eHealth Ontario

Privacy and Data Protection Policy

Privacy Office

Document ID: 00998

Version: 6.4

Owner: Chief Privacy Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

Tables

1 Purpose / Objective

The *eHealth Ontario Privacy and Data Protection Policy:*

- Supports decision-making at eHealth Ontario ('eHealth Ontario' or 'the Agency') by establishing guiding principles for how the Agency will protect privacy, and the confidentiality of personal information (PI) and personal health information (PHI);
- Establishes a culture of privacy protection and privacy compliance, including fostering the application of 'Privacy by Design'; and
- Identifies core privacy responsibilities for eHealth Ontario personnel and third party service providers to foster co-ordination among eHealth Ontario divisions and teams in protecting privacy.

2 Scope

This Policy applies to eHealth Ontario's personnel and third party service providers.

It applies to:

- Personal Information (PI) protected by the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA);
- Personal Health Information (PHI) protected by the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3 (PHIPA); and
- Any other information that the Chief Privacy Officer (CPO) determines that the Agency shall treat as PI/PHI.

eHealth Ontario maintains a comprehensive set of privacy and data protection policies that are subordinate and complementary to the *eHealth Ontario Privacy and Data Protection Policy*. The subordinate policies, listed in section 7, define privacy roles, responsibilities, accountabilities and requirements relevant to a given context (e.g. for the management of PHI and for PI) and may apply not only to eHealth Ontario but also to parties such as health information custodians (HICs) and third party service providers.

Where the repository or system is governed by the Electronic Health Record (EHR) Privacy Policies, follow the appropriate policies and procedures outlined in the *eHealth Ontario Electronic Health Record Privacy Policies*.

3 Context

The Context section explains why protecting privacy is critical at eHealth Ontario and introduces the sources for the Agency's privacy requirements.

3.1 Protecting Privacy is Central to eHealth Ontario's Mandate

Protecting privacy is not only an obligation for the Agency- it's also part of its mandate. Along with providing eHealth Services and support for the effective and efficient planning, management and delivery of health care in Ontario, and developing eHealth Services strategy and operational policy, the Agency is to: 'protect the privacy of individuals whose personal information or personal health information is collected, transmitted, stored or exchanged by and

through the Agency, in accordance with the *Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004* and any other applicable law.[1]

3.2 Agency Privacy Requirements

The Agency's privacy requirements derive from many sources including:

- Laws, rules, orders, regulations and by-laws, particularly its Enabling Regulation, PHIPA, FIPPA and orders made by the Information and Privacy Commissioner/ Ontario
- The Agency's Memorandum of Understanding with the Minister of Health and Long Term Care (MOHLTC)
- Government of Ontario Directives that apply to eHealth Ontario[2]
- Agency policies
- Agreements
- Industry best practices
- Stakeholder expectations

The regulatory requirements that apply to any given Agency activity depend on the facts and circumstances involved.

eHealth Ontario's subordinate privacy policies and procedures explain the regulatory requirements in detail.

3.3 Fostering a Culture of Privacy Protection

The Agency believes that protecting privacy effectively involves not only complying with applicable privacy requirements but also having a strong culture of privacy protection.

This Policy mandates the Agency's Privacy Protection Program. The Privacy Protection Program comprises comprehensive safeguards for PI/PHI and programs, practices, processes, tools and techniques to protect privacy proactively. eHealth Ontario establishes a culture of privacy protection by maintaining and continuously improving its Privacy Protection Program.

4 Policy

The Agency has established Guiding Principles for its approach to protecting privacy. Section 4.1 articulates the Guiding Principles which also serve as an interpretative tool for the policy statements that follow in section 4.2.

