# MANUAL FOR THE REVIEW AND APPROVAL OF PRESCRIBED PERSONS AND PRESCRIBED ENTITIES

# Table of Contents

# PROCESS FOR THE REVIEW AND APPROVAL OF PRESCRIBED PERSONS AND PRESCRIBED ENTITIES

The *Personal Health Information Protection Act, 2004* ("the *Act*") is a consent-based statute, meaning that persons or organizations in the health sector defined as "health information custodians"[1] may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances pursuant to subsection 39(1)(c) of the *Act*.[2] Another such disclosure that is permitted without consent is the disclosure of personal health information to prescribed entities for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system pursuant to section 45 of the *Act*.[3]

These disclosures are permitted without consent provided that the prescribed persons and prescribed entities comply with the requirements set out in the *Act* and Regulation 329/04 to the *Act* ("regulation").

## Requirements for Disclosure to Prescribed Persons and Prescribed Entities

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person or prescribed entity without consent, the prescribed person or prescribed entity must have in place practices and procedures approved by the Information and Privacy Commissioner of Ontario to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. In the case of a prescribed person, this requirement is set out in subsection 13(2) of the regulation to the *Act*. In the case of a prescribed entity, this requirement is set out in subsection 45(3) of the *Act*.

These practices and procedures must also be reviewed by the Information and Privacy Commissioner of Ontario every three years from the date of their initial approval in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person or prescribed entity without consent and in order for the prescribed person or prescribed entity to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act* and the regulation to the *Act*. In the case of a prescribed

[1] Persons or organizations described in subsection 3(1) of the *Act* that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

[2] Persons prescribed for purposes of subsection 39(1)(c) of the *Act* are set out in subsection 13(1) of Regulation 329/04 to the *Act*.

[3] Entities prescribed for purposes of section 45 of the *Act* are set out in subsection 18(1) of Regulation 329/04 to the *Act*.

person, this requirement is set out in subsection 13(2) of the regulation to the *Act*. In the case of a prescribed entity, this requirement is set out in subsection 45(4) of the *Act*.

## Previous Review Process for Prescribed Persons and Prescribed Entities

This section describes the previous process that was followed by the Information and Privacy Commissioner of Ontario in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

Each prescribed person and prescribed entity was requested to provide the Information and Privacy Commissioner of Ontario with documentation describing the practices and procedures implemented to protect the privacy of individuals whose personal health information it received and to maintain the confidentiality of that information. The request was made by the Information and Privacy Commissioner of Ontario approximately one year prior to the date that the approval was required pursuant to the *Act* or one year prior to the date that the prescribed person or prescribed entity required approval.

Upon receipt, the Information and Privacy Commissioner of Ontario reviewed the documentation describing the practices and procedures implemented by the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. Additional documentation and clarifications were then requested if deemed necessary by the Information and Privacy Commissioner of Ontario.

Once any additional documentation and necessary clarifications were received, an on-site meeting was held between the Information and Privacy Commissioner of Ontario and representatives of the prescribed person or prescribed entity. The purpose of the on-site meeting was to discuss the practices and procedures implemented by the prescribed person or prescribed entity, to provide the Information and Privacy Commissioner of Ontario with an opportunity to ask questions arising from the review of the practices and procedures implemented, and to provide the Information and Privacy Commissioner of Ontario with an opportunity to review the physical security measures put in place to protect personal health information.

Following the on-site meeting, each prescribed person and prescribed entity was informed of the actions that were required to be taken by the prescribed person or prescribed entity prior to the approval or continued approval of its practices and procedures. Once all necessary actions were taken, the Information and Privacy Commissioner of Ontario prepared a draft report that was submitted to the prescribed person or prescribed entity, as the case may be, for review and comment prior to the report being finalized. Once the report was finalized, it was posted on the website of the Information and Privacy Commissioner of Ontario, along with a letter of approval.

## Purpose of this Manual

The purpose of the *Manual For The Review and Approval of Prescribed Persons and Prescribed Entities* ("the Manual") is to outline the new process that will be followed by the Information and Privacy Commissioner of Ontario, commencing on January 31, 2010, in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information. The purpose of the Manual is also to set out the obligations imposed on prescribed persons and prescribed entities arising from the new review process.

The Manual may be amended from time to time by the Information and Privacy Commissioner of Ontario. It is the responsibility of the prescribed persons and prescribed entities to ensure continued compliance with the Manual as amended from time to time.

## New Review Process for Prescribed Persons and Prescribed Entities

A new process will be followed by the Information and Privacy Commissioner of Ontario in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information, commencing on January 31, 2010.

Each prescribed person and prescribed entity will continue to be required to have in place practices and procedures to protect the privacy of individuals whose personal health information is received 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 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 persons and prescribed entities, the amount and sensitivity of the personal health information collected and the number and nature of the individuals with access to the personal health information.

The process that will be followed by the Information and Privacy Commissioner of Ontario in conducting its review will depend on whether the review relates to the initial review of the practices and procedures implemented by the prescribed person or prescribed entity or relates to the ongoing review of these practices and procedures, which is conducted every three years from the date of the initial approval by the Information and Privacy Commissioner of Ontario.

### *Initial Review of the Prescribed Persons and Prescribed Entities*

Each prescribed person and prescribed entity seeking the initial approval of the Information and Privacy Commissioner of Ontario in respect of the practices and procedures implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, must submit the applicable practices and procedures

described in Appendix "A" and containing the minimum content set out in Appendix "B" to the Manual, to the Information and Privacy Commissioner of Ontario. These practices and procedures must be submitted six months prior to the date that the approval of the Information and Privacy Commissioner of Ontario is requested.

Upon receipt, the Information and Privacy Commissioner of Ontario will review the practices and procedures implemented by the prescribed person or prescribed entity 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 Information and Privacy Commissioner of Ontario and representatives of the prescribed person or prescribed entity. The purpose of the on-site meeting is to discuss the practices and procedures implemented by the prescribed person or prescribed entity, to provide the Information and Privacy Commissioner of Ontario with an opportunity to ask questions arising from the review of the practices and procedures implemented, and to provide the Information and Privacy Commissioner of Ontario with an opportunity to review the physical security measures put in place to protect personal health information.

Following the on-site meeting, the prescribed person or prescribed entity will be informed of the actions that are required to be taken by the prescribed person or prescribed entity prior to the approval of its practices and procedures. Once all necessary actions have been taken, the Information and Privacy Commissioner of Ontario will prepare a draft report and submit the draft report to the prescribed person or prescribed entity, as the case may be, for review and comment prior to the report being finalized. Once the report is finalized it will be posted on the website of the Information and Privacy Commissioner of Ontario, 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 person or prescribed entity.

A person or organization may not operate as a prescribed person or prescribed entity unless it has submitted its practices and procedures to the Information and Privacy Commissioner of Ontario and the Information and Privacy Commissioner of Ontario 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 Persons and Prescribed Entities*

Each prescribed person and prescribed entity seeking the continued approval of the practices and procedures it has implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, which is required every three years from the date of the initial approval, must submit a detailed written report and sworn affidavit to the Information and Privacy Commissioner of Ontario one year prior to the date that the continued approval is required pursuant to the *Act* or its regulation.

The written report must demonstrate that the prescribed person or prescribed entity has developed and implemented practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the practices and procedures set out in Appendix "A," and is adhering to these

practices and procedures. It must also demonstrate that these practices and procedures, at a minimum, contain the content set out in Appendix "B" to this Manual.

If compliance with the requirements in Appendix "A" or Appendix "B" has not been achieved, the written report 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 person or prescribed entity, there is a clear rationale for not complying with one or more of the requirements in Appendix "A" or Appendix "B," this must be identified in the written report. The written report must also provide detailed information in support of this opinion. For example, if a prescribed person or prescribed entity does not use personal health information for research purposes, the prescribed person or prescribed entity would not be required to implement policies and procedures with respect to the use of personal health information for research purposes or a log of approved uses of personal health information for research purposes.

The written report must also report on, provide information concerning and assess the performance of the prescribed person or prescribed entity with respect to each of the privacy, security and other indicators set out in Appendix "C" to this Manual.

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 person or prescribed entity 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 person or prescribed entity comply with the *Act* and its regulation and with the requirements in this Manual and that the prescribed person or prescribed entity has taken steps that are reasonable in the circumstances to ensure compliance with the practices and procedures that it has implemented.

Upon receipt, the Information and Privacy Commissioner of Ontario will review the written report and accompanying sworn affidavit and decide, in its sole and absolute discretion, whether further action is required on the part of the prescribed person or prescribed entity 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 Information and Privacy Commissioner of Ontario of all the practices and procedures implemented by the prescribed person or prescribed entity;

- A partial detailed review by the Information and Privacy Commissioner of Ontario of one or more of the practices and procedures implemented by the prescribed person or prescribed entity;

- A request for further information from the prescribed person or prescribed entity with respect to one, more or all of its practices and procedures;

- An on-site meeting between the Information and Privacy Commissioner of Ontario and representatives of the prescribed person or prescribed entity;

- Requiring the prescribed person or prescribed entity to amend, implement or adhere to one or more of its practices and procedures or to develop and implement one or more additional practices or procedures;

- Requiring the prescribed person or prescribed entity to amend the written report or sworn affidavit submitted; and/or

- Any other action by the prescribed person or prescribed entity deemed appropriate in the sole and absolute discretion of the Information and Privacy Commissioner of Ontario.

If further action is warranted, the prescribed person or prescribed entity 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 entity or prescribed person must comply with such further action(s) as required by the Information and Privacy Commissioner of Ontario 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 Information and Privacy Commissioner of Ontario, or in the event that no further action is warranted, the Information and Privacy Commissioner of Ontario will advise the prescribed person or prescribed entity, in writing, that it continues to meet the requirements of the *Act* and its regulation. This is subject to any further actions that the Information and Privacy Commissioner of Ontario may require the prescribed person or prescribed entity to take prior to the next scheduled review of its practices and procedures.

The Information and Privacy Commissioner of Ontario will then make the letter advising the prescribed person or prescribed entity that it continues to meet the requirements of the *Act* and its regulation, and the detailed written report and sworn affidavit submitted by the prescribed person or prescribed entity, publicly available on its website at www.ipc.on.ca. The prescribed person or prescribed entity 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 person or prescribed entity unless it has submitted a detailed written report and accompanying sworn affidavit to the Information and Privacy Commissioner of Ontario and the Information and Privacy Commissioner of Ontario has advised the prescribed person or prescribed entity, in writing, that it continues to meet the requirements of the *Act* and its regulation.

## Rationale for the Change in the Review Process

Due to resource constraints and the large number of persons and organizations seeking to be prescribed as a prescribed person or prescribed entity, the process for the three-year review of the practices and procedures of the prescribed persons and prescribed entities needed to be streamlined.

The new review process ensures that prescribed persons and prescribed entities develop, implement and adhere to consistent and uniform practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information and ensures that the prescribed persons and prescribed entities are subject to appropriate oversight in respect of these practices and procedures.

# 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 person or prescribed entity | 15 |
| | 2. Policy and procedures for ongoing review of privacy policies, procedures and practices | 18 |
| **Transparency** | 3. Policy on the transparency of privacy policies, procedures and practices | 19 |
| **Collection of Personal Health Information** | 4. Policy and procedures for the collection of personal health information | 20 |
| | 5. List of data holdings containing personal health information | 22 |
| | 6. Policy and procedures for statements of purpose for data holdings containing personal health information | 23 |
| | 7. Statements of purpose for data holdings containing personal health information | 24 |
| **Use of Personal Health Information** | 8. Policy and procedures for limiting agent access to and use of personal health information | 24 |
| | 9. Log of agents granted approval to access and use personal health information | 28 |
| | 10. Policy and procedures for the use of personal health information for research | 28 |
| | 11. Log of approved uses of personal health information for research | 32 |

| Categories | Required Documentation | Page No. Appendix "B" |
|---|---|---|
| **Disclosure of Personal Health Information** | 12. Policy and procedures for disclosure of personal health information for purposes other than research | 33 |
| | 13. Policy and procedures for disclosure of personal health information for research purposes and the execution of research agreements | 37 |
| | 14. Template research agreement | 41 |
| | 15. Log of research agreements | 45 |
| **Data Sharing Agreements** | 16. Policy and procedures for the execution of data sharing agreements | 45 |
| | 17. Template data sharing agreement | 46 |
| | 18. Log of data sharing agreements | 50 |
| **Agreements with Third Party Service Providers** | 19. Policy and procedures for executing agreements with third party service providers in respect of personal health information | 50 |
| | 20. Template agreement for all third party service providers | 51 |
| | 21. Log of agreements with third party service providers | 57 |
| **Data Linkage and Data De-Identification** | 22. Policy and procedures for the linkage of records of personal health information | 57 |
| | 23. Log of approved linkages of records of personal health information | 60 |
| | 24. Policy and procedures with respect to de-identification and aggregation | 60 |

| Categories | Required Documentation | Page No. Appendix "B" |
|---|---|---|
| **Privacy Impact Assessments** | 25. Privacy impact assessment policy and procedures | 62 |
| | 26. Log of privacy impact assessments | 64 |
| **Privacy Audit Program** | 27. Policy and procedures in respect of privacy audits | 65 |
| | 28. Log of privacy audits | 66 |
| **Privacy Breaches, Inquiries and Complaints** | 29. Policy and procedures for privacy breach management | 66 |
| | 30. Log of privacy breaches | 69 |
| | 31. Policy and procedures for privacy complaints | 70 |
| | 32. Log of privacy complaints | 73 |
| | 33. Policy and procedures for privacy inquiries | 73 |

## Part 2 – Security Documentation

| Categories | Required Documentation | Page No. Appendix "B" |
|---|---|---|
| **General Security Policies and Procedures** | 1. Information security policy | 75 |
| | 2. Policy and procedures for ongoing review of security policies, procedures and practices | 77 |
| **Physical Security** | 3. Policy and procedures for ensuring physical security of personal health information | 78 |
| | 4. Log of agents with access to the premises of the prescribed person or prescribed entity | 81 |
| **Retention, Transfer and Disposal** | 5. Policy and procedures for secure retention of records of personal health information | 82 |
| | 6. Policy and procedures for secure retention of records of personal health information on mobile devices | 84 |
| | 7. Policy and procedures for secure transfer of records of personal health information | 87 |
| | 8. Policy and procedures for secure disposal of records of personal health information | 88 |
| **Information Security** | 9. Policy and procedures relating to passwords | 91 |
| | 10. Policy and procedures for maintaining and reviewing system control and audit logs | 92 |
| | 11. Policy and procedures for patch management | 94 |
| | 12. Policy and procedures related to change management | 95 |
| | 13. Policy and procedures for back-up and recovery of records of personal health information | 96 |
| | 14. Policy and procedures on the acceptable use of technology | 98 |

| Categories | Required Documentation | Page No. Appendix "B" |
|---|---|---|
| **Security Audit Program** | 15. Policy and procedures in respect of security audits | 99 |
| | 16. Log of security audits | 100 |
| **Information Security Breaches** | 17. Policy and procedures for information security breach management | 101 |
| | 18. Log of information security breaches | 103 |

