Personal Health Information Pursuant to a Direction Issued by the Minister*;
- Receiving and responding to request for access and correction of records of personal health information accessible by means of the electronic health record pursuant to the *Policy and Procedures for Responding to Request for Access and Correction of Records of Personal Health Information*;
- Ensuring the electronic health record is audited and monitored pursuant to the *Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs*;
- Receiving and responding to requests from health information custodians and the Commissioner for the electronic records that the prescribed organization is required to maintain pursuant to the *Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs*;

- Conducting, reviewing and approving privacy impact assessments in accordance with the *Privacy Impact Assessment Policy and Procedures*;
- 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*.

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the 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 organization must be developed.

The job description 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. 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:

- Developing, implementing, reviewing and amending security policies, procedures and practices;
- Ensuring compliance with the security policies, procedures and practices implemented;
- Ensuring employees and other persons acting on behalf of the prescribed organization are aware of the security policies, procedures and practices implemented by the prescribed organization and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial and ongoing security training and fostering a culture of information security awareness;
- Maintenance and ongoing review of system control and audit logs pursuant to the *Policy and Procedures for Maintaining and Reviewing System Control and Audit Logs*;
- 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*.

10. Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

The policy and procedures shall require employees and other persons acting on behalf of the prescribed organization, as well as their supervisors, to notify the prescribed organization of the termination or cessation of the employment, contractual or other relationship. The policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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.

Secure Return of All Property

The policy and its procedures shall require employees and other persons acting on behalf of the prescribed organization to securely return all property of the prescribed organization 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 and procedures and this definition must, at a minimum, include records of personal health information, de-identified and aggregate information that has been derived from personal health information, identification cards, access cards and/or keys.

The policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing and executing the documentation; and the required content of the documentation.

The procedures to be followed in the event that the property of the prescribed organization is not securely returned upon termination or cessation of the employment, contractual or other relationship shall also be addressed, including the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for implementing the procedure and the time frame following termination or cessation within which the procedure must be implemented.

Terminating Access to Premises and Operational Environments

The policy and procedures shall also require that access to the premises of the prescribed organization, 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 termination or cessation of the employment, contractual or other relationship.

The policy and procedures must identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation.

Compliance, Audit and Enforcement

The prescribed organization shall require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization 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 employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

11. Policy and Procedures for Discipline and Corrective Action

The prescribed organization shall develop and implement a policy and associated procedures for discipline and corrective action in respect of personal health information.

The policy and procedures shall address the investigation of disciplinary matters, including the employee(s) or other person(s) acting on behalf of the prescribed organization responsible for conducting the investigation; the procedure that must be followed in undertaking the investigation; any documentation that must be completed, provided and/or executed in undertaking the investigation; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing and executing the documentation; the required content of the documentation; and the employee(s) and other person(s) acting on behalf of the prescribed organization to whom the results of the investigation must be reported.

The types of discipline that may be imposed by the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the employee(s) and other person(s) acting on behalf of the prescribed organization that must be consulted in making this determination; and the documentation that must be completed, provided and/or executed, shall also be identified.

It is also 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for retaining the documentation.

Part 4 - Organizational and Other Documentation

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 organization must be established.

Accountability for Compliance

The privacy governance and accountability framework must stipulate that the Chief Executive Officer is ultimately accountable for ensuring that the prescribed organization and its employees and other persons acting on behalf of the prescribed organization comply with the *Act* and its regulation and comply with the privacy policies, procedures and practices implemented.

Individuals, Committees and Teams that Support the Privacy Program

The position(s) that have been delegated day-to-day authority to manage the privacy program must be identified in the privacy governance and accountability framework and the nature of the reporting relationship to the Chief Executive Officer must be described. The privacy governance and accountability framework shall also 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.

It is also recommended that the privacy governance and accountability framework be accompanied by a privacy governance organizational chart.

Updates of Board of Directors

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, must also be addressed. The privacy governance and accountability framework shall also 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated. At a minimum, it is recommended that the Board of Directors be updated on an annual basis, preferably in the form of a written report.