4.1 Guiding Principles

1. By proactively protecting privacy and PI/PHI, and fostering a culture of privacy protection, eHealth Ontario:
    - Demonstrates respect for individuals' privacy rights and for its stakeholders;
    - Reduces privacy, operational and other risks for the Agency and for its stakeholders, particularly the public; and
    - Builds confidence in the Agency.
2. Protecting PI/PHI in accordance with the Agency's privacy requirements is a core eHealth Ontario business practice. The Agency's privacy requirements derive not only from legal requirements but also from Agency policies, industry best practices and individuals' privacy preferences.

[1] Ontario Regulation 43/02, R.S.O. 1990, c. D. 10, as amended from time to time, s3.3

[2] The Agency's Memorandum of Understanding with the Minister of Health and Long Term Care requires eHealth Ontario to comply with Government of Ontario Directives that apply to eHealth Ontario. The person with authority to make a Directive binding on the Agency is also the person who can exempt the Agency from having to apply aspects of the Directive.

3. The Agency proactively embeds privacy protections into the design and operation of its programs, services, systems, and processes. Privacy protections shall seek to prevent privacy invasive events from occurring and shall safeguard PI/PHI throughout its lifecycle.

4. eHealth Ontario personnel all play a role in protecting privacy and PI/PHI, working under the leadership of the CPO. eHealth Ontario managers, including the CPO, are responsible for making sure that eHealth Ontario manages privacy protection consistently and in a coordinated manner.

5. The Agency employs a risk-based approach to protecting privacy. Risk management practices provide the opportunity to establish the optimum level of oversight, control and discipline to enable the Agency to manage risk in changing environments and help provide the proper level of assessment that business objectives and strategies, including privacy protection, are being met.

6. The Agency will continuously improve its Privacy Protection Program. It will seek opportunities to do so by learning from its stakeholders' experiences and results, and by encouraging feedback and suggestions, particularly from personnel.

4.2 Policy Requirements

Accountability

7. The Agency's Board of Directors oversees the protection of privacy at eHealth Ontario.

8. The Chief Executive Officer (CEO) is responsible for managing privacy protection at the Agency, including ensuring that eHealth Ontario complies with applicable privacy requirements and fostering a culture of privacy protection.

9. The CEO delegates responsibility to the CPO to:

    - Lead the design and operation of the Agency's Privacy Protection Program, including privacy-related governance bodies;
    - Provide advice, support and direction to personnel about privacy matters applicable to their areas of responsibility; and
    - Monitor and report on privacy protection at eHealth Ontario.

10. eHealth Ontario managers are responsible for achieving and demonstrating compliance with privacy requirements applicable to their areas of responsibility.

11. eHealth Ontario shall provide its personnel and third party providers with formal direction on their accountabilities, roles and responsibilities for protecting privacy. Means of providing such direction may include: training and awareness programs, agreements, written policies and procedures and job descriptions.

Privacy Protection Program

12. The Agency shall maintain a Privacy Protection Program that comprises comprehensive and aligned safeguards for PI/PHI, and programs, practices, processes, tools and techniques that enable it to:

    - Protect individuals' privacy and the confidentiality of their PI/PHI proactively and respect their privacy preferences; and
    - Comply with its privacy requirements, particularly those derived from its Enabling Regulation, from PHIPA and FIPPA and the Regulations made under those Acts, and from its policies.

13. The Privacy Protection Program shall include processes, practices and tools and techniques to:

    - Build privacy and security protection into the design and operation of the Agency's programs, operations and services, including business practices, systems and physical design and infrastructure;
    - Safeguard PI/PHI throughout its lifecycle;
    - Achieve, monitor, assess and enforce privacy compliance;

- Identify and manage privacy risks proactively;
- Train personnel and third party service providers about protecting privacy;
- Develop and implement privacy policies, practices and standards;
- Provide privacy services such as Privacy Impact Assessments (PIAs);
- Manage, investigate and respond to privacy- and security- related incidents, breaches, complaints and inquiries; and
- Engage internal and external stakeholders about privacy matters.

14. The CPO shall lead the design, implementation and operation of the Privacy Protection Program, working collaboratively with personnel.