## 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 | 105 |
| | 2. Log of attendance at initial privacy orientation and ongoing privacy training | 107 |
| **Security Training and Awareness** | 3. Policy and procedures for security training and awareness | 107 |
| | 4. Log of attendance at initial security orientation and ongoing security training | 110 |
| **Confidentiality Agreements** | 5. Policy and procedures for the execution of confidentiality agreements by agents | 110 |
| | 6. Template confidentiality agreement with agents | 111 |
| | 7. Log of executed confidentiality agreements with agents | 112 |
| **Responsibility for Privacy and Security** | 8. Job description for the position(s) delegated day-to-day authority to manage the privacy program | 113 |
| | 9. Job description for the position(s) delegated day-to-day authority to manage the security program | 114 |
| **Termination of Relationship** | 10. Policy and procedures for termination or cessation of the employment or contractual relationship | 114 |
| **Discipline** | 11. Policy and procedures for discipline and corrective action | 116 |

## Part 4 – Organizational and Other Documentation

| Categories | Required Documentation | Page No. Appendix "B" |
|---|---|---|
| **Governance** | 1. Privacy governance and accountability framework | 117 |
| | 2. Security governance and accountability framework | 118 |
| | 3. Terms of reference for committees with roles with respect to the privacy program and/or security program | 119 |
| **Risk Management** | 4. Corporate risk management framework | 119 |
| | 5. Corporate risk register | 121 |
| | 6. Policy and procedures for maintaining a consolidated log of recommendations | 121 |
| | 7. Consolidated log of recommendations | 122 |
| **Business Continuity and Disaster Recovery** | 8. Business continuity and disaster recovery plan | 122 |

# APPENDIX "B"
# MINIMUM CONTENT OF REQUIRED DOCUMENTATION

## Part 1 – Privacy Documentation

### 1. Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity

An overarching privacy policy, or equivalent, must be developed and implemented in relation to personal health information received by the person or organization as a prescribed person or prescribed entity under the *Personal Health Information Protection Act, 2004* ("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 person or organization as a prescribed person or prescribed entity under the *Personal Health Information Protection Act, 2004* ("the *Act*") and the duties and responsibilities that arise as a result of this status. In particular, the Privacy Policy must indicate that the prescribed person or prescribed entity has implemented policies, procedures and practices to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information and that these policies, procedures and practices are subject to review by the Information and Privacy Commissioner of Ontario every three years.

The Privacy Policy must also articulate a commitment by the prescribed person or prescribed entity to comply with the provisions of the *Act* and its regulation applicable to prescribed persons or prescribed entities, as the case may be.

#### *Privacy and Security Accountability Framework*

The accountability framework for ensuring compliance with the *Act* and its regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity 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 regulation and for ensuring compliance with the privacy and security policies, procedures and practices implemented.

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 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.

### *Collection of Personal Health Information*

The Privacy Policy must identify the purposes for which personal health information is collected, the types of personal health information collected and the persons or organizations from which personal health information is typically collected. In identifying the purposes for which personal health information is collected, the prescribed person or prescribed entity must ensure that each collection identified in the Privacy Policy is consistent with the collections of personal health information permitted by the *Act* and its regulation.

The Privacy Policy must also articulate a commitment by the prescribed person or prescribed entity not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose. In this regard, the Privacy Policy must outline the policies, procedures and practices implemented by the prescribed person or prescribed entity to ensure that both the amount and the type of personal health information collected is limited to that which is reasonably necessary for its purpose.

The Privacy Policy must also contain a list of the data holdings of personal health information maintained by the prescribed person or prescribed entity and must identify where an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding of personal health information.

### *Use of Personal Health Information*

The purposes for which the prescribed person or prescribed entity uses personal health information must be identified. In identifying these purposes, the prescribed person or prescribed entity must clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information and between the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the *Act*, as the case may be, and the use of personal health information for research purposes. The prescribed person or prescribed entity must also ensure that each use of personal health information identified in the Privacy Policy is consistent with the uses of personal health information permitted by the *Act* and its regulation.

The Privacy Policy must further articulate a commitment by the prescribed person or prescribed entity not to use personal health information if other information will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose and must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity in this regard, including limits on the use of personal health information by agents.

The Privacy Policy should also state that the prescribed person or prescribed entity remains responsible for personal health information used by its agents and should identify the policies, procedures and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with the *Act* and its regulation and in compliance with the privacy and security policies, procedures and practices implemented.

### *Disclosure of Personal Health Information*

The Privacy Policy must identify the purposes for which and the circumstances in which personal health information is disclosed, to whom such disclosures are typically made and the statutory or other requirements that must be satisfied prior to such disclosures. The prescribed person or prescribed entity must ensure that each disclosure identified in the Privacy Policy is consistent with the disclosures of personal health information permitted by the *Act* and its regulation.

The Privacy Policy must also clearly distinguish between the purposes for which and the circumstances in which personal health information is disclosed and the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed. It must further indicate that the prescribed person or prescribed entity will review all de-identified and/or aggregate information prior to its disclosure in order to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual.

Additionally, the Privacy Policy must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose and must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity in this regard.

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

The Privacy Policy must address the secure retention of records of personal health information in both paper and electronic format, including how long records of personal health information are retained, whether the records are retained in identifiable form and the secure manner in which they are retained. It must also address the manner in which records of personal health information 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 is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

### *Inquiries, Concerns or Complaints Related to Information Practices*

The Privacy Policy is required to identify the agent(s) to whom and the manner in which individuals may direct inquiries, concerns or complaints related to the privacy policies, procedures and practices of the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.

The information provided must include the name and/or title, mailing address and contact information for the agent(s) to whom inquiries, concerns or complaints may be directed and the manner and format in which these inquiries, concerns or complaints may be made. It should also state that individuals may direct complaints regarding the compliance of the prescribed person or prescribed entity with the *Act* and its regulation to the Information and Privacy Commissioner of Ontario and provide the mailing address and contact information for the Information and Privacy Commissioner of Ontario.

### *Transparency of Practices in Respect of Personal Health Information*

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

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

A policy and associated procedures must be developed and implemented for the ongoing review of the privacy policies, procedures and practices put in place by the prescribed person or prescribed entity. The purpose of the review is to determine whether amendments are needed or whether new privacy policies, procedures and practices are required.

The policy and procedures must identify the frequency of the review, the agent(s) responsible for undertaking the review, the procedure to be followed in undertaking the review and the time frame in which the review will be undertaken. At a minimum, the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity must be reviewed on an annual basis. The policy and procedures must also identify the agent(s) responsible and the procedure to be followed in amending and/or drafting new privacy policies, procedures and practices if deemed necessary as a result of the review, and the agent(s) responsible and the procedure that must be followed in obtaining approval of any amended or newly developed privacy policies, procedures and practices.

In undertaking the review and determining whether amendments and/or new privacy policies, procedures and practices are necessary, the prescribed person or prescribed entity must have regard to any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; evolving industry privacy standards and best practices; amendments to the *Act* and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. It must also take into account whether the privacy policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

The policy and its associated procedures must further identify the agent(s) responsible and the procedure to be followed in communicating the amended or newly developed privacy policies, procedures and practices, including the method and nature of the communication. It shall also identify the agent(s) responsible for and the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed privacy policies, procedures and practices.

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

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*.

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

A policy must be developed and implemented that identifies the information made available to the public and other stakeholders relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and that identifies the means by which such information is made available. At a minimum, the policy must require the prescribed person or prescribed entity to make the following information available:

- Its Privacy Policy;
- Brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity;
- Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information;
- A list of the data holdings of personal health information maintained by the prescribed person or prescribed entity; and
- The name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.

It is recommended that privacy impact assessments or a summary of the privacy impact assessments conducted also be made available.

The policy must also set out the minimum content of the brochures or frequently asked questions described above. In particular, the brochures or frequently asked questions must describe the status of the prescribed person or prescribed entity under the *Act*, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including:

- The types of personal health information collected and the persons or organizations from which this personal health information is typically collected;
- The purposes for which personal health information is collected;
- The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and
- The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.

The brochures or frequently asked questions must also identify some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

It is also recommended that the brochures or frequently asked questions provide the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.

## 4. Policy and Procedures for the Collection of Personal Health Information

A policy and procedures must be developed and implemented to identify the purposes for which personal health information will be collected by the prescribed entity or prescribed person, the nature of the personal health information that will be collected, from whom the personal health information will typically be collected and the secure manner in which personal health information will be collected.

The policy and procedures must articulate a commitment by the prescribed person or prescribed entity not to collect personal health information unless the collection is permitted by the *Act* and its regulation, not to collect personal health information if other information will serve the purpose and not to collect more personal health information than is reasonably necessary to meet the purpose.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

### *Review and Approval Process*

The policy and procedures must identify the agent(s) responsible for reviewing and determining whether to approve the collection of personal health information and the process that must be followed and the requirements that must be satisfied in this regard.

The policy and procedures must further set out the criteria that must be considered by the agent(s) responsible for determining whether to approve the collection of personal health information. At a minimum, the criteria must require the agent(s) responsible for determining whether to approve the collection of personal health information to ensure that the collection is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. The criteria must also require the agent(s) responsible for determining whether to approve the collection of personal health information to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

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

### *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 collection of personal health information, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements. The conditions or restrictions identified in the policy and procedures, including the documentation and/or agreements that must be completed, provided or executed, shall have regard to the requirements of the *Act* and its regulation.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the collection of personal health information have in fact been satisfied.

### *Secure Retention*

The policy and procedures must require that the records of personal health information collected by the prescribed person or prescribed entity be retained in a secure manner in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

### *Secure Transfer*

If the personal health information is being collected by an agent of the prescribed person or prescribed entity, such as a chart abstractor, the policy and procedures shall require the records of personal health information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

### *Secure Return or Disposal*

The policy and procedures must identify the agent(s) responsible for ensuring that the records of personal health information that have been collected are either securely returned or securely disposed of, as the case may be, following the retention period or the date of termination set out in any documentation and/or agreements executed prior to the collection of the personal health information.

If the records of personal health information are to be returned to the person or organization from which they were collected, the policy and procedures must require the records to be transferred in a secure manner and in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*. If the records are to be disposed of, the policy and procedures must require the records to be disposed of in a secure manner and in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information.*

## 5. List of Data Holdings Containing Personal Health Information

The prescribed person or prescribed entity shall develop and retain an up-to-date list and brief description of the data holdings of personal health information maintained by the prescribed person or prescribed entity.

## 6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

A policy and procedures must be developed and implemented with respect to the creation, review, amendment and approval of statements of purpose for data holdings containing personal health information. The policy and procedures shall require the statements of purpose to set out the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.

The policy and procedures must also identify the agent(s) responsible and the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other persons or organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose shall also be specified.

The persons and organizations that will be provided the statements of purpose 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 in the data holding is collected.

The policy and procedures shall further require that the statements of purpose be reviewed on an ongoing basis in order to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes. In this regard, the frequency with which and the circumstances in which the statements of purpose are required to be reviewed must be identified.

The agent(s) responsible and the process that must be followed in reviewing the statements of purpose and in amending the statements of purpose, if necessary, shall also be documented. This shall include the agent(s) or other persons or organizations that must be consulted in reviewing, and if necessary, amending the statements of purpose and the agent(s) responsible for approving the amended statements of purpose. The policy and procedures must further identify the persons and organizations that will be provided amended statements of purpose upon approval, including health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 7. Statements of Purpose for Data Holdings Containing Personal Health Information

For each data holding containing personal health information, the prescribed person or prescribed entity must draft a statement identifying the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.

## 8. Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information

A policy and procedures must be developed and implemented to limit access to and use of personal health information by agents based on the "need to know" principle. The purpose of this policy and its procedures is to ensure that agents of the prescribed person or prescribed entity access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.

The policy and procedures must identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal health information and the levels of access to personal health information that may be granted. The prescribed person or prescribed entity must ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal health information.

For all other purposes and in all other circumstances, the policy and procedures must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy and Procedures with Respect to De-Identification and Aggregation.*

In this regard, the policy and procedures must explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.

The policy and procedures must also prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

### *Review and Approval Process*

The agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information shall be set out in the policy and procedures, along with the various level(s) of access that may be granted by the prescribed person or prescribed entity.

In outlining the process to be followed, the policy and procedures must set out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also set out the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal health information and, if the request is approved, the criteria that must be considered in determining the appropriate level of access. At a minimum, the agent(s) responsible for determining whether to approve or deny the request must be satisfied that:

- The agent making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities;

- The identified purpose for which access to and use of personal health information is requested is permitted by the *Act* and its regulation;

- The identified purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without personal health information;

- De-identified and/or aggregate information will not serve the identified purpose; and

- In approving the request, no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request for access to and use of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

### *Conditions or Restrictions on the Approval*

The policy and procedures must identify the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.

In the event that an agent only requires access to and use of personal health information for a specified period, the policy and procedures must set out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period.

It is recommended that all approved accesses and uses of personal health information be subject to an automatic expiry, following which an agent is again required to request approval to access and use personal health information in accordance with the policy and its procedures. At a minimum, it is recommended that the expiry date be one year from the date approval is granted.

The policy and procedures must also prohibit an agent granted approval to access and use personal health information from accessing and using personal health information except as necessary for his or her employment, contractual or other responsibilities; from accessing and using personal health information if other information will serve the identified purpose; and from accessing and using more personal health information than is reasonably necessary to meet the identified purpose. The prescribed person or prescribed entity must also ensure that all accesses to and uses of personal health information are permitted by the *Act* and its regulation.

Further, the policy and procedures must impose conditions or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal health information is permitted to disclose that personal health information. The prescribed person or prescribed entity must ensure that any such disclosures are permitted by the *Act* and its regulation.

### *Notification and Termination of Access and Use*

The policy and procedures must require an agent granted approval to access and use personal health information, as well as his or her supervisor, to notify the prescribed person or prescribed entity when the agent is no longer employed or retained by the prescribed person or prescribed entity or no longer requires access to or use of the personal health information.

The procedure to be followed in providing the notification must also be identified. In particular, the policy and procedures must identify the agent(s) to whom this notification must be provided; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed, if any; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also identify the agent(s) responsible for terminating access to and use of the personal health information, the procedure to be followed in terminating access to

and use of the personal health information and the time frame within which access to and use of the personal health information must be terminated.