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.

Communication of Security Governance and Accountability Framework

The privacy governance and accountability framework shall also set out the manner in which the privacy governance and accountability framework will be communicated to employees and other persons acting on behalf of the prescribed organization, the method by which it will be communicated and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for this communication.

Relationship to Security Governance and Accountability Framework

This governance and accountability framework may either be a stand-alone document or may be combined with the *Security Governance and Accountability Framework*.

2. 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 organization must be established.

Accountability for Compliance

The security governance and accountability framework must stipulate that the Chief Executive Officer is ultimately accountable for ensuring the security of personal health information and for ensuring that the prescribed organization and its employees and other persons acting on behalf of the prescribed organization comply with the security policies, procedures and practices implemented.

Individuals, Committees and Teams that Support the Security Program

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 must be described. The security governance and accountability framework shall also 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.

It is also recommended that the security governance and accountability framework be accompanied by a security governance organizational chart.

Updates of Board of Directors

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, must also be addressed.

The security governance and accountability framework shall also 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing such updates and the matters with respect to which the Board of Directors is required to be updated. At a minimum, it is recommended that the Board of Directors be updated on an annual basis, preferably in the form of a written report.

The update provided to the Board of Directors must address the initiatives undertaken by the security program including security training and the development and implementation of security policies, procedures and practices. It shall also 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. The 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.

Communication of Security Governance and Accountability Framework

The security governance and accountability framework shall also set out the manner in which the security governance and accountability framework will be communicated to employees and other persons acting on behalf of the prescribed organization, the method by which it will be communicated and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for this communication.

Relationship to Privacy Governance and Accountability Framework

This governance and accountability framework may either be a stand-alone document or may be combined with the *Privacy Governance and Accountability Framework*.

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

The prescribed organization 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. The terms of reference shall also set out to whom the committee reports; the types of reports produced by the committee, if any; the format of the reports; to whom these reports are presented; and the frequency of these reports.

4. Corporate Risk Management Framework

The prescribed organization 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 for the purpose of developing or maintaining the electronic health record and to maintain the confidentiality of that information.

Risk Identification

The corporate risk management framework must address the employee(s) and other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in identifying risks that may negatively affect the ability of the prescribed organization to protect the privacy of individuals whose personal health information is received for the purpose of developing or maintaining the electronic health record and to maintain the confidentiality of that information. This shall include a discussion of the employee(s) and other person(s) acting on behalf of the prescribed organization or other persons or organizations that must be consulted in identifying the risks; the documentation that must be completed, provided and/or executed; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation; the employee(s) and other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Risk Assessment

The risk management framework must address the employee(s) and other person(s) acting on behalf of the prescribed organization responsible, the process that must be followed and the criteria that must be considered in ranking the identified risks and assessing the likelihood of the risks occurring and the potential impact if they occur. In outlining the process to be followed, the risk management framework shall:

- Set out the employee(s) and other person(s) acting on behalf of the prescribed organization or other persons or organizations that must be consulted in assessing and ranking the risks;
- Require these employee(s) and other person(s) acting on behalf of the prescribed organization and other persons or organizations to document the rationale for the assessment and ranking of the risks and identify the employee(s) or other persons acting on behalf of the prescribed organization to whom the documentation must be provided; and
- Identify the documentation that must be completed, provided and/or executed in assessing and ranking the risks, including;
    - the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation;
    - the employee(s) and other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and
    - the required content of the documentation.

Risk Mitigation

The corporate risk management framework must identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

In outlining the process to be followed and the criteria to be considered, the policy and procedures shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for assigning other employees and other persons acting on behalf of the prescribed organization 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.

The corporate risk management framework must further address the documentation that must be completed, provided and/or executed in identifying, implementing, monitoring and ensuring the implementation of the mitigation strategies; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation; the employee(s) and other person(s) acting on behalf of the prescribed organization to whom this documentation must be provided; and the required content of the documentation.