15. eHealth Ontario managers shall design, implement and operate aspects of the Privacy Protection Program applicable to their areas of responsibility, working collaboratively and proactively with the CPO.

16. eHealth Ontario managers shall ensure that privacy risks related to their areas of responsibility are identified, monitored, managed and subject to mitigation. The CPO shall provide tools and methods to achieve that objective, aligned with the Agency's overall risk management approach.

17. Personnel and third party service providers shall seek to design privacy-protective features, including privacy defaults, into Agency products, services and operations.

18. The Agency shall conduct privacy and security assessments to accompany any proposals for new initiatives or changes to existing initiatives that may affect individuals' privacy.

19. At the CPO or designee's direction, eHealth Ontario may extend privacy protections to information that is not subject to privacy and data protection laws, regulations or similar requirements.

eHealth Ontario Policies and Practices

20. eHealth Ontario's policies and practices shall:

    - Protect privacy and the confidentiality of PI/PHI while achieving the Agency's other business interests and objectives (e.g. effectively facilitating the delivery of services and programs and realizing value for money); and
    - Comply with all applicable privacy requirements, in particular the Guiding Principles and Policy Requirements articulated in the *Privacy and Data Protection Policy*.

21. The CPO shall:

    - Advise eHealth Ontario managers about the privacy implications of, and requirements for, policies and practices in their areas of responsibility;
    - Provide advice and support to the Shareholder Relations and Business Planning Department during Agency strategic Policy development initiatives; and
    - Establish and maintain written policies and practices that direct the design and management of the Agency's Privacy Protection Program.

22. eHealth Ontario managers shall:

    - Confirm that policies and practices applicable to their areas of responsibility comply with the *Privacy and Data Protection Policy* and any applicable subordinate privacy policies;
    - Seek advice from the CPO about the privacy implications and requirements for their policies and practices, particularly at the design stage and when making significant changes; and
    - Establish, maintain and ensure compliance with written policies and practices that protect individuals' privacy and the confidentiality of PI/PHI applicable to their areas of responsibility.

23. The CPO and Chief Security Officer (CSO) shall ensure that the Agency's policies and practices that protect individuals' privacy and the confidentiality of their PI/PHI are comprehensive, aligned and complementary.

24. The Agency shall comply with its policies and practices that protect individuals' privacy and the confidentiality of

PI/PHI.

25. The Agency may consult with external and internal stakeholders in the development of its policies and practices that protect privacy and the confidentiality of PI/PHI.

Privacy Training and Awareness

26. The CPO shall provide a foundational privacy training program suitable for all personnel and third party service providers. The CPO shall review and update the program annually at a minimum to address any substantive changes to eHealth Ontario's privacy requirements and any other relevant matters.

27. The CPO, supported by the Privacy Office, shall develop and provide role-based privacy training for personnel commensurate with their responsibilities and whether or not personnel may have access to PI/PHI.

28. The Privacy Office shall deliver or make available role-based privacy training for personnel and third party service providers with access to, or the potential to access, PI/PHI on the eHealth Ontario network, in accordance with the *eHealth Ontario Personal Information Privacy Policy and the eHealth Ontario Personal Health Information Privacy Policy*.

29. Personnel shall:

    - Agree to the eHealth Ontario Privacy and Security Acknowledgement and Agreement prior to commencing their work with the Agency;
    - Complete foundational privacy training, *Privacy and Security Fundamentals*, within thirty (30) days of beginning work at eHealth Ontario, and annually thereafter; and
    - Undertake role-based privacy training as directed by eHealth Ontario managers.

30. Third Party Service Providers shall:

    - Agree to the eHealth Ontario Privacy and Security Acknowledgement and Agreement prior to commencing their work with the Agency; and
    - Complete privacy training as directed by eHealth Ontario managers.