The prescribed person or prescribed entity must ensure that the procedures implemented in this regard are consistent with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

### *Secure Retention*

The policy and procedures must require an agent granted approval to access and use personal health information to securely retain the records of personal health information in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

### *Secure Disposal*

The policy and procedures must require an agent granted approval to access and use personal health information to securely dispose of the records of personal health information in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.

### *Tracking Approved Access to and Use of Personal Health Information*

The policy and procedures must require that a log be maintained of agents granted approval to access and use personal health information and must identify the agent(s) responsible for maintaining such a log. It is also recommended that the policy and procedures address where documentation related to the receipt, review, approval, denial or termination of access to and use of personal health information is to be retained and the agent(s) responsible for retaining this documentation.

### *Compliance, Audit and Enforcement*

The prescribed person or prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.

In the event that there is no automatic expiry date on the approval to access and use personal health information, regular audits of agents granted approval to access and use personal health information must be conducted in accordance with the *Policy and Procedures In Respect of Privacy Audits*. The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by the prescribed person or prescribed entity and continue to require access to the same amount and type of personal health information. In this regard, the policy and procedures must identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, audits must be conducted on an annual basis.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 9. Log of Agents Granted Approval to Access and Use Personal Health Information

A prescribed person or prescribed entity must maintain a log of agents granted approval to access and use personal health information. At a minimum, the log must include the name of the agent granted approval to access and use personal health information; the data holdings of personal health information to which the agent has been granted approval to access and use; the level or type of access and use granted; the date that access and use was granted; and the termination date or the date of the next audit of access to and use of the personal health information.

## 10. Policy and Procedures for the Use of Personal Health Information for Research

A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be used for research purposes.

The policy and procedures must articulate a commitment by the prescribed person or prescribed entity not to use personal health information for research purposes if other information will serve the research purpose and not to use more personal health information than is reasonably necessary to meet the research purpose.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of the policy or its procedures.

### *Where the Use of Personal Health Information is Permitted for Research*

If the prescribed person or prescribed entity permits personal health information to be used for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be used for research purposes.

### Distinction between the Use of Personal Health Information for Research and Other Purposes

The policy and its procedures must clearly distinguish between the use of personal health information for research purposes and the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the *Act*, as the case may be. The criteria that must be considered in determining when a use of personal health information is for research purposes and when a use is for purposes of subsection 39(1)(c) or section 45 of the *Act*, as well as the agent(s) responsible and the procedure to be followed in making this determination, must also be addressed.

### Review and Approval Process

The policy and procedures must also identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.

At a minimum, prior to any approval of the use of personal health information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to review the written research plan to ensure it complies with the requirements in the *Act* and its regulation, to ensure that the written research plan has been approved by a research ethics board and to ensure that the prescribed person or prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan.

In addition, prior to any approval of the use of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

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

### Conditions or Restrictions on the Approval

The policy and procedures must identify the conditions or restrictions that will be imposed on the approval to use personal health information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation. In determining the conditions or restrictions that will be imposed, the policy and procedures shall have regard to the *Act* and its regulation. At a minimum, the agent(s) granted approval to use personal health information for research purposes must be required to comply with subsections 44(6) (a) to (f) of the *Act*.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of personal health information for research purposes are in fact being satisfied.

### Secure Retention

The policy and procedures must require the agent granted approval to use personal health information for research purposes to retain the records of personal health information in compliance with the written research plan approved by the research ethics board and in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*.

### Secure Return or Disposal

The policy and procedures must address whether an agent granted approval to use personal health information for research purposes is required to securely return or securely dispose of the records of personal health information or is permitted to de-identify and retain the records following the retention period in the written research plan approved by the research ethics board.

If the records of personal health information are required to be securely returned to the prescribed person or prescribed entity, the policy and procedures must stipulate the time frame following the retention period set out in the written research plan within which the records must be securely returned, the secure manner in which the records must be returned and the agent to whom the records must be securely returned.

If the records of personal health information are required to be disposed of in a secure manner, the policy and procedures must require the records to be disposed of in accordance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*. The policy and procedures must further stipulate the time frame following the retention period in the written research plan within which the records must be securely disposed of, must require a certificate of destruction to be provided, must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided and must identify the time frame following secure disposal within which the certificate of destruction must be provided. The certificate of destruction confirming the secure disposal must be required to identify the records of personal health information securely disposed of and the date, time and

method of secure disposal employed and must be required to bear the name and signature of the agent who performed the secure disposal.

If the records of personal health information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, the policy and procedures shall require the records of personal health information to be de-identified in compliance with the *Policy and Procedures With Respect to De-Identification and Aggregation*. The policy and procedures must further stipulate the time frame following the retention period set out in the written research plan within which the records must be de-identified.

The policy and procedures must also identify the agent(s) responsible for ensuring that records of personal health information used for research purposes are securely returned, securely disposed of or de-identified within the stipulated time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of personal health information are not securely returned, a certificate of destruction is not received or the records of personal health information are not de-identified within the time frame identified.

### Tracking Approved Uses of Personal Health Information for Research

The policy and procedures must require that a log be maintained of the approved uses of personal health information for research purposes and must identify the agent(s) responsible for maintaining such a log. It is also recommended that the policy and procedures address where written research plans, copies of the decisions of research ethics boards, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.

## *Where the Use of Personal Health Information is not Permitted for Research*

If the prescribed person or prescribed entity does not permit personal health information to be used for research purposes, the policy and procedures must expressly prohibit the use of personal health information for research purposes and must indicate whether or not de-identified and/or aggregate information may be used for research purposes.

### Review and Approval Process

If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of de-identified and/or aggregate information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de-identified and/or aggregate information for research purposes. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the use of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

### Conditions or Restrictions on the Approval

The policy and procedures must also identify the conditions or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.

At a minimum, the policy and procedures must prohibit an agent granted approval to use de-identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.

## 11. Log of Approved Uses of Personal Health Information for Research

A prescribed person or prescribed entity that permits the use of personal health information for research purposes must maintain a log of the approved uses that, at a minimum, includes:

- The name of the research study;
- The name of the agent(s) to whom the approval was granted;
- The date of the decision of the research ethics board approving the written research plan;

- The date that the approval to use personal health information for research purposes was granted by the prescribed person or prescribed entity;
- The date that the personal health information was provided to the agent(s);
- The nature of the personal health information provided to the agent(s);
- The retention period for the records of personal health information identified in the written research plan approved by the research ethics board;
- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained following the retention period; and
- The date the records of personal health information were securely returned or a certificate of destruction was received or the date by which they must be returned or disposed of, if applicable.

## 12. Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, personal health information is permitted to be disclosed for purposes other than research.

The policy and procedures must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

### *Where the Disclosure of Personal Health Information is Permitted*

If the prescribed person or prescribed entity permits personal health information to be disclosed for purposes other than research, the policy and procedures must set out the purposes for which and the circumstances in which the disclosure of personal health information is permitted. The policy and procedures must further require that all disclosures of personal health information comply with the *Act* and its regulation.

#### Review and Approval Process

The policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.

At a minimum, the agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that the disclosure is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. For example, if a prescribed entity is requested to disclose personal health information to a health information custodian who provided the personal health information directly or indirectly to the prescribed entity, the prescribed entity must ensure that the personal health information does not contain any additional identifying information.

The criteria must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of personal health information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

### 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 disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements. At a minimum, the policy and procedures must require a Data Sharing Agreement to be executed in accordance with the *Policy and Procedures for the Execution of Data Sharing Agreements* and the *Template Data Sharing Agreement* prior to any disclosure of personal health information for purposes other than research.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a Data Sharing Agreement.

### Secure Transfer

The policy and procedures shall require records of personal health information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

### Secure Return or Disposal

The policy and procedures must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.

The policy and procedures 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 within a reasonable period of time following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement. This shall include the agent(s) responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented.

### Documentation Related to Approved Disclosures of Personal Health Information

It is recommended that the policy and procedures address where documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research will be retained and the agent(s) responsible for retaining this documentation.

### *Where the Disclosure of Personal Health Information is not Permitted*

If the prescribed person or prescribed entity does not permit personal health information to be disclosed in these circumstances, the policy and procedures must expressly prohibit the disclosure of personal health information for non-research purposes, except where required by law, and must indicate whether or not de-identified and/or aggregate information may be disclosed.

#### Review and Approval Process

If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for non-research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

#### Conditions or Restrictions on the Approval

The policy and procedures must also identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.

At a minimum, the prescribed person or prescribed entity must require the person or organization to which the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policy and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.

## 13. Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements

A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes.

The policy and procedures must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information for research purposes if other information will serve the research purpose and not to disclose more personal health information than is reasonably necessary to meet the research purpose.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

### *Where the Disclosure of Personal Health Information is Permitted for Research*

If the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be disclosed for research purposes.

## Review and Approval Process

The policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by the researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.

At a minimum, prior to any approval of the disclosure of personal health information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that the prescribed person or prescribed entity is in receipt of a written application, a written research plan and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the *Act* and its regulation.

In addition, prior to any approval of the disclosure of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.

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

## 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 disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements. At a minimum, the policy and procedures must require that a Research Agreement be executed in accordance with the *Template Research Agreement* prior to the disclosure of personal health information for research purposes.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information for research purposes have in fact been satisfied, including the execution of a Research Agreement.

### Secure Transfer

The policy and procedures shall require the records of personal health information disclosed for research purposes to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information.*

### Secure Return or Disposal

The policy and procedures must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a researcher for research purposes are either securely returned, securely disposed of or de-identified, as the case may be, following the retention period set out in the Research Agreement. The policy and procedures must further address the process to be followed by the responsible agent(s) where records of personal health information are not securely returned, a certificate of destruction is not received or written confirmation of de-identification is not received within the time set out in the Research Agreement.

### Documentation Related to Approved Disclosures of Personal Health Information for Research

It is recommended that the policy and procedures also address where written applications, written research plans, copies of the decisions of research ethics boards, Research Agreements, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.

## *Where the Disclosure of Personal Health Information is not Permitted for Research*

If the prescribed person or prescribed entity does not permit personal health information to be disclosed for research purposes, the policy and procedures must expressly prohibit the disclosure of personal health information for research purposes and must indicate whether or not de-identified and/or aggregate information may be disclosed for research purposes.

### Review and Approval Process

If the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or

prescribed entity or by a researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

For example, the policy and procedures should address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with the *Act* and its regulation and/or requires research ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for research purposes. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the approval and disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.

The policy and procedures should also set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

### Conditions or Restrictions on the Approval

The policy and procedures must also identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.

At a minimum, the prescribed person or prescribed entity must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

The policy and procedures must also identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policy and procedures shall require the responsible agent(s) to track receipt of the executed written acknowledgments and shall set out the procedure that must be followed and the documentation that must be maintained in this regard.

## 14. Template Research Agreement

A Research Agreement must be executed with the researchers to whom personal health information will be disclosed prior to the disclosure of the personal health information for research purposes. At a minimum, the Research Agreement must address the matters set out below.

### *General Provisions*

The Research Agreement must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status. It must also specify the precise nature of the personal health information that will be disclosed by the prescribed person or prescribed entity for research purposes and must provide a definition of personal health information that is consistent with the *Act* and its regulation.

### *Purposes of Collection, Use and Disclosure*

The research purpose for which the personal health information is being disclosed by the prescribed person or prescribed entity and the purposes for which the personal health information may be used or disclosed by the researcher must be identified in the Research Agreement, as must the statutory authority for each collection, use and disclosure identified.

In particular, the Research Agreement must only permit the researcher to use the personal health information for the purposes set out in the written research plan approved by the research ethics board and must prohibit the use of the personal health information for any other purpose. The Research Agreement must also prohibit the researcher from permitting persons to access and use the personal health information except those persons described in the written research plan approved by the research ethics board.

In identifying the purposes for which the personal health information may be used, the Research Agreement shall explicitly state whether or not the personal health information may be linked to other information and must prohibit the personal health information from being linked except in accordance with the written research plan approved by the research ethics board.

The Research Agreement shall also require the researcher to acknowledge that the personal health information that is being disclosed pursuant to the Research Agreement is necessary for the identified research purpose and that other information, namely de-identified and/or aggregate information, will not serve the research purpose. The researcher must also be required to acknowledge that no more personal health information is being collected and will be used than is reasonably necessary to meet the research purpose.

The Research Agreement must also impose restrictions on the disclosure of personal health information. At a minimum, the Research Agreement must require the researcher to acknowledge and agree not to disclose the personal health information except as required by law and subject to the exceptions and additional requirements prescribed in the regulation to the *Act*; not to publish the personal health information in a form that could reasonably enable a person to

ascertain the identity of the individual; and not to make contact or attempt to make contact with the individual to whom the personal health information relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of the *Act*.

### *Compliance with the Statutory Requirements for the Disclosure for Research Purposes*

The Research Agreement must require the researcher and the prescribed person or prescribed entity to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the *Act* and its regulation, and a copy of the decision of the research ethics board approving the written research plan.

The researcher must also be required to acknowledge and agree that the researcher will comply with the Research Agreement, with the written research plan approved by the research ethics board and with the conditions, if any, specified by the research ethics board in respect of the written research plan.

### *Secure Transfer*

The Research Agreement shall require the secure transfer of records of personal health information that will be disclosed pursuant to the Research Agreement. The Research Agreement shall set out the secure manner in which records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that will be followed in ensuring that the records of personal health information are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, the Research Agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

### *Secure Retention*

The retention period for the records of personal health information subject to the Research Agreement must also be identified, including the length of time that the records of personal health information will be retained in identifiable form. The retention period identified must be consistent with that set out in the written research plan approved by the research ethics board.

The Research Agreement shall require the researcher to ensure that the records of personal health information are retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained. In identifying the secure manner in which the records of personal health information will be retained, the Research Agreement may have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* and shall have regard to the written research plan approved by the research ethics board.

The Research Agreement must also require the researcher to take steps that are reasonable in the circumstances to ensure that the personal health information subject to the Research Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records

of personal health information subject to the Research Agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken by the researcher must be detailed in the Research Agreement and, at a minimum, shall include those set out in the written research plan approved by the research ethics board.

### *Secure Return or Disposal*

The Research Agreement must also address whether the records of personal health information subject to the Research Agreement will be returned in a secure manner, will be disposed of in a secure manner or will be de-identified and retained by the researcher following the retention period set out in the Research Agreement. In this regard, the provisions in the Research Agreement shall be consistent with the written research plan approved by the research ethics board.

If the records of personal health information are required to be returned in a secure manner, the Research Agreement must stipulate the time frame following the retention period within which the records must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned.