Risk Communication and Reporting

The corporate risk management framework must 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. This involves identifying the employee(s) and other person(s) acting on behalf of the prescribed organization 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. Approval and endorsement of the results of the risk management process, including the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for approval and endorsement, shall also be outlined.

Risk Register

The corporate risk management framework 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 organization to protect the privacy of individuals whose personal health information is received for the purpose of developing or maintaining the electronic health record and to maintain the confidentiality of that information continue to be identified, assessed and mitigated.

The frequency with which the corporate risk register must be reviewed and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible and the process that must be followed in reviewing and amending the corporate risk register must also be identified.

Integration of Risk Management Framewor

The manner in which the corporate risk management framework will be integrated into the policies, procedures and practices of the prescribed organization and into the projects undertaken by the prescribed organization and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for integration shall also be addressed.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits* 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization 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 employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

5. Corporate Risk Register

The prescribed organization must develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the prescribed organization to protect the privacy of individuals whose personal health information is received for the purpose of developing or maintain the electronic health record 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for implementation of the mitigation strategy.

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

The prescribed organization 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. The consolidated and centralized log shall also be required to include recommendations made by the IPC that must be addressed by the prescribed organization prior to the next review of its practices and procedures.

The policy and procedures shall also set out the frequency with which and the circumstances in which the consolidated and centralized log must be reviewed, the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for reviewing and amending the log and the process that must be followed in this regard. At a minimum, it is 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 IPC is completed and each time that a recommendation has been addressed. It is also 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 prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits* 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization 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 employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

7. Consolidated Log of Recommendations

The prescribed organization 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 IPC.

In particular, the log must set out the name and date of the document, investigation, audit and/or review from which the recommendation 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for addressing the recommendation.

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 organization in the event of short and long-term business interruptions and in the event of threats to the operating capabilities of the prescribed organization, including natural, human, environmental and technical interruptions and threats.

The business continuity and disaster recovery plan 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.

Notification of Interruption or Threat

The business continuity and disaster recovery plan shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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 organization and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for providing such notification.

The business continuity and disaster recovery plan must also 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. In this regard, a contact list must be required to be developed and maintained of all health information custodians, employees and other persons acting on behalf of the prescribed organization, 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for developing and maintaining this contact list.

Assessment of Interruption or Threat

The business continuity and disaster recovery plan shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for the assessment, the criteria pursuant to which this assessment is to be made and the employee(s) and other

person(s) acting on behalf of the prescribed organization and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat. It must also 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 employee(s) and other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and to whom the results of this assessment must be reported.

In relation to the assessment of the interruption or threat, the business continuity and disaster recovery plan shall set out the employee(s) and other person(s) acting on behalf of the prescribed organization 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 organization. In outlining the process to be followed, the business continuity and disaster recovery plan shall identify the:

- Employee(s) and other person(s) acting on behalf of the prescribed organization 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 utilized in conducting assessment;
- Documentation that must be completed, provided and/or executed;
- Employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation;
- Employee(s) and other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and
- Employee(s) and other person(s) acting on behalf of the prescribed organization to whom the results of the initial impact assessment must be communicated.

The business continuity and disaster recovery plan must further identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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. It must further address the manner in which the assessment is required to be conducted; the employee(s) and other person(s) acting on behalf of the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation; the employee(s) and other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the employee(s) and other person(s) acting on behalf of the prescribed organization to whom the results of the assessment must be communicated.

Resumption and Recovery Following the Interruption or Threat

The business continuity and disaster recovery plan shall also identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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.

In outlining the process to be followed, the business continuity and disaster recovery plan shall identify the employee(s) and other person(s) acting on behalf of the prescribed organization 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for completing, providing, executing and/or ensuring the execution of the documentation; the employee(s) and other person(s) acting on behalf of the prescribed organization to whom the documentation must be provided; and the employee(s) and other person(s) acting on behalf of the prescribed organization to whom the results of these activities must be communicated.

Documenting Interruptions and Threats

The business continuity and disaster recovery plan must set out the procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of the prescribed organization will be documented and communicated and by whom and to whom they will be communicated.