31. The Vice President, Human Resources and the Vice President, Strategic Sourcing and Vendor Management shall:

    - Implement procedures to enable personnel and third party service providers to agree to the eHealth Ontario Privacy and Security Acknowledgement and Agreement and complete required privacy training in a timely manner; and
    - Provide regular compliance reports to eHealth Ontario managers and to the CPO.

32. eHealth Ontario managers shall ensure that personnel or third party service providers reporting to them meet their privacy training requirements.

Working with Third Party Providers

33. eHealth Ontario shall enter into signed, written agreements with third party providers that include appropriate privacy requirements prior to the third parties providing services or goods to the Agency.

34. With guidance from the CPO, the Vice President, Strategic Sourcing and Vendor Management shall maintain standard content about privacy for procurement templates (e.g. privacy requirements, assessment and scoring criteria) and for agreements with third party providers. The CPO and Vice President, Strategic Sourcing and Vendor Management shall periodically review and update the standard content.

35. The Agency shall modify the standard content of agreements and procurement templates to reflect the nature of the services or goods that a third party provider will deliver, any specific privacy requirements arising and the associated privacy-related risks.

Protecting PI/PHI

36. eHealth Ontario shall protect PI/PHI with technical, administrative, and physical safeguards that:

- Are appropriate to the information's sensitivity, the format in which it is held, and the related privacy risks; and
- Secure the PI/PHI against: theft, loss, unauthorized access, collection, use or disclosure and unauthorized copying, modification, retention or disposal.

37. Personnel and third party service providers shall not access PI/PHI unless:

- Access is necessary in order to perform their roles;
- They have been authorized to do so by their eHealth Ontario manager, the system owner and with the requisite authority from the Privacy Office and Security Services;
- They agree to the eHealth Ontario Privacy and Security Acknowledgement and Agreement and completed applicable privacy training;
- They have formally agreed to comply with any additional privacy-related requirements and restrictions established by eHealth Ontario; and
- They are in compliance with all applicable Agency policies.

Openness

38. The Agency shall publish its privacy policies and practices on its website and make copies of them available through the Privacy Office. For the benefit of clarity, the Agency shall not publish or make available policies or practices if doing so could compromise the security of PI/PHI or would reveal a trade secret or confidential scientific, technical, commercial or labour relations information.

39. eHealth Ontario shall publish the CPO or designee's name, title and contact information on its website and advise individuals of this information on request.

40. eHealth Ontario shall publish summaries of the results of privacy assessments carried out on eHealth Ontario's services when eHealth Ontario is providing services under O. Reg. 329/04 sections 6 and 6.2.

Monitoring Compliance and Performance

41. eHealth Ontario shall conduct privacy compliance reviews and maintain privacy-related performance metrics on a basis and schedule set by the CPO. Regular reports will be provided to the Agency's Chief Internal Auditor and a report shall be provided not less than annually to the Agency's Board of Directors.

Complaints and Inquiries

42. The CPO shall manage and respond to complaints, questions and feedback about the Agency's privacy practices.

43. The Agency shall review, investigate and document every complaint received and shall monitor for any trends arising.

44. If the sender provides contact information, the Agency shall:

- Acknowledge the complaint, question or feedback within four (4) days of receipt and provide information about any relevant internal and external complaint mechanisms;
- Respond to the sender's question, feedback or complaint within thirty (30) days of receipt; and
- Notify the sender of its expected timeframe for responding if it anticipates a delay arising.

45. The Agency shall take appropriate measures to respond to complaints and feedback, which may include changing its policies and practices.

46. The Agency shall provide a means for personnel to share privacy-related concerns in confidence and shall ensure that reporting personnel suffer no reprisals.

Non-Compliance

47. eHealth Ontario shall take appropriate remedial action to address non-compliance with its privacy requirements.

48. The consequences of non-compliance or for failing to take appropriate remedial action shall be consistent with

the Agency's disciplinary and procurement policies and procedures and may include invoking measures up to and including dismissal or termination of contract.

5 Responsibilities

5.1 Board of Directors