In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

If the records of personal health information are required to be disposed of in a secure manner, the Research Agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information subject to the Research Agreement must be securely disposed of. The Research Agreement must also stipulate the time frame following the retention period set out in the Research Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Further, the Research Agreement must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction. 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, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

If the records of personal health information are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de-identification must be set out in the Research Agreement. In identifying the manner and process for de-identification, regard may be had to the *Policy and Procedures with Respect to De-Identification and Aggregation* implemented by the prescribed person or prescribed entity. The Research Agreement must also require the researcher to submit written confirmation that the records were de-identified and shall stipulate the time frame following the retention period set out in the Research Agreement within which the written confirmation must be provided and the agent of the prescribed person or prescribed entity to whom the written confirmation must be provided.

### *Notification*

At a minimum, the Research Agreement must require the researcher to notify the prescribed person or prescribed entity immediately, in writing, if the researcher becomes aware of a breach or suspected breach of the Research Agreement, a breach or suspected of subsection 44(6) of the *Act* or if personal health information subject to the Research Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The Research Agreement should also identify the agent of the prescribed person or prescribed entity to whom notification must be provided and must require the researcher to take steps that are reasonable in the circumstances to contain the breach and to contain the theft, loss or access by unauthorized persons.

### *Consequences of Breach and Monitoring Compliance*

The Research Agreement must outline the consequences of breach of the agreement and must indicate whether compliance with the Research Agreement will be audited by the prescribed person or prescribed entity and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

The Research Agreement must also require the researcher to ensure that all persons who will have access to the personal health information, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the Research Agreement prior to being given access to the personal health information. The Research Agreement must set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Research Agreement.

## 15. Log of Research Agreements

A prescribed person or prescribed entity must maintain a log of executed Research Agreements. At a minimum, the log must include:

- The name of the research study;
- The name of the principal researcher to whom the personal health information was disclosed pursuant to the Research Agreement;
- The date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan;
- The date that the approval to disclose the personal health information for research purposes was granted by the prescribed person or prescribed entity;
- The date that the Research Agreement was executed;
- The date that the personal health information was disclosed;
- The nature of the personal health information disclosed;
- The retention period for the records of personal health information as set out in the Research Agreement;
- Whether the records of personal health information will be securely returned, securely disposed of or de-identified and retained by the researcher following the retention period set out in the Research Agreement; and
- The date that the records of personal health information were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.

## 16. Policy and Procedures for the Execution of Data Sharing Agreements

A policy and procedures must be developed and implemented to identify the circumstances requiring the execution of a Data Sharing Agreement and the process that must be followed and the requirements that must be satisfied prior to the execution of a Data Sharing Agreement.

The policy and procedures must set out the circumstances requiring the execution of a Data Sharing Agreement prior to the collection of personal health information for purposes other than research and must require the execution of a Data Sharing Agreement prior to any disclosure of personal health information for purposes other than research.

The policy and procedures must further identify the agent(s) responsible for ensuring that a Data Sharing Agreement is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

In relation to the disclosure of personal health information for purposes other than research, the agent(s) responsible for ensuring that a Data Sharing Agreement is executed must be satisfied that the disclosure was approved in accordance with the *Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research*. In relation to the collection of personal health information for purposes other than research, the agent(s) responsible for ensuring that a Data Sharing Agreement is executed must be satisfied that the collection was approved in accordance with the *Policy and Procedures for the Collection of Personal Health Information*.

The policy and procedures must also require that a log of Data Sharing Agreements be maintained and must identify the agent(s) responsible for maintaining such a log. In addition, it is recommended that the policy and procedures address where documentation related to the execution of Data Sharing Agreements will be retained and the agent(s) responsible for retention.

The prescribed person or prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. 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 agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 17. Template Data Sharing Agreement

A prescribed person or prescribed entity must ensure that a Data Sharing Agreement is executed in the circumstances set out in the *Policy and Procedures for the Execution of Data Sharing Agreements* that, at a minimum, addresses the matters set out below.

### *General Provisions*

The Data Sharing Agreement must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status. It must also

specify the precise nature of the personal health information subject to the Data Sharing Agreement and must provide a definition of personal health information that is consistent with the *Act* and its regulation. The Data Sharing Agreement shall also identify the person or organization that is collecting personal health information and the person or organization that is disclosing personal health information pursuant to the Data Sharing Agreement.

### *Purposes of Collection, Use and Disclosure*

The Data Sharing Agreement must also identify the purposes for which the personal health information subject to the Data Sharing Agreement is being collected and for which the personal health information will be used.

In identifying these purposes, the Data Sharing Agreement shall explicitly state whether or not the personal health information collected pursuant to the Data Sharing Agreement will be linked to other information. If the personal health information will be linked to other information, the Data Sharing Agreement must identify the nature of the information to which the personal health information will be linked, the source of the information to which the personal health information will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.

The Data Sharing Agreement shall also contain an acknowledgement that the personal health information collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it was collected and that other information, namely de-identified and/or aggregate information, will not serve the purpose and that no more personal health information is being collected and will be used than is reasonably necessary to meet the purpose.

The Data Sharing Agreement must also identify the purposes, if any, for which the personal health information subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.

The Data Sharing Agreement must also require the collection, use and disclosure of personal health information subject to the Data Sharing Agreement to comply with the *Act* and its regulation and must set out the specific statutory authority for each collection, use and disclosure contemplated in the Data Sharing Agreement.

### *Secure Transfer*

The Data Sharing Agreement shall require the secure transfer of the records of personal health information subject to the Data Sharing Agreement. The Data Sharing Agreement shall set out the secure manner in which the records of personal health information will be transferred, including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner. In identifying the secure manner in which the records of personal health information will be transferred, regard may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

### *Secure Retention*

The retention period for the records of personal health information subject to the Data Sharing Agreement must also be specified. In identifying the relevant retention period, it must be ensured that the records of personal health information are retained only for as long as necessary to fulfill the purposes for which the records of personal health information were collected.

The Data Sharing Agreement shall also require the records of personal health information to be retained in a secure manner and shall identify the precise manner in which the records of personal health information in paper and electronic format will be securely retained, including whether the records will be retained in identifiable form. In identifying the secure manner in which the records of personal health information will be retained, the Data Sharing Agreement may have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

The Data Sharing Agreement must also require reasonable steps to be taken to ensure that the personal health information subject to the Data Sharing Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken shall also be detailed in the Data Sharing Agreement.

### *Secure Return or Disposal*

The Data Sharing Agreement must also address whether the records of personal health information subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.

If the records of personal health information are required to be returned in a secure manner, the Data Sharing Agreement must stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the person to whom the records must be securely returned. In identifying the secure manner in which the records of personal health information will be returned, regard may be had to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

If the records of personal health information are required to be disposed of in a secure manner, the Data Sharing Agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information subject to the Data Sharing Agreement must be securely disposed of. The Data Sharing Agreement must also stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of personal health information must be securely disposed of and within which a certificate of destruction must be provided.

In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*. In addition, regard may be had to the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

Further, the Data Sharing Agreement must identify the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction. 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, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

### *Notification*

At a minimum, the Data Sharing Agreement must require that notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the personal health information subject to the Data Sharing Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. It should also identify whether the notification must be verbal and/or in writing and to whom the notification must be provided. The Data Sharing Agreement must also require that reasonable steps be taken to contain the breach of the Data Sharing Agreement and to contain the theft, loss or access by unauthorized persons.

### *Consequences of Breach and Monitoring Compliance*

The Data Sharing Agreement must outline the consequences of breach of the agreement and must indicate whether compliance with the Data Sharing Agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

The Data Sharing Agreement must also require that all persons who will have access to the personal health information are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the personal health information. The Data Sharing Agreement must set out the method by which this will be ensured. This may include requiring the persons that will have access to the personal health information to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement.

## 18. Log of Data Sharing Agreements

A prescribed person or prescribed entity must maintain a log of executed Data Sharing Agreements. At a minimum, the log must include:

- The name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;
- The date that the collection or disclosure of personal health information was approved, as the case may be;
- The date that the Data Sharing Agreement was executed;
- The date the personal health information was collected or disclosed, as the case may be;
- The nature of the personal health information subject to the Data Sharing Agreement;
- The retention period for the records of personal health information set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement;
- Whether the records of personal health information will be securely returned or will be securely disposed of following the retention period set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

## 19. Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information

A policy and procedures must be developed and implemented requiring written agreements to be entered into with third party service providers prior to permitting third party service providers to access and use the personal health information of the prescribed person or prescribed entity. 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 agent(s) responsible for ensuring that an agreement is executed, as well as the process that must be followed and the requirements that must be satisfied prior to the execution of such an agreement, must also be identified in the policy and procedures.

The policy and procedures must also state that the prescribed person or prescribed entity shall not provide personal health information to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will not provide

more personal health information than is reasonably necessary to meet the purpose. The agent responsible for making this determination must also be identified in the policy and procedures.

The policy and procedures must further identify the agent(s) responsible for ensuring that records of personal health information provided to a third party service provider are either securely returned to the prescribed person or prescribed entity or are securely disposed of, as the case may be, following the termination of the agreement. 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 agent(s) responsible for implementing this process and the time frame following termination within which this process must be implemented.

The policy and procedures must require that a log be maintained of all agreements executed with third party service providers and must identify the agent(s) responsible for maintaining such a log. In addition, it is recommended that the policy and procedures address where documentation related to the execution of agreements with third party service providers will be retained and the agent(s) responsible for retaining this documentation.

The prescribed person or prescribed entity must also require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. 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 agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 20. Template Agreement for All Third Party Service Providers

A written agreement must be entered into with third party service providers that will be permitted to access and use personal health information of the prescribed person or prescribed entity, including those that are contracted to retain, transfer or dispose of records of personal health information and those that are contracted to provide services for the purpose of enabling the prescribed person or prescribed entity to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information (“electronic service providers”). At a minimum, the written agreement must address the matters set out below.

### *General Provisions*

The agreement must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status. The agreement must also state whether or not the third party service provider is an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.

All third party service providers that are permitted to access and use personal health information in the course of providing services to the prescribed person or prescribed entity shall be considered agents of the prescribed entity or prescribed person, with the possible exception of electronic service providers. Agreements with electronic service providers shall explicitly state whether or not the third party service provider is an agent of the prescribed person or prescribed entity in providing services pursuant to the agreement.

If the third party service provider is an agent of the prescribed person or prescribed entity, the agreement must require the third party service provider to comply with the provisions of the *Act* and its regulation relating to prescribed persons or prescribed entities, as the case may be, and to comply with the privacy and security policies and procedures implemented by the prescribed person or prescribed entity in providing services pursuant to the agreement.

It is also recommended that the agreement provide a definition of personal health information and that the definition provided be consistent with the *Act* and its regulation. Where appropriate, the agreement should also specify the precise nature of the personal health information that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

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 agents of the third party service provider.

### *Obligations with Respect to Access and Use*

The agreement shall identify the purposes for which the third party service provider is permitted to access and use the personal health information of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to use personal health information, the prescribed person or prescribed entity must ensure that each use identified in the agreement is consistent with the uses of personal health information permitted by the *Act* and its regulation. The agreement must also prohibit the third party service provider from using personal health information except as permitted in the agreement.

In the case of an electronic service provider that is not an agent of the prescribed person or prescribed entity, the agreement must explicitly prohibit the electronic service provider from using personal health information except as necessary in the course of providing services pursuant to the agreement.

Further, the agreement must prohibit the third party service provider from using personal health information if other information will serve the purpose and from using more personal health information than is reasonably necessary to meet the purpose.

### *Obligations with Respect to Disclosure*

The agreement must identify the purposes, if any, for which the third party service provider is permitted to disclose the personal health information of the prescribed entity or prescribed person and any limitations, conditions or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to disclose personal health information, the prescribed person or prescribed entity must ensure that each disclosure identified in the agreement is consistent with the disclosures of personal health information permitted by the *Act* and its regulation. In this regard, the agreement must prohibit the third party service provider from disclosing personal health information except as permitted in the agreement or as required by law, from disclosing personal health information if other information will serve the purpose and from disclosing more personal health information than is reasonably necessary to meet the purpose.

In the case of an electronic service provider that is not an agent of the prescribed entity or prescribed person, the agreement must prohibit the electronic service provider from disclosing personal health information to which it has access in the course of providing services except as required by law.

### *Secure Transfer*

Where it is necessary to transfer records of personal health information to or from the prescribed person or prescribed entity, the agreement must require the third party service provider to securely transfer the records of personal health information and must set out the responsibilities of the third party service provider in this regard. In particular, the agreement must specify the secure manner in which the records will be transferred by the third party service provider, the conditions pursuant to which the records will be transferred by the third party service provider, to whom the records will be transferred and the procedure that must be followed by the third party service provider in ensuring that the records are transferred in a secure manner.

In identifying the secure manner in which records of personal health information must be transferred, the agreement shall have regard to the *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

In addition, where the retention of records of personal health information or where the disposal of records of personal health information outside the premises of the prescribed person or prescribed entity is the primary service provided to the prescribed person or prescribed entity, the agreement shall require the third party service provider to provide documentation to the prescribed person or prescribed entity setting out the date, time and mode of transfer of the

records of personal health information and confirming receipt of the records of personal health information by the third party service provider. In these circumstances, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records of personal health information transferred.

### *Secure Retention*

The agreement shall require the third party service provider to retain the records of personal health information, where applicable, in a secure manner and shall identify the precise methods by which records of personal health information in paper and electronic format will be securely retained by the third party service provider, including records of personal health information retained on various media.

The agreement must further outline the responsibilities of the third party service provider in securely retaining the records of personal health information. In identifying the secure manner in which the records of personal health information will be retained, and the methods by which the records of personal health information will be securely retained, the agreement shall have regard to the *Policy and Procedures for Secure Retention of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

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

### *Secure Return or Disposal Following Termination of the Agreement*

The agreement must address, where applicable, whether records of personal health information will be securely returned to the prescribed person or prescribed entity or will be disposed of in a secure manner following the termination of the agreement.

If the records of personal health information are required to be returned in a secure manner, the agreement must stipulate the time frame following the date of termination of the agreement within which the records of personal health information must be securely returned, the secure manner in which the records must be returned and the agent of the prescribed person or prescribed entity to whom the records must be securely returned. In identifying the secure manner in which the 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* implemented by the prescribed person or prescribed entity.

If the records of personal health information are required to be disposed of in a secure manner, the agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of personal health information are to be securely disposed of.

In identifying the secure manner in which the records of personal health information will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*; and with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by the prescribed person or prescribed entity.

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 to the prescribed person or prescribed entity. The agreement must further identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided and must identify the required content of the certificate of destruction. 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 is the primary service provided to the prescribed person or prescribed entity by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement must further set out the responsibilities of the third party service provider in securely disposing of the records of personal health information, including:

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

The agreement should also enable the prescribed person or prescribed entity, at its discretion, to witness the secure disposal of the records of personal health information subject to such reasonable terms or conditions as may be required in the circumstances.

### *Implementation of Safeguards*

The agreement shall require the third party service provider to take steps that are reasonable in the circumstances to ensure that the personal health information accessed and used in the course of providing services pursuant to the agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information subject to the

agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be implemented by the third party service provider must be detailed in the agreement.