Inventory of Critical Applications, Business Functions, Hardware and Software

The business continuity and disaster recovery plan must require that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licenses, 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 further identify the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for developing and maintaining the inventory, the employee(s) and other person(s) acting on behalf of the prescribed organization 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.

Testing, Maintenance and Assessment of Business Continuity and Disaster Recovery Plan

The business continuity and disaster recovery plan must also address the testing, maintenance and assessment of the business continuity and disaster recovery plan. This includes identifying the frequency of testing; the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for ensuring that the business continuity and disaster recovery plan is tested, maintained and assessed; the employee(s) and other person(s) acting on behalf of the prescribed organization 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 disaster recovery plan; and the employee(s) and other person(s) acting on behalf of the prescribed organization responsible for approving the business continuity and disaster recovery plan and any amendments thereto.

Communication of Business Continuity and Disaster Recovery Plan

The business continuity and disaster recovery plan must further address the employee(s) and other person(s) acting on behalf of the prescribed organization responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all employees and other persons acting on behalf of the prescribed organization, including any amendments thereto, and the method and nature of the communication. The employee(s) and other person(s) acting on behalf of the prescribed organization responsible for managing communications in relation to the threat or interruption shall also be identified, including the method and nature of the communication.

Compliance, Audit and Enforcement

The prescribed organization must require employees and other persons acting on behalf of the prescribed organization to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits* 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 employee(s) and other person(s) acting on behalf of the prescribed organization responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

Notification of Breach

The policy and procedures must also require employees and other persons acting on behalf of the prescribed organization to notify the prescribed organization 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 employee or other person acting on behalf of the prescribed organization breaches or believes there may have been a breach of this policy or its procedures.

Appendix "C"
Privacy, Security and Other Indicators

Part 1 - Privacy Indicators

Categories	Privacy Indicators
General Privacy Policies, Procedures and Practices	• The dates that the privacy policies and procedures were reviewed by the prescribed organization since the prior review by the IPC. • Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made. • Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented. • The date that each amended and newly developed privacy policy and procedure was communicated to employees or other persons acting on behalf of the prescribed organization and, for each amended and newly developed privacy policy and procedure communicated to employees or other persons acting on behalf of the prescribed organization, the nature of the communication. • Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.
Receiving Personal Health Information	• The number of repositories of personal health information that are accessible by means of the electronic health record. • The number of descriptions of types of personal health information received by the prescribed organization for the purpose of creating or maintaining the electronic health record. • The number of descriptions of types of personal health information received by the prescribed organization for the purpose of creating or maintaining the electronic health record that were reviewed since the prior review by the IPC. • Whether amendments were made to existing descriptions of types of personal health information as a result of the review, and if so, for each description amended, a brief explanation of the amendments made.

Categories	Privacy Indicators
Managing Consent in the Electronic Health Record	• The number of instances in which a consent directive has been made, modified or withdrawn since the prior review by the IPC. • The number of instances in which a notice of a consent directive has been provided to a health information custodian in accordance with subsection 55.6 (7) of the *Act* since the prior review by the IPC. • The number of instances in which a health information custodian has overridden a consent directive pursuant to section 55.7 of the *Act* since the prior review by the IPC and the number of occasions on which each of subsection 55.7(1), (2) or (3) of the *Act* was invoked to override the consent directive. • The number of instances in which a notice of a consent override has been provided to a health information custodian in accordance with subsection 55.7(6) of the *Act* since the prior review by the IPC. • The dates on which reports of consent overrides were made to the IPC pursuant to paragraph 16 of section 55.3 of the *Act* since the prior review by the IPC. • The number of requests received from health information custodians pursuant to paragraph 9 of section 55.3 of the *Act* for the electronic records of consent directives and consent overrides since the prior review by the IPC. • The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records of consent directives and consent overrides since the prior review by the IPC.
Viewing, Handling or Otherwise Dealing with Personal Health Information	• The number of employees or other persons acting on behalf of the prescribed organization granted approval to view, handle or otherwise deal with personal health information.

Categories	Privacy Indicators
Provision of Personal Health Information Pursuant to Direction	• The number of directions issued by a member of a data integration unit of the Minister pursuant to subsection 55.9(3) of the Act requiring the prescribed organization to provide to the member of the data integration unit personal health information that is accessible by means of the electronic health record since the prior review by the IPC. • The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a person for the purposes of subsection 55.10(1) of the *Act* since the prior review by the IPC. • The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a prescribed person for the purposes of clause 39(1)(c) of the *Act* since the prior review by the IPC. • The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a person for the purposes of subsection 39(2) of the *Act* since the prior review by the IPC. • The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a researcher for the purposes of section 44 of the *Act* since the prior review by the IPC. • The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a prescribed entity for the purposes of section 45 of the *Act* since the prior review by the IPC.

Categories	Privacy Indicators
Access and Correction	• The number of requests made by individuals to access records of personal health information that are accessible by means of the electronic health record since the prior review by the IPC. • The number of requests made by individuals to correct records of personal health information that are accessible by means of the electronic health record since the prior review by the IPC. • The number of refusals under the *Act* of a request for access to a record, the provisions of the *Act* under which access was refused and the number of occasions on which each provision was invoked. • The number of refusals under the *Act* of a request to correct a record, the provisions of the *Act* under which the correction was refused and the number of occasions on which each provision was invoked. • The amount of fees collected by the prescribed organization under subsection 54 (10) of the *Act*, if any.
Agreements with Third Party Service Providers	• The number of agreements executed with third party service providers with access to personal health information since the prior review by the IPC.
Privacy Impact Assessments	• The number and a list of privacy impact assessments completed since the prior review by the IPC and for each privacy impact assessment: - A description of the existing or proposed system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record or the types of personal health information that will be provided to the prescribed entity for the purpose of developing or maintaining the electronic health record, as the case may be; - For each system that retrieves or will retrieve, process or integrate personal health information, a description of the types of personal health information that is or will be retrieved, processed or integrated; - The date of completion of the privacy impact assessment; - A brief description of each recommendation; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.

Categories	Privacy Indicators
Privacy Impact Assessments (cont'd)	• The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC and the proposed date of completion. • The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion. • The number of determinations made since the prior review by the IPC that a privacy impact assessment is not required and, for each determination, the existing or proposed system that retrieves, processes or integrates personal health information, and a description of the types of personal health information that is or will be retrieved, processed or integrated that is at issue, and a brief description of the reasons for the determination. • The number and a list of privacy impact assessments reviewed since the prior review by the IPC and a brief description of any amendments made.
Privacy Audit Program	• For the electronic records the prescribed organization is required to keep pursuant to paragraphs 5 and 6 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3, since the prior review by the IPC: - The number of audits conducted or the frequency with which the audits have been conducted; - The nature and scope of each audit conducted; - The date of completion of the audit; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed. • The dates of audits of employees and other persons acting on behalf of the prescribed organization granted approval to view, handle or otherwise deal with personal health information since the prior review by the IPC and for each audit conducted: - The date of completion of the audit; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.

Categories	Privacy Indicators
Privacy Audit Program (Cont'd)	• The number and a list of audits completed to assess compliance with the privacy policies, procedures and practices put in place by the prescribed organization completed since the prior review by the IPC and for each audit: - The date of completion of the audit; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed. • The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: - A description of the nature and type of audit conducted; - The date of completion of the audit; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.
Privacy Breaches	• The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed organization since the prior review by the IPC. • The number of privacy breaches identified by the prescribed organization since the prior review by the IPC. • The number of privacy breaches caused by one or more health information custodians. • The number of privacy breaches caused by the prescribed organization or a system that retrieves, processes or integrates personal health information in the electronic health record. • The number of privacy breaches caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian.