### *Training of Agents of the Third Party Service Provider*

The agreement shall require the third party service provider to provide training to its agents on the importance of protecting the privacy of individuals whose personal health information is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations.

The agreement must also require the third party service provider to ensure that its agents who will have access to the records of personal health information are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the personal health information. The agreement must set out the method by which this will be ensured. This may include requiring agents to sign an acknowledgement, prior to being granted access to the personal health information, indicating that they are aware of and agree to comply with the terms and conditions of the agreement.

### *Subcontracting of the Services*

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

### *Notification*

At a minimum, the agreement must require the third party service provider to notify the prescribed person or prescribed entity at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if personal health information handled by the third party service provider on behalf of the prescribed person or prescribed entity is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. The 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 theft, loss or access by unauthorized persons.

### *Consequences of Breach and Monitoring Compliance*

The agreement must outline the consequences of breach of the agreement and must indicate whether the prescribed person or prescribed entity will be auditing compliance with the

agreement and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided to the third party service provider of the audit.

## 21. Log of Agreements with Third Privacy Service Providers

A prescribed person or prescribed entity must maintain a log of executed agreements with third party service providers. At a minimum, the log must include:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use of personal health information;
- The date that the agreement with the third party service provider was executed;
- The date that the records of personal health information or access to the records of personal health information, if any, was provided;
- The nature of the personal health information provided or to which access was provided;
- The date of termination of the agreement with the third party service provider;
- Whether the records of personal health information, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and
- The date the records of personal health information were securely returned or a certificate of destruction was provided or the date that access to the personal health information was terminated or the date by which the records of personal health information must be returned or disposed of or access terminated.

## 22. Policy and Procedures for the Linkage of Records of Personal Health Information

A policy and procedures must be developed and implemented with respect to linkages of records of personal health information.

The policy and procedures must identify whether or not the prescribed person or prescribed entity permits the linkage of records of personal health information and if it is not permitted, the policy and procedures must expressly prohibit the linkage of records of personal health information. If the linkage of records of personal health information is permitted, the purposes for which and the circumstances in which such linkages are permitted must be identified.

In identifying the purposes for which and the circumstances in which the linkage of records of personal health information is permitted, regard must be had to the sources of the records of personal health information that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of personal health information, including:

- The linkage of records of personal health information solely in the custody of the prescribed person or prescribed entity for the exclusive use of the linked records of personal health information by the prescribed person or prescribed entity;

- The linkage of records of personal health information in the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for the exclusive use of the linked records of personal health information by the prescribed person or prescribed entity;

- The linkage of records of personal health information solely in the custody of the prescribed person or prescribed entity for purposes of disclosure of the linked records of personal health information to another person or organization; and

- The linkage of records of personal health information in the custody of the prescribed person or prescribed entity with records of personal health information to be collected from another person or organization for purposes of disclosure of the linked records of personal health information to that other person or organization.

### *Review and Approval Process*

The policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request to link records of personal health information and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must also address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to link records of personal health information.

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

### *Conditions or Restrictions on the Approval*

Where the linked records of personal health information will be disclosed by the prescribed person or prescribed entity to another person or organization, the policy and procedures must require that the disclosure be approved pursuant to the *Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* or the *Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research,* as may be applicable.

Where the linked records of personal health information will be used by the prescribed person or prescribed entity, the policy and procedures must require that the use be approved pursuant to the *Policy and Procedures for the Use of Personal Health Information for Research* or the *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information,* as may be applicable. The policy and procedures must further require that the linked records of personal health information be de-identified and/or aggregated as soon as practicable pursuant to the *Policy and Procedures with Respect to De-Identification and Aggregation* and that, to the extent possible, only de-identified and/or aggregate information be used by agents of the prescribed person or prescribed entity.

### *Process for the Linkage of Records of Personal Health Information*

The policy and procedures must outline the process to be followed in linking records of personal health information, the manner in which the linkage of records of personal health information must be conducted and the agent(s) responsible for linking records of personal health information when approved in accordance with this policy and its procedures.

### *Retention*

The policy and procedures must require that linked records of personal health information be retained in compliance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information* until they are de-identified and/or aggregated pursuant to the *Policy and Procedures with Respect to De-Identification and Aggregation*.

### *Secure Disposal*

The policy and procedures must address the secure disposal of records of personal health information linked by the prescribed person or prescribed entity and, in particular, must require that the records of personal health information be securely disposed of in compliance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information*.

### *Compliance, Audit and Enforcement*

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the

agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

### *Tracking Approved Linkages of Records of Personal Health Information*

The policy and procedures must require that a log be maintained of the linkages of records of personal health information approved by the prescribed person or prescribed entity and must identify the agent(s) responsible for maintaining such a log. It is also recommended that the policy and procedures address where documentation related to the receipt, review, approval or denial of requests to link records of personal health information will be retained and the agent(s) responsible for retaining this documentation.

## 23. Log of Approved Linkages of Records of Personal Health Information

A prescribed person or prescribed entity, as the case may be, must maintain a log of linkages of records of personal health information approved by the prescribed person or prescribed entity. At a minimum, the log must include the name of the agent, person or organization who requested the linkage; the date that the linkage of records of personal health information was approved; and the nature of the records of personal health information linked.

## 24. Policy and Procedures with Respect to De-Identification and Aggregation

A policy and procedures must be developed and implemented with respect to de-identification and aggregation. The policy and procedures must require that personal health information not be used or disclosed if other information, namely de-identified and/or aggregate information, will serve the identified purpose.

The policy of the prescribed person or prescribed entity with respect to cell-sizes of less than five and the exceptions thereto must also be articulated. In articulating the policy with respect to cell-sizes of less than five, regard must be had to the restrictions related to cell-sizes of less than five contained in Data Sharing Agreements, Research Agreements and written research plans pursuant to which the personal health information was collected by the prescribed person or prescribed entity.

The policy and procedures must provide a definition of de-identified information and aggregate information that identifies the meaning ascribed to each of these terms. The definitions adopted and the policy of the prescribed person or prescribed entity with respect to cell-sizes of less than five shall have regard to, and must be consistent with, the meaning of “identifying information” in subsection 4(2) of the *Act*.

The information that must be removed, encrypted and/or truncated in order to constitute de-identified information and the manner in which the information must be grouped, collapsed or averaged in order to constitute aggregate information must also be identified. The policy and procedures shall also address the agent(s) responsible for de-identifying and/or aggregating information and the procedure to be followed in this regard.

Further, the policy and procedures must require de-identified and/or aggregate information, including information of cell-sizes of less than five, to be reviewed prior to use or disclosure in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for conducting this review shall also be identified.

The process to be followed in reviewing the de-identified and/or aggregate information and the criteria to be used in assessing the risk of re-identification shall also be set out. In establishing the criteria to be used in assessing the risk of re-identification, the prescribed person or prescribed entity shall have regard to the type of identifying information available, including information that can be used to identify an individual directly (e.g., name, address, health card number) or indirectly (e.g., date-of-birth, postal code, gender).

It is recommended that the prescribed person or prescribed entity explore new tools that are being developed to assist in ensuring that the policy and procedures developed with respect to de-identification and aggregation are based on an assessment of the actual risk of re-identification.

The policy and procedures must also prohibit agents from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. The policy and procedures must also identify the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for*

*Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 25. 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, it is recommended that the policy and procedures ensure that prescribed persons or prescribed entities conduct privacy impact assessments on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated.

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 agent(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 data holdings involving personal health information and new or changes to existing information systems, technologies or programs involving personal health information, the policy and procedures must require that privacy impact assessments be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving personal health information, the policy and procedures must require that a timetable be developed to ensure privacy impact assessments are conducted and the policy and procedures must identify the agent(s) responsible for developing the timetable.

Once privacy impact assessments have been completed, the policy and procedures shall require that they be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of the prescribed person or prescribed entity. The policy and procedures must also identify the circumstances in which and the frequency with which privacy impact assessments are required to be reviewed.

The policy and procedures must also identify the agent(s) responsible and the process that must be followed in identifying when privacy impact assessments are required; in identifying when privacy impact assessments are required to be reviewed in accordance with the policy and procedures; in ensuring that privacy impact assessments are conducted and completed; and in ensuring that privacy impact assessments are reviewed and amended, if necessary. The role of

agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified in respect of privacy impact assessments.

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 data holding, information system, technology or program at issue;
- The nature and type of personal health information collected, used or disclosed or that is proposed to be collected, used or disclosed;
- The sources of the personal health information;
- The purposes for which the personal health information is collected, used or disclosed or is proposed to be collected, used or disclosed;
- The reason that the personal health information is required for the purposes identified;
- The flows of the personal health information;
- The statutory authority for each collection, use and disclosure of personal health information identified;
- The limitations imposed on the collection, use and disclosure of the personal health information;
- Whether or not the personal health information is or will be linked to other information;
- The retention period for the records of personal health information;
- The secure manner in which the records of personal health information are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the personal health information and the functionality to audit logs for unauthorized use or disclosure;
- The risks to the privacy of individuals whose personal health information is or will be part of the data holding, information system, technology or program and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- 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 agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations, is also required to be outlined.

The policy 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 agent(s) responsible for maintaining such a log.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

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*, published by the Information and Privacy Commissioner of Ontario.

## 26. Log of Privacy Impact Assessments

A prescribed person or prescribed entity shall maintain a log of privacy impact assessments that have been completed and of privacy impact assessments that have been undertaken but that have not been completed. The log shall describe the data holding, information system, technology or program involving personal health information that is at issue; the date that the privacy impact assessment was completed or is expected to be completed; the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment; the recommendations arising from the privacy impact assessment; the agent(s) responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

A prescribed person or prescribed entity shall also maintain a log of data holdings involving personal health information and of new or changes to existing information systems, technologies or programs involving personal health information for which privacy impact assessments have not been undertaken. For each such data holding, information system, technology or program, the log shall either set out the reason that a privacy impact assessment will not be undertaken and the agent(s) responsible for making this determination or set out the date that the privacy impact

assessment is expected to be completed and the agent(s) responsible for completing or ensuring the completion of the privacy impact assessment.

## 27. 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. At a minimum, the audits required to be conducted shall include audits to assess compliance with the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and audits of the agent(s) permitted to access and use personal health information pursuant to *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*.

With respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the agent(s) responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures shall require a privacy audit schedule to be developed and shall identify the agent(s) responsible for developing the privacy audit schedule.

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

The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.

The policy 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 agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.

The policy 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 agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer or the Executive Director.

The policy and procedures must further require that a log be maintained of privacy audits and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They should further address where documentation related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.

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

## 28. Log of Privacy Audits

A prescribed person or prescribed entity shall maintain a log of privacy audits that have been completed. The log shall set out the nature and type of the privacy audit conducted; the date that the privacy audit was completed; the agent(s) responsible for completing the privacy audit; the recommendations arising from the privacy audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

## 29. 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.

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 not in compliance with the *Act* or its regulation;
- A contravention of the privacy policies, procedures or practices implemented by the prescribed person or prescribed entity;

- A contravention of Data Sharing Agreements, Research Agreements, Confidentiality Agreements and Agreements with Third Party Service Providers retained by the prescribed person or prescribed entity; and

- Circumstances where personal health information is stolen, lost or subject to unauthorized use or disclosure or where records of personal health information are subject to unauthorized copying, modification or disposal.

The policy and procedures shall impose a mandatory requirement on agents to notify the prescribed person or prescribed entity of a privacy breach or suspected privacy breach.

In this regard, the policy and procedures shall identify the agent(s) who must be notified of the privacy breach or suspected privacy breach and shall provide contact information for the agent(s) who must be notified. The policy 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, the policy and procedures shall require a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, personal health information has been breached. The agent(s) responsible for making this determination must also be identified.

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

The policy and procedures shall also require that containment be initiated immediately and shall identify the agent(s) responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation.

In undertaking containment, the policy and procedures must ensure that reasonable steps are taken in the circumstances to protect personal health information from further theft, loss or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal. At a minimum, these steps shall include ensuring that no copies of the records of personal health information have been made and ensuring that the records of personal health information are either retrieved or disposed of in a secure manner. Where the records of personal health information are securely disposed of, written confirmation should be obtained related to the date, time and method of secure disposal. These steps 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 any other information and, if necessary, taking further action to prevent additional privacy breaches.

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

The policy and procedures must require the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, the policy and procedures shall set out the agent(s) responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that must be provided upon notification. At a minimum, the policy and procedures must require the health information custodian or other organization to be advised of the extent of the privacy breach, the nature of the personal health information at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. As a secondary collector of personal health information, a prescribed person or prescribed entity should not directly notify the individual to whom the personal health information relates of a privacy breach. The required notification shall be provided by the health information custodian.

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 agent(s) responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

The policy and procedures must further identify the agent(s) responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy breach. This shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also identify the agent(s) responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy 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 agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director.

In addition, 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.

Further, the policy and procedures must require that a log be maintained of privacy breaches and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. They should further address where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained and the agent(s) responsible for retaining this documentation.

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

In developing the policy and procedures, it is recommended that the prescribed person or prescribed entity have regard to the guidelines produced by the Information and Privacy Commissioner of Ontario entitled *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*.

## 30. Log of Privacy Breaches

A prescribed person or prescribed entity shall maintain a log of privacy breaches setting out:

- The date of the privacy breach;

- The date that the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external;
- The nature of the personal health information that was the subject matter of the privacy breach and the nature and extent of the privacy breach;
- The date that the privacy breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity was notified;
- The date that the investigation of the privacy breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

## 31. 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. A definition of the term "privacy complaint" shall be provided that, at a minimum, includes concerns or complaints relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.

The information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy concerns or complaints shall also be identified. At a minimum, the name and/or title, mailing address and contact information of the agent(s) to whom concerns or complaints may be directed and information related to the manner in which and format in which privacy concerns or complaints may be directed to the prescribed person or prescribed entity should be made publicly available. It is also recommended that individuals be advised that they may make a complaint regarding compliance with the *Act* and its regulation to the Information and Privacy Commissioner of Ontario and that the mailing address and contact information for the Information and Privacy Commissioner of Ontario be provided.

The policy and procedures must further establish the process to be followed in receiving privacy complaints. This shall include any documentation that must be completed, provided and/or executed by the individual making the privacy complaint; the agent(s) responsible for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint.

Upon receipt of a privacy complaint, the policy and procedures shall require a determination to be made of whether or not the privacy complaint will be investigated. In this regard, the policy and procedures shall identify the agent(s) responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation.

In the event that it is determined that an investigation will not be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the prescribed person or prescribed entity has contravened or is about to contravene the *Act* or its regulation; and providing contact information for the Information and Privacy Commissioner of Ontario.