Categories	Privacy Indicators
Privacy Breaches (Cont'd)	• With respect to each privacy breach caused by the prescribed organization; a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; or a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian since the prior review by the IPC: - Whether the privacy breach or suspected privacy breach was caused by the prescribed organization; - Whether the privacy breach or suspected privacy breach was caused by a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; - Whether the privacy breach or suspected privacy breach was caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian; - The nature and scope of the privacy breach; - The cause of the privacy breach; - The date that senior management of the prescribed organization was notified; - The containment measures implemented; - The date(s) that the containment measures were implemented; - The date(s) that notification was provided to the health information custodians or any other organizations; - The date that the investigation was commenced; - The date that the investigation was completed; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.

Categories	Privacy Indicators
Privacy Complaints	• The number of privacy complaints received since the prior review by the IPC. • Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each privacy complaint investigated: - The date that the privacy complaint was received; - The nature of the privacy complaint; - The date that the investigation was commenced; - The date of the written communication to the individual who made the privacy complaint in relation to the commencement of the investigation; - The date that the investigation was completed; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; - The manner in which each recommendation was addressed or is proposed to be addressed; and - The date of the written communication to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint. • Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each privacy complaint not investigated: - The date that the privacy complaint was received; - The nature of the privacy complaint; and - The date of the written communication to the individual who made the privacy complaint and a brief description of the content of the letter.

Part 2 - Security Indicators

Categories	Security Indicators
General Security Policies and Procedures	• The dates that the security policies and procedures were reviewed by the prescribed organization since the prior review by the IPC. • Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made. • Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented. • The dates that each amended and newly developed security policy and procedure was communicated to employees and other persons acting on behalf of the prescribed organization and, for each amended and newly developed security policy and procedure communicated to employees and other persons acting on behalf of the prescribed organization, the nature of the communication. • Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.
Physical Security	• The dates of audits of employees and other persons acting on behalf of the prescribed organization granted approved to access the premises and locations within the premises where records of personal health information are retained since the prior review by the IPC and for each audit: - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.
Acceptable Use Agreements	- The number of Acceptable Use Agreements acknowledged and agreed to by employees or other persons acting on behalf of the prescribed organization since the prior review by the IPC.
End User Agreements	- The number of End User Agreements acknowledged and agreed to by end users who provide personal health information to or collect personal health information by means of the electronic health record.

Categories	Security Indicators
Security Audit Program	• The number of requests received from health information custodians pursuant to paragraph 9 of section 55.3 for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the *Act*, since the prior review by the IPC. • The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the *Act*, since the prior review by the IPC. • For the electronic records the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3 of the *Act*, since the prior review by the IPC: - The number of audits conducted or the frequency with which the audits have been conducted; - The nature and scope of each audit conducted; - The date of completion of the audit; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed. • The dates of the review of all other system control and audit logs since the prior review by the IPC and a general description of the findings, if any, arising from the review of system control and audit logs. • The number and a list of all other security audits completed since the prior review by the IPC and for each audit: - A description of the nature and type of audit conducted; - The date of completion of the audit; - A brief description of each recommendation made; - The date that each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is expected to be addressed.

Categories	Security Indicators
Threat and Risk Assessments	• The date of all threat and risk assessments that have been completed since the prior review by the IPC and for each threat and risk assessment: - The system that is at issue; - The date the threat and risk assessment was completed or is expected to be completed; - A brief description of the recommendations arising from the threat and risk assessment; - The date each recommendation was or is expected to be addressed; and - The manner in which each recommendation was or is expected to be addressed.
Information Security Breaches	• The number of notifications of security breaches or suspected security breaches received by the prescribed organization since the prior review by the IPC. • The number of security breaches identified since the prior review by the IPC. • The number of security breaches caused by one or more health information custodians. • The number of security breaches caused by the prescribed organization or a system that retrieves, processes or integrates personal health information in the electronic health record. • The number of security breaches caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian. • With respect to each security breach or suspected security breach caused by the prescribed organization; a system that retrieves, processes or integrates personal health information in the electronic health record; or a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian since the prior review by the IPC: - Whether the security breach or suspected security breach was caused by the prescribed organization; - Whether the security breach or suspected information security breach was caused by a system that retrieves, processes or integrates personal health information in the electronic health record;

Categories	Security Indicators
Information Security Breaches (Cont'd)	- Whether the security breach or suspected security breach was caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian; - The nature and scope of the security breach; - The cause of the security breach; - The date that senior management of the prescribed organization was notified; - The containment measures implemented; - The date(s) that the containment measures were implemented; - The date(s) that notification was provided to the health information custodians or any other organizations; - The date that the investigation was commenced; - The date that the investigation was completed; - A brief description of each recommendation made; - The date each recommendation was addressed or is proposed to be addressed; and - The manner in which each recommendation was addressed or is proposed to be addressed.