In the event that it is determined that an investigation will be undertaken, the policy and procedures must require that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; advising that an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.

The policy and procedures must identify the agent(s) responsible for sending the above noted letters to the individuals making privacy complaints and the time frame within which the letters will be sent to the individuals.

Where an investigation of a privacy complaint will be undertaken, the policy and procedures must identify the agent(s) responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. This shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified in the policy and procedures.

The process for addressing the recommendations arising from the investigation of privacy complaints and the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations and for monitoring and ensuring the implementation of the recommendations shall also be addressed in the policy and procedures. The policy and procedures must also set out the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, including the agent(s) responsible for completing, preparing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy 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 agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the Chief Executive Officer or the Executive Director.

The policy 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 Information and Privacy Commissioner of Ontario if there are reasonable grounds to believe that the *Act* or its regulation has been or is about to be contravened. The contact information for the Information and Privacy Commissioner of Ontario shall also be provided. The agent(s) responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided, shall also be addressed.

The policy and procedures should also address whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the manner by which, the format in which and the time frame within which the notification must be provided and the agent(s) responsible for providing the notification.

Further, the policy and procedures must require that a log be maintained of privacy complaints and must identify the agent(s) responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. They should further address where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained and the agent(s) responsible for retaining this documentation.

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the

agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Breach Management* shall also be addressed.

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

## 32. Log of Privacy Complaints

A prescribed person or prescribed entity shall maintain a log of privacy complaints received that, at a minimum, sets out:

- The date that the privacy complaint was received and the nature of the privacy complaint;
- The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;
- The date that the individual making the complaint was advised that the complaint will not be investigated and was provided a response to the complaint;
- The date that the individual making the complaint was advised that the complaint will be investigated;
- The agent(s) responsible for conducting the investigation;
- The dates that the investigation was commenced and completed;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.

## 33. 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. A definition of

the term “privacy inquiry” shall be provided that, at a minimum, includes inquiries relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and related to the compliance of the prescribed person or prescribed entity with the *Act* and its regulation.

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 agent(s) to whom privacy inquiries may be directed; information relating to the manner in which privacy inquiries may be directed to the prescribed person or prescribed entity; and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity.

The policy and procedures must further establish the process to be followed in receiving and responding to privacy inquiries. This shall include the agent(s) responsible for receiving and responding to privacy inquiries; any documentation that must be completed, provided and/or executed; the required content of the documentation; and the format and content of the response to the privacy inquiry. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Complaints* and the *Policy and Procedures for Privacy Breach Management* shall also be addressed.

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

## Part 2 – Security Documentation

### 1. Information Security Policy

An overarching information security policy, or equivalent, must be developed and implemented in relation to personal health information received by the prescribed person or prescribed entity under the *Act*. The information security policy must require that steps be taken that are reasonable in the circumstances to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal.

The information security policy must also require the prescribed person or prescribed entity to undertake comprehensive and organization-wide threat and risk assessments of all information security assets, including personal health information, as well as appropriate project specific threat and risk assessments. 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.

The information security policy shall 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 agents 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;
- 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 monitoring, including policies and procedures for maintaining and reviewing system control and audit logs and 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 are set out in this Manual.

The information security policy shall also outline the information security infrastructure implemented by the prescribed person or prescribed entity 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.

In addition, 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 data holdings containing personal health information.

The prescribed person or prescribed entity must require agents to comply with this policy and with all other security policies, procedures and practices implemented by the prescribed person or prescribed entity and must address how and by whom compliance will be enforced and the consequences of breach. In this regard, 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 agent(s) responsible for conducting the audit and for ensuring compliance with the policy.

The policy must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or 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 person or prescribed entity. The purpose of the review is to determine whether amendments are needed or whether new security policies, procedures and practices are required.

The policy and procedures must identify the frequency of the review, the agent(s) responsible for undertaking the review, the procedure to be followed in undertaking the review and the time frame in which the review will be undertaken. At a minimum, the security policies, procedures and practices implemented by the prescribed person or prescribed entity must be reviewed on an annual basis. The policy and procedures must also identify the agent(s) 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 agent(s) responsible and the procedure that must be followed in obtaining approval of any amended 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, the prescribed person or prescribed entity must have regard to any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; evolving industry security standards and best practices; technological advancements; amendments to the *Act* and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. It must also take into account whether the security policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices and whether there is consistency between and among the security and privacy policies, procedures and practices implemented.

The policy and associated procedures must further identify the agent(s) responsible and the procedure to be followed in communicating the amended or newly developed security policies, procedures and practices, including the method and nature of the communication. It shall also identify the agent(s) responsible for and the procedure to be followed in reviewing and amending the communication materials available to the public and other stakeholders as a result of the amended or newly developed security policies, procedures and practices.

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be

audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

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*.

## 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 implemented by the prescribed person or prescribed entity to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

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.

It is recommended that the premises of the prescribed person or prescribed entity be divided into varying levels of security with each successive level being more secure and restricted to fewer individuals. It is further recommended 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.

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

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

### *Policy, Procedures and Practices with Respect to Access by Agents*

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 agent(s) responsible for receiving, reviewing, granting and terminating access by agents 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. The process to be followed and the requirements that must be satisfied shall also be identified, including any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy and procedures must further address the criteria that must be considered by the agent(s) 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 agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, the policy and procedures must establish a process 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 by the agent(s) responsible for making the determination; and the required content of the documentation.

The policy and procedures must also address the agent(s) 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. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

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

The policy and procedures shall require agents to notify the prescribed person or prescribed entity 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. This shall include a discussion of the agent(s) 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; and the required content of the documentation.

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 agent(s) responsible for implementing these safeguards shall also be outlined.

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 agent(s) responsible for their issuance. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for

completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; the required content of the documentation; the agent(s) 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 agent(s) responsible for implementing the process and the time frame within which the process must be implemented, shall also be addressed.

### Termination of the Employment, Contractual or Other Relationship

The policy and procedures shall require agents, as well as their supervisors, to notify the prescribed person or prescribed entity of the termination of their employment, contractual or other relationship with the prescribed person or prescribed entity and to return their identification cards, access cards and/or keys to the prescribed person or prescribed entity on or before the date of termination 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 agent 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 person or prescribed entity when the agent no longer requires such access.

The policy and procedures shall identify the agent(s) 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 agent(s) 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 Agents with Access to the Premises

Audits must be conducted of agents with access to the premises of the prescribed person or prescribed entity and to locations within the premises where records 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 agents granted access to the premises and to locations within the premises where records of personal health information are retained continue to have an employment, contractual or other relationship with the prescribed person or prescribed entity and continue to require the same level of access.

In this regard, the policy and procedures must identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, 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 agents granted approval to access the premises of the prescribed person or prescribed entity and to locations within the premises where records of personal health information are retained and must identify the agent(s) 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 agent(s) responsible for maintaining this documentation.

### *Policy, Procedures and Practices with Respect to Access by Visitors*

The policy and procedures must address the agent(s) responsible and the process to be followed in identifying, screening and supervising visitors to the premises of the prescribed person or prescribed entity. 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 agent(s) responsible for identifying, screening and supervising visitors; and the documentation that must be completed, provided and/or 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 agent(s) with whom the visitors are meeting.

The duties of agent(s) 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 person or prescribed entity; 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 agent(s) 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 agent(s) responsible for retaining this documentation.

## 4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

A log must be maintained of agents granted approval to access the premises of the prescribed person or prescribed entity and the level of access granted. At a minimum, the log must include

the name of the agent granted approval to access the premises; 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 agent; 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 person or prescribed entity, 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 in paper and electronic format.

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. For records of personal health information used for research purposes, the prescribed person or prescribed entity must ensure that the records of personal health information are not being retained for a period longer than that set out in the written research plan approved by a research ethics board. For records of personal health information collected pursuant to a Data Sharing Agreement, the policy and procedures must prohibit the records from being retained for a period longer than that set out in the Data Sharing Agreement. In any event, the policy and procedures must mandate that records of personal health information be retained for only as long as necessary to fulfill the purposes for which the personal health information was collected.

The policy and procedures must also require the records of personal health information to be retained in a secure manner and must identify the agent(s) 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 agents of the prescribed person or prescribed entity to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that must be taken by agents shall also be outlined in the policy and procedures.

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

The policy and procedures must address the circumstances in which and the purposes for which records of personal health information will be transferred to the third party service provider for secure retention. They must detail the procedure to be followed in securely transferring the records of personal health information to the third party service provider 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 agent(s) 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.*

Further, 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 agent(s) 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 upon 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 person or prescribed entity and must identify the agent(s) responsible for maintaining the detailed inventory.

Further, where a third party service provider is contracted to retain records of personal health information, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the *Template Agreement For All Third Party Service Providers*, and must identify the agent(s) responsible for ensuring that the agreement has been executed prior to transferring the records of personal health information for secure retention.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 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 person or prescribed entity permits personal health information 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, it is recommended that the prescribed person or prescribed entity have regard to orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace*.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

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

If the prescribed person or prescribed entity permits personal health information to be retained on a mobile device, the policy and procedures must set out 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 process that must be followed and the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the retention of personal health information on a mobile device. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must further address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny 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 agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose 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 agent(s) 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 Limiting Agent Access to Personal Health Information*.

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 agent(s) 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 agents granted approval to retain personal health information on a mobile device must comply. At a minimum, the agents 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;

- 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 agents to protect the personal health information retained on a mobile device against theft, loss and unauthorized use or disclosure and to protect the records of personal health information retained on a mobile device against unauthorized copying, modification or disposal.

The policy and procedures must also require agents 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 person or prescribed entity 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 may be accessed remotely through a secure connection or virtual private network.

If the prescribed person or prescribed entity permits personal health information to be accessed remotely, the policy and procedures must set out 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 process that must be followed and the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to personal health information. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must further address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for remote access.

At a minimum, prior to any approval of a request to remotely access personal health information, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose 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 agent(s) 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 Limiting Agent Access to Personal Health Information*.

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 agents granted approval to access personal health information remotely must comply. At a minimum, the agents 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 agents in remotely accessing personal health information.

## 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 in paper and electronic format.

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 person or prescribed entity. The policy and procedures shall require agents to use the approved methods of transferring records of personal health information and shall prohibit all other methods.

The procedures that must be followed in transferring records of personal health information through each of the approved methods must also be outlined. This shall include a discussion of the conditions pursuant to which records of personal health information will be transferred; the agent(s) 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 agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

The policy and procedures must also address whether the agent 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 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 agent(s) responsible for doing so.

The administrative, technical and physical safeguards that must be implemented by agents in transferring records of personal health information through each of the approved methods must also be outlined in order to ensure that the records of personal health information are transferred in a secure manner.

The prescribed person or prescribed entity must ensure that 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 are consistent with:

- Orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including but not limited to Order HO-004 and Order HO-007;
- Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including *Privacy Protection Principles for Electronic Mail Systems* and *Guidelines on Facsimile Transmission Security*; and
- Evolving privacy and security standards and best practices.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 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 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. The policy and procedures must further 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 in paper and electronic format must be securely disposed of, the prescribed person or prescribed entity must ensure that the method of secure disposal adopted is consistent with the *Act* and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*.

The policy and procedures must further address the secure retention of records of personal health information pending their secure disposal in accordance with the *Policy and Procedures for Secure Retention of Records of Personal Health Information*. 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 must also identify the agent(s) responsible for ensuring the secure retention of records of personal health information pending their 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 agent, who is not a third party service provider, the policy and procedures must identify the designated agent responsible for securely disposing of the records of personal health information; the responsibilities of the designated agent 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 agent 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 agent(s) who performed the secure disposal.

The time frame within which and the agent(s) 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 an agent 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 person or prescribed entity 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 agent(s) 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 agent(s) responsible for ensuring the secure transfer of records of personal health information to document the date, time and mode of transfer of the records of personal health information 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 agent(s) responsible for maintaining this inventory.

Further, where a third party service provider is retained to securely dispose of records of personal health information, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the *Template Agreement For All Third Party Service Providers*, and must identify the agent(s) 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, whether from the third party service provider or from the designated agent that is not a third party service provider, and the agent(s) 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 agent(s) responsible for implementing this process.

It is also recommended that the policy and procedures address where certificates of destruction will be retained and the agent(s) responsible for retaining the certificates of destruction.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 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 regardless of whether they are owned, leased or operated by the prescribed person or prescribed entity.

The policy and procedures must identify the required minimum and maximum length of the password, the standard mandated for password composition and any other restrictions imposed on passwords, such as re-use of prior passwords and the use of passwords that resemble prior passwords. At a minimum, passwords must be comprised of a combination of upper and lower case letters as well as numbers and non-alphanumeric characters.

The time frame within which passwords will automatically expire, the frequency with which passwords must be changed, the consequences arising from a defined number of failed log-in attempts and the imposition of a mandatory system-wide password-protected screen saver after a defined period of inactivity must also be addressed.

The policy and procedures shall further identify the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords in order to ensure that the personal health information 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, agents 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 agent. Agents must also be prohibited from writing down, displaying, concealing, hinting at, providing, sharing or otherwise making their password known to any other individual, including another agent of the prescribed person or prescribed entity.

The prescribed person or prescribed entity must ensure that the policy and procedures it has developed in this regard, are consistent with any orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; with any guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; and with evolving privacy and security standards and best practices.

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the

agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 10. 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 that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the personal health information maintained, with the number and nature of agents with access to personal health information and with the threats and risks associated with the personal health information.

The policy and procedures shall require the prescribed person or prescribed entity to ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information.

The policy and procedures shall also set out the types of events that are required to be audited and the nature and scope of the information that must be contained in system control and audit logs. It is recommended that the system control and audit logs set out the date and time that personal health information is accessed; the date and time of the disconnection; the nature of the disconnection; the name of the user accessing personal health information; the network name or identification of the computer through which the connection is made; and the operations or actions that create, amend, delete or retrieve personal health information including the nature of the operation or action, the date and time of the operation or action, the name of the user that performed the action or operation and the changes to values, if any.

The agent(s) responsible for ensuring that the types of events that are required to be audited are in fact audited and that the nature and scope of the information that is required to be contained in system control and audit logs is in fact logged shall also be identified.

The policy and procedures shall require the system control and audit logs to be immutable, that is, the prescribed person or prescribed entity 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 agent(s) responsible for implementing these procedures.

The policy and procedures shall also identify the length of time that system control and audit logs are required to be retained, the agent(s) responsible for retaining the system control and audit logs and where the system control and audit logs will be retained.

The review of system control and audit logs must also be addressed, including the agent(s) responsible for reviewing the system control and audit logs, the frequency with which and the circumstances in which system control and audit logs are required to be reviewed and the process to be followed in conducting the review.

The agent(s) responsible for reviewing system control and audit logs shall be required to notify the prescribed person or prescribed entity, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Management* and/or of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management*. The relationship between this policy and its procedures and the *Policy and Procedures for Privacy Breach Management* and the *Policy and Procedures for Information Security Breach Management* must also be identified.

Further, the policy and procedures must address the findings arising from the review of system control and audit logs, including the agent(s) responsible for assigning other agent(s) 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 policy and procedures shall also set out the nature of the documentation, if any, that must be completed, provided and/or executed following the review of system control and audit logs; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; the time frame within which the documentation must be provided; and the required content of the documentation.

The manner and format for communicating the findings of the review and how the findings have been or are being addressed must also be outlined. This shall include a discussion of the agent(s) responsible for communicating the findings of the review of system control and audit logs; the mechanism and format for communicating the findings of the review; the time frame within which the findings of the review must be communicated; and to whom the findings of the review must be communicated.

Further, the policy and procedures must set out the process to be followed in tracking that the findings of the review of system control and audit logs have been addressed within the identified timelines, including the agent(s) responsible for tracking that the findings have been addressed.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for*

*Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 11. Policy and Procedures for Patch Management

A policy and procedures must be developed and implemented for patch management.

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

The agent(s) 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 agent(s) responsible for undertaking this analysis and making this determination.

In circumstances where a determination is made that the patch should not be implemented, the policy and procedures shall require the responsible agent(s) 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 agent(s) responsible for determining the time frame for implementation of the patch and the priority of the patch. The policy and procedures shall also set out the criteria upon which these determinations are to be made, the process by which these determinations are to be made and the documentation that must be completed, provided and/or executed in this regard.

The policy and procedures shall also set out the process for patch implementation, including the agent(s) responsible for patch implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for patch implementation.

The circumstances in which patches must be tested, the time frame within which patches must be tested, the procedure for testing and the agent(s) responsible for testing shall also be addressed, including the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

The policy and procedures must also require documentation to be maintained in respect of patches that have been implemented and must identify the agent(s) 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 agent(s) responsible for implementing the

patch; the date, if any, when the patch was tested; the agent(s) responsible for testing; and whether or not the testing was successful.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 12. Policy and Procedures Related to Change Management

A policy and procedures must be developed and implemented for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment of the prescribed person or prescribed entity.

The policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment and the process that must be followed and the requirements that must be satisfied in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. At a minimum, the documentation shall describe the change requested, the rationale for the change, 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 agent(s) 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 agent(s) to document the change to the operational environment requested, the name of the agent 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 agent(s) 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 criteria upon which these determinations are to be made, the process by which these determinations are to be made and any documentation that must be completed, provided and/or executed in this regard.

The policy and procedures shall also set out the process for implementation of the change to the operational environment, including the agent(s) responsible for implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for implementation.

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 agent(s) responsible for testing shall also be addressed in the policy and procedures, including the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

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

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 13. 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.

The policy and procedures shall identify the nature and types of back-up storage devices maintained by the prescribed person or prescribed entity; the frequency with which records of personal health information are backed-up; the agent(s) 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. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures shall also address testing the procedure for back-up and recovery of records of personal health information, the agent(s) responsible for testing, the frequency with which the procedure is tested and the process that must be followed in conducting such testing. This shall include a discussion of any documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

The policy and procedures shall further identify the agent(s) responsible for ensuring that back-up storage devices containing records of personal health information are retained in a secure manner, 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 agent(s) responsible for ensuring that they are retained in a secure manner.

Additionally, if a third party service provider is contracted 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 agent(s) 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 agent(s) 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 upon receipt of the backed-up records of personal health information.

Also, where a third party service provider is contracted to retain backed-up records of personal health information, the policy and procedures must require that a written agreement be executed

with the third party service provider containing the relevant language from the *Template Agreement For All Third Party Service Providers* and must identify the agent(s) 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.

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.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 14. 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 regardless of whether they are owned, leased or operated by the prescribed person or prescribed entity.

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 agent(s) responsible for receiving, reviewing and determining whether to approve or deny the request and the process that must be followed and the requirements that must be satisfied in this regard. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request shall also be identified.

The policy and procedures must also identify the conditions or restrictions with which agents granted approval must comply.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 15. 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 person or prescribed entity; threat and risk assessments; security reviews or assessments; vulnerability assessments; penetration testing; ethical hacks and reviews of system control and audit logs.

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 agent(s) 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 agent(s) 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also set out the process that must be followed in addressing the recommendations arising from security audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.

The policy 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, including the agent(s) responsible for completing, providing and/or executing the documentation, the required content of the documentation and the agent(s) to whom the documentation must be provided.

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 agent(s) 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 agent(s) 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 agent(s) responsible for retaining this documentation.

The policy and procedures must also require the agent(s) responsible for conducting the security audit to notify the prescribed person or prescribed entity, 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*.

## 16. Log of Security Audits

A prescribed person or prescribed entity shall maintain a log of 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 agent(s) responsible for completing the security audit; the recommendations arising from the security audit; the agent(s) responsible for addressing each recommendation; the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

## 17. 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 and 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 person or prescribed entity.

The policy and procedures shall impose a mandatory requirement on agents to notify the prescribed person or prescribed entity of an information security breach or suspected information security breach.

In this regard, the policy and procedures shall identify the agent(s) who must be notified of the information security breach or suspected information security breach and shall provide contact information for the agent(s) 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, the policy and procedures shall require a determination to be made 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 agent(s) responsible for making these determinations must also be identified.

The policy and procedures must address the process to be followed where the breach is a privacy breach as well as an information security breach and when the breach is reported as an information security breach but is determined to be a privacy breach.

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

The policy and procedures shall also require that containment be initiated immediately and shall identify the agent(s) responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation. 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 agent(s) 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 by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The policy and procedures must require the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, the policy and procedures shall set out the agent(s) responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that will be provided upon notification. At a minimum, the policy and procedures must require the health information custodian or other organization 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 agent(s) responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification

The policy and procedures must further identify the agent(s) 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. This shall include a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.

The policy and procedures shall also identify the agent(s) responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. 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, including the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The policy 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 agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the Chief Executive Officer or the Executive Director.

Further, the policy and procedures must require that a log be maintained of information security breaches and must identify the agent(s) 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 agent(s) responsible for retaining this documentation.

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

## 18. Log of Information Security Breaches

A prescribed person or prescribed entity 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;
- 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 date that the information security breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to the prescribed person or prescribed entity was notified, if applicable;

- The date that the investigation of the information security breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

## Part 3 – Human Resources Documentation

### 1. Policy and Procedures for Privacy Training and Awareness

A policy and procedures must be developed and implemented requiring agents of the prescribed person or prescribed entity to attend initial privacy orientation as well as ongoing privacy training.

The policy and procedures shall set out the time frame within which agents must complete the initial privacy orientation as well as address the frequency of ongoing privacy training. At a minimum, the policy and procedures shall require an agent to complete the initial privacy orientation prior to being given access to personal health information and to attend ongoing privacy training provided by the prescribed person or prescribed entity on an annual basis.

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

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

- A description of the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal health information collected and from whom this information is typically collected;
- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the *Act* and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of the privacy policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the privacy policies, procedures and practices implemented;

- An explanation of the privacy program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the privacy program;

- The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;

- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity;

- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and

- An explanation of the *Policy and Procedures for Privacy Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.

The policy and procedures shall also require the ongoing privacy training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and to have regard to any recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints.

The policy and procedures must require that a log be maintained to track attendance at the initial privacy orientation as well as the ongoing privacy training and the policy and procedures must identify the agent(s) responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial privacy orientation as well as the ongoing privacy training shall also be outlined, including the documentation that must be completed, provided and/or executed to verify attendance; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation. The procedure to be followed and the agent(s) responsible for identifying agent(s) who do not attend the initial privacy orientation or the ongoing privacy training and for ensuring that such agent(s) attend the initial privacy orientation and the ongoing privacy training shall also be identified, including the time frame following the date of the privacy orientation or the 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 privacy orientation and the ongoing privacy training is to be retained and the agent(s) responsible for retaining this documentation.

The policy and procedures shall also discuss the other mechanisms implemented by the prescribed person or prescribed entity to foster a culture of privacy and to raise awareness of the privacy program and the privacy policies, procedures and practices implemented. The policy and procedures shall also discuss the frequency with which the prescribed person or prescribed entity communicates with its agents in relation to privacy, the method and nature of the communication and the agent(s) responsible for the communication.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

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*.

## 2. Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training

A prescribed person or prescribed entity shall maintain a log of the attendance of agents at the initial privacy orientation and ongoing privacy training. At a minimum, the log must set out the name of the agent, the date that the agent attended the initial privacy orientation and the dates that the agent attended ongoing privacy training.

## 3. Policy and Procedures for Security Training and Awareness

A policy and procedures must be developed and implemented requiring agents of the prescribed person or prescribed entity to attend initial security orientation as well as ongoing security training.

The policy and procedures shall set out the time frame within which agents must complete the initial security orientation as well as address the frequency of ongoing security training. At a minimum, the policy and procedures shall require an agent to complete the initial security orientation prior to being given access to personal health information and to attend ongoing security training provided by the prescribed person or prescribed entity on an annual basis.

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

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

- An overview of the security policies, procedures and practices that have been implemented by the prescribed person or prescribed entity and the obligations arising from these policies, procedures and practices;

- 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 agent(s) that have been delegated day-to-day authority to manage the security program;

- The administrative, technical and physical safeguards implemented by the prescribed person or prescribed entity to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;

- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by the prescribed person or prescribed entity; and

- An explanation of the *Policy and Procedures for Information Security Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

The policy and procedures shall also require the ongoing security training to be formalized and standardized; to include role-based training in order to ensure that agents understand how to apply the security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new security policies, procedures and practices and significant amendments to existing security policies, procedures and practices; and to have regard to any recommendations with respect to security training made in privacy impact assessments, the investigation of information security breaches and the conduct of security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.

The policy and procedures must require that a log be maintained to track attendance at the initial security orientation as well as the ongoing security training and the policy and procedures must identify the agent(s) responsible for maintaining such a log and tracking attendance.

The process to be followed in tracking attendance at the initial security orientation 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom this documentation must be provided; and the required content of the documentation. The procedure to be followed and the agent(s) responsible for identifying agent(s) who do not attend the initial security orientation or the ongoing security training and for ensuring that such agent(s) attend the initial security orientation and the ongoing security training shall also be identified, including the time frame following the date of the security orientation or the 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 orientation and the ongoing security training will be retained and the agent(s) responsible for retaining this documentation.

The policy and procedures shall also discuss the other mechanisms implemented by the prescribed person or prescribed entity to raise awareness of the security program and the security policies, procedures and practices implemented. The policy and procedures shall also discuss the frequency with which the prescribed person or prescribed entity communicates with its agents in relation to information security, the method and nature of the communication and the agent(s) responsible for the communication.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

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*.

## 4. Log of Attendance at Initial Security Orientation and Ongoing Security Training

A prescribed person or prescribed entity shall maintain a log of the attendance of agents at the initial security orientation and ongoing security training. At a minimum, the log must set out the name of the agent, the date that the agent attended the initial security orientation and the dates that the agent attended ongoing security training.

## 5. Policy and Procedures for the Execution of Confidentiality Agreements by Agents

A policy and procedures must be developed and implemented requiring agents to execute a Confidentiality Agreement in accordance with the *Template Confidentiality Agreement with Agents* at the commencement of their employment, contractual or other relationship with the prescribed person or prescribed entity and prior to being given access to personal health information. It is further recommended that the policy and procedures require that a Confidentiality Agreement be executed by agents on an annual basis and identify the time frame each year in which the Confidentiality Agreement is required to be executed.

The policy and procedures must further identify the agent(s) responsible for ensuring that a Confidentiality Agreement is executed with each agent of the prescribed person or prescribed entity at the commencement of the employment, contractual or other relationship and thereafter on an annual basis and the process that must be followed in this regard.

In particular, the policy and procedures shall outline the process that must be followed in notifying the responsible agent(s) each time an agent has commenced or will commence an employment, contractual or other relationship with the prescribed person or prescribed entity. This shall include a discussion of the agent(s) responsible for providing notification, the time frame within which notification must be provided and the format of the notification.

The policy and procedures shall also outline the process that must be followed by the responsible agent(s) in tracking the execution of Confidentiality Agreements, including the process that must be followed where an executed Confidentiality Agreement is not received within a defined period of time following the commencement of the employment, contractual or other relationship or within a defined period of time following the date that the Confidentiality Agreement is required to be executed on an annual basis.

The policy and procedures shall also require that a log be maintained of executed Confidentiality Agreements and must identify the agent(s) responsible for maintaining such a log. It is also recommended that the policy and procedures address where documentation related to the execution of Confidentiality Agreements will be retained and the agent(s) responsible for retaining this documentation.

The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance with the policy and its procedures and with the Confidentiality Agreement will be audited in accordance

with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and its procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 6. Template Confidentiality Agreement with Agents

A Confidentiality Agreement must be executed by each agent of the prescribed person or prescribed entity in accordance with the *Policy and Procedures for the Execution of Confidentiality Agreements by Agents* that, at a minimum, addresses the matters set out below.

### *General Provisions*

The Confidentiality Agreement must describe the status of the prescribed person or prescribed entity under the *Act* and the duties and responsibilities arising from this status. It must also state that individuals executing the agreement are agents of the prescribed person or prescribed entity in respect of personal health information and must outline the responsibilities associated with this status.

The Confidentiality Agreement must also require agents to comply with the provisions of the *Act* and its regulation relating to prescribed persons or prescribed entities, as the case may be, and with the terms of the Confidentiality Agreement as may be amended from time to time.

Agents must also be required to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by the prescribed person or prescribed entity and to comply with any privacy and security policies, procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

It is also recommended that the Confidentiality Agreement provide a definition of personal health information and that the definition provided be consistent with the *Act* and its regulation.

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

The Confidentiality Agreement shall identify the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of the prescribed person or prescribed entity and any limitations, conditions or restrictions imposed thereon.

In identifying the purposes for which agents are permitted to collect, use or disclose personal health information, the prescribed person or prescribed entity must ensure that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by the *Act* and its regulation. In this regard, the Confidentiality Agreement must prohibit agents from collecting and using personal health information except as permitted in the Confidentiality Agreement and from disclosing such information except as permitted in the Confidentiality Agreement or as required by law.

Further, the Confidentiality Agreement must prohibit agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.

### *Termination of the Contractual, Employment or Other Relationship*

The Confidentiality Agreement shall require agents to securely return all property of the prescribed person or prescribed entity, including records of personal health information and all identification cards, access cards and/or keys, on or before the date of termination of the employment, contractual or other relationship in accordance with the *Policy and Procedures For Termination or Cessation of the Employment or Contractual Relationship*. The Confidentiality Agreement shall also stipulate the time frame within which the property of the prescribed person or prescribed entity must be securely returned, the secure manner in which the property must be returned and the agent to whom the property must be securely returned.

### *Notification*

At a minimum, the Confidentiality Agreement shall require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management* and/or the *Policy and Procedures for Information Security Breach Management*, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or security policies, procedures and practices implemented by the prescribed person or prescribed entity.

### *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 Agents

A prescribed person or prescribed entity must maintain a log of Confidentiality Agreements that have been executed by agents at the commencement of their employment, contractual or other

relationship with the prescribed person or prescribed entity and on an annual basis. At a minimum, the log must include the name of the agent, the date of commencement of the employment, contractual or other relationship with the prescribed person or prescribed entity and the dates that the Confidentiality Agreements were executed.

## 8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

A job description for the position(s) that have been delegated day-to-day authority to manage the privacy program on behalf of the prescribed person or prescribed entity must be developed.

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 or the Executive Director, as the case may be. 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 agents are aware of the *Act* and its regulation and their duties thereunder;
- Ensuring agents are aware of the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy;
- Conducting, reviewing and approving privacy impact assessments;
- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *Policy and Procedures for Privacy Complaints*;
- Receiving and responding to privacy inquiries pursuant to the *Policy and Procedures for Privacy Inquiries*;

- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *Policy and Procedures for Privacy Breach Management*; and

- Conducting privacy audits pursuant to the *Policy and Procedures In Respect of Privacy Audits*.

## 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 person or prescribed entity 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 or the Executive Director, as the case may be. The job description must also identify the responsibilities and obligations of the position(s) in respect of the security program. At a minimum, these responsibilities and obligations must include:

- Developing, implementing, reviewing and amending security policies, procedures and practices;

- Ensuring compliance with the security policies, procedures and practices implemented;

- Ensuring agents are aware of the security policies, procedures and practices implemented by the prescribed person or prescribed entity and are appropriately informed of their duties and obligations thereunder;

- Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness;

- 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 agents, as well as their supervisors, to notify the prescribed person or prescribed entity of the termination of the employment, contractual or other relationship. The policy and procedures shall identify the agent(s) to whom notification must be

provided, the nature and format of the notification, the time frame within which notification must be provided and the process that must be followed in providing notification.

The policy and its procedures shall also require agents to securely return all property of the prescribed person or prescribed entity on or before the date of termination of the employment, contractual or other relationship. In this regard, a definition of property must be provided in the policy and procedures and this definition must, at a minimum, include records of personal health information, identification cards, access cards and/or keys.

The policy and procedures shall identify the agent(s) to whom the property must be securely returned; the secure method by which the property must be returned; the time frame within which the property must be securely returned; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation. The procedures to be followed in the event that the property of the prescribed person or prescribed entity is not securely returned upon termination of the employment, contractual or other relationship shall also be addressed, including the agent(s) responsible for implementing the procedure and the time frame following termination within which the procedure must be implemented.

The policy and procedures shall also require that access to the premises of the prescribed person or prescribed entity, to locations within the premises where records of personal health information are retained and to the information technology operational environment, be immediately terminated upon the cessation of the employment, contractual or other relationship. The policy and procedures must identify the agent(s) responsible for terminating access; the procedure to be followed in terminating access; the time frame within which access must be terminated; the documentation that must be completed, provided and/or executed and the agent(s) responsible for completing, providing and/or executing the documentation.

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

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management* and/or the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 11. Policy and Procedures for Discipline and Corrective Action

The prescribed person or prescribed entity 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 person(s) responsible for conducting the investigation; the procedure that must be followed in undertaking the investigation; any documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the required content of the documentation; and the agent(s) to whom the results of the investigation must be reported.

The types of discipline that may be imposed by the prescribed person or prescribed entity and the factors that must be considered in determining the appropriate discipline and corrective action shall also be set out in the policy and procedures. The agent(s) responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the agent(s) that must be consulted in making this determination; and the documentation that must be completed, provided and/or executed, 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 agent(s) 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 person or prescribed entity must be established.

The privacy governance and accountability framework must stipulate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring that the prescribed person or prescribed entity and its agents comply with the *Act* and its regulation and comply with the privacy policies, procedures and practices implemented.

The 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 or the Executive Director 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.

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 agent(s) 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.

It is also recommended that the privacy governance and accountability framework be accompanied by a privacy governance organizational chart.

The privacy governance and accountability framework shall also set out the manner in which the privacy governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity, the method by which it will be communicated and the agent(s) responsible for this communication.

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 person or prescribed entity must be established.

The security governance and accountability framework must stipulate that the Chief Executive Officer or the Executive Director, as the case may be, is ultimately accountable for ensuring the security of personal health information and for ensuring that the prescribed person or prescribed entity and its agents comply with the security policies, procedures and practices implemented.

The position(s) that have been delegated day-to-day authority to manage the security program must be identified in the security governance and accountability framework and the nature of the reporting relationship to the Chief Executive Officer or the Executive Director 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.

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 agent(s) 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.

It is also recommended that the security governance and accountability framework be accompanied by a security governance organizational chart.

The security governance and accountability framework shall also set out the manner in which the security governance and accountability framework will be communicated to agents of the prescribed person or prescribed entity, the method by which it will be communicated and the agent(s) responsible for this communication.

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 person or prescribed entity shall establish terms of reference for each committee that has a role in respect of the privacy and/or the security program. For each committee, the terms of reference must identify the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and/or the security program and the frequency with which the committee meets. 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

A prescribed person or prescribed entity must develop and implement a comprehensive and integrated corporate risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

The corporate risk management framework must address the agent(s) responsible and the process that must be followed in identifying risks that may negatively affect the ability of the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. This shall include a discussion of the agents or other persons or organizations that must be consulted in identifying the risks; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

It must also address the agent(s) responsible, the process that must be followed and the criteria that must be considered in ranking the risks and assessing the likelihood of the risks occurring and the potential impact if they occur. This shall include a discussion of the agents or other persons or organizations that must be consulted in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in assessing and ranking the

risks; the documentation that must be completed, provided and/or executed in setting out the rationale for the assessment and ranking of the risks; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The corporate risk management framework must also identify the agent(s) responsible, the process that must be followed and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed, the process for implementing the mitigation strategies and the agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

This includes identifying the agent(s) responsible for assigning other agent(s) to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented. 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 agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The corporate risk management framework must also address the manner and format in which the results of the corporate risk management process, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy and the status of implementation of the mitigation strategies, are communicated and reported. This involves identifying the agent(s) responsible for communicating and reporting the results of the corporate risk management process, the nature and format of the communication; and to whom the results will be communicated and reported, including to the Chief Executive Officer or the Executive Director. Approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement, shall also be outlined.

Further, 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 person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information continue to be identified, assessed and mitigated.

The frequency with which the corporate risk register must be reviewed and the agent(s) responsible and the process that must be followed in reviewing and amending the corporate risk register must also be identified.

The manner in which the corporate risk management framework will be integrated into the policies, procedures and practices of the prescribed person or prescribed entity and into the projects undertaken by the prescribed person or prescribed entity and the agent(s) responsible for integration shall also be addressed.

## 5. Corporate Risk Register

A prescribed person or prescribed entity must develop and maintain a corporate risk register that identifies each risk identified that may negatively affect the ability of the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. For each risk identified, the corporate risk register shall include an assessment of the risk, a ranking of the risk, the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date that the mitigation strategy was implemented or is required to be implemented, and the agent(s) responsible for implementation of the mitigation strategy.

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

The prescribed person or prescribed entity shall develop and implement a policy and associated procedures requiring a consolidated and centralized log to be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches. The consolidated and centralized log shall also be required to include recommendations made by the Information and Privacy Commissioner of Ontario that must be addressed by the prescribed person or prescribed entity prior to the next review of its practices and procedures.

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 agent(s) 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 Privacy Commissioner of Ontario 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 person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach. The policy and procedures must also stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits* and the *Policy and Procedures In Respect of Security Audits*, as the case may be, and must set out the frequency with which the policy and procedures will be audited and the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures must also require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity in accordance with the *Policy and Procedures for Privacy Breach Management* and/or the *Policy and Procedures for Information Security Breach Management*, as the case may be, if an agent breaches or believes there may have been a breach of this policy or its procedures.

## 7. Consolidated Log of Recommendations

A prescribed person or prescribed entity must develop and maintain a consolidated and centralized log of all recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches and reviews by the Information and Privacy Commissioner of Ontario.

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 agent(s) 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 person or prescribed entity in the event of short and long-term business interruptions and in the event of threats to the operating capabilities of the prescribed person or prescribed entity, including natural, human, environmental and technical interruptions and threats.

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.

In relation to notification of the interruption or threat, the business continuity and disaster recovery plan shall identify the agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity and the agent(s) responsible for providing such notification. 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 agents, service providers, stakeholders and other persons or organizations that must be notified of business interruptions and threats and the business continuity and disaster recovery plan must identify the agent(s) responsible for creating and maintaining this contact list.

In relation to the assessment of the severity level of the interruption or threat, the business continuity and disaster recovery plan shall identify the agent(s) responsible for the assessment, the criteria pursuant to which this assessment is to be made and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat. 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 agent(s) 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 agent(s) responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of the prescribed person or prescribed entity. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the initial impact assessment must be communicated.

The business continuity and disaster recovery plan must further identify the agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover and restore infrastructure elements, information systems and/or services. It must further address the manner in which the assessment is required to be conducted; the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be considered in undertaking the assessment; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the assessment must be communicated.

The business continuity and disaster recovery plan shall also identify the agent(s) responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined, and the recovery time objectives for critical applications. This shall include a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of these activities must be communicated.

In this regard, the business continuity and disaster recovery plan must require that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like. The business continuity and disaster recovery plan must further identify the agent(s)

responsible for developing and maintaining the inventory, the agent(s) and other persons and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions must be made.

The procedure by which decisions made and actions taken during business interruptions and threats to the operating capabilities of the prescribed person or prescribed entity will be documented and communicated and by whom and to whom they will be communicated must also be discussed.

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 agent(s) responsible for ensuring that the business continuity and discovery plan is tested, maintained and assessed; the agent(s) responsible for amending the business continuity and discovery plan as a result of the testing; the procedure to be followed in testing, maintaining, assessing and amending the business continuity and discovery plan; and the agent(s) responsible for approving the business continuity and disaster recovery plan and any amendments thereto.

The business continuity and disaster recovery plan must further address the agent(s) responsible and the procedure to be followed in communicating the business continuity and disaster recovery plan to all agents, including any amendments thereto, and the method and nature of the communication. The agent(s) responsible for managing communications in relation to the threat or interruption shall also be identified, including the method and nature of the communication.

# 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 person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.<br>▪ 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.<br>▪ 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.<br>▪ The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.<br>▪ 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. |
| **Collection** | ▪ The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.<br>▪ The number of statements of purpose developed for data holdings containing personal health information.<br>▪ The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made. |

| Categories | Privacy Indicators |
|---|---|
| **Use** | ▪ The number of agents granted approval to access and use personal health information for purposes other than research.<br>▪ The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario. |
| **Disclosure** | ▪ The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario. |

| Categories | Privacy Indicators |
|---|---|
| **Data Sharing Agreements** | ▪ The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. |
| **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 Information and Privacy Commissioner of Ontario. |
| **Data Linkage** | ▪ The number and a list of data linkages of PHI approved since the prior review by the Information and Privacy Commissioner of Ontario. |
| **Privacy Impact Assessments** | ▪ The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:<br>– The data holding, information system, technology or program,<br>– The date of completion of the privacy impact assessment,<br>– A brief description of each recommendation,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed.<br>▪ The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion.<br>▪ 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.<br>▪ The number of determinations made since the prior review by the Information and Privacy Commissioner of Ontario that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.<br>▪ The number and a list of privacy impact assessments reviewed since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made. |

| Categories | Privacy Indicators |
|---|---|
| **Privacy Audit Program** | ▪ The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed.<br><br>▪ The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:<br>– A description of the nature and type of audit conducted,<br>– The date of completion of the audit,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– 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 person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.<br><br>▪ With respect to each privacy breach or suspected privacy breach:<br>– The date that the notification was received,<br>– The extent of the privacy breach or suspected privacy breach,<br>– Whether it was internal or external,<br>– The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations,<br>– The date that the investigation was commenced,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– 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 Information and Privacy Commissioner of Ontario.<br>▪ Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint investigated:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint,<br>– The date that the investigation was commenced,<br>– The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed,<br>– The manner in which each recommendation was addressed or is proposed to be addressed, and<br>– The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.<br>▪ Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint, and<br>– The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter. |

## Part 2 – Security Indicators

| Categories | Security Indicators |
|---|---|
| **General Security Policies and Procedures** | ▪ The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario.<br>▪ 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.<br>▪ 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.<br>▪ The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.<br>▪ 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 agents 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 Information and Privacy Commissioner and for each audit:<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. |

| Categories | Security Indicators |
|---|---|
| **Security Audit Program** | ▪ The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.<br>▪ The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:<br>– A description of the nature and type of audit conducted,<br>– The date of completion of the audit,<br>– A brief description of each recommendation made,<br>– The date that each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is expected to be addressed. |
| **Information Security Breaches** | ▪ The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ With respect to each information security breach or suspected information security breach:<br>– The date that the notification was received,<br>– The extent of the information security breach or suspected information security breach,<br>– The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations,<br>– The date that the investigation was commenced,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– 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 agents who have received and who have not received initial privacy orientation since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.<br>▪ The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication. |
| **Security Training and Awareness** | ▪ The number of agents who have received and who have not received initial security orientation since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.<br>▪ The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the Information and Privacy Commissioner of Ontario. |
| **Confidentiality Agreements** | ▪ The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ The date of commencement of the employment, contractual or other relationship for agents that 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 agents since the prior review by the Information and Privacy Commissioner of Ontario 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 person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario.<br>▪ 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 Information and Privacy Commissioner of Ontario.<br>▪ 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], the [INSERT TITLE] of [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY], MAKE OATH AND SAY:

1. [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY] has in place policies, procedures and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

2. The policies, procedures and practices implemented by [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY] comply with the *Personal Health Information Protection Act, 2004* and the regulations thereto, as may be amended from time to time.

3. The policies, procedures and practices implemented by [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY] comply with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* 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 PERSON OR PRESCRIBED ENTITY] 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 Persons and Prescribed Entities*.

5. [INSERT NAME OF PRESCRIBED PERSON OR PRESCRIBED ENTITY] 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 is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

**SWORN (OR AFFIRMED) BEFORE ME** )
)
at the City/Town/Etc. of _____, in the )
)
County/Regional Municipality/Etc. of )
)
_____, on _____ 20 __. )

_____
[SIGNATURE OF DEPONENT]

_____
Commissioner for Taking Affidavits