Part 3 - Human Resources Indicators

Categories	Human Resources Indicators
Privacy Training and Awareness	• The number of employees or other persons acting on behalf of the prescribed organization who have received and who have not received initial privacy training since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for employees or other persons acting on behalf of the prescribed organization who have yet to receive initial privacy training and the scheduled date of the initial privacy training. • The number of employees or other persons acting on behalf of the prescribed organization who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC. • The dates and number of communications to agents by the prescribed organization in relation to privacy since the prior review by the IPC and a brief description of each communication.
Security Training and Awareness	• The number of employees or other persons acting on behalf of the prescribed organization who have received and who have not received initial security training since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for employees or other persons acting on behalf of the prescribed organization who have yet to receive initial security training and the scheduled date of the initial security training. • The number of employees or other persons acting on behalf of the prescribed organization who have attended and who have not attended ongoing security training each year since the prior review by the IPC. • The dates and number of communications to agents by the prescribed organization in relation to information security since the prior review by the IPC and a brief description of each communication.
Confidentiality Agreements	• The number of employees or other persons acting on behalf of the prescribed organization who have executed and who have not executed Confidentiality Agreements each year since the prior review by the IPC. • The date of commencement of the employment, contractual or other relationship for employees or other persons acting on behalf of the prescribed organization who have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.

Categories	Human Resources Indicators
Termination or Cessation	• The number of notifications received from employees or other persons acting on behalf of the prescribed organization since the prior review by the IPC related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.

Part 4 - Organizational Indicators

Categories	Organizational Indicators
Risk Management	• The dates that the corporate risk register was reviewed by the prescribed organization since the prior review by the IPC. • Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.
Business Continuity and Disaster Recovery	• The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC. • Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.

Appendix "D"
Sworn Affidavit

I, [INSERT NAME], of the City of [INSERT CITY NAME], in the province of Ontario,
MAKE OATH AND SAY:

1. I am [INSERT POSITION TITLE] at [INSERT NAME OF PRESCRIBED ORGANIZATION] and, as such, have knowledge of the matters to which I hereinafter depose, except where such knowledge is based on information and belief, in which case I have stated the source of the information and believe the information to be true.

2. [INSERT NAME OF PRESCRIBED ORGANIZATION] has in place policies, procedures and practices to protect the privacy of individuals whose personal health information it receives for the purpose of developing and maintaining the electronic health record and to maintain the confidentiality of that information.

3. The policies, procedures and practices implemented by [INSERT NAME OF PRESCRIBED ORGANIZATION] comply with the *Manual for the Review and Approval of Prescribed Organizations* that has been published by the Information and Privacy Commissioner of Ontario, as it may be amended from time to time.

4. [INSERT NAME OF PRESCRIBED ORGANIZATION] has submitted a written report to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Organizations*.

5. [INSERT NAME OF PRESCRIBED ORGANIZATION] has taken steps that are reasonable in the circumstances to ensure compliance with the policies, procedures and practices implemented and to ensure that the personal health information received for the purpose of developing and maintained the electronic health record is protected against theft, loss and collection, use or disclosure without authority and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME)
)
at the City/Town/Etc. of _____, in the)
)
County/Regional Municipality/Etc. of)
)
_____, on _____ 20 ____.)

_____
[SIGNATURE OF DEPONENT]

_____
Commissioner for Taking Affidavits

Manual for the Review and Approval of Prescribed Organizations

Information and Privacy
Commissioner of Ontario

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

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

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

October 2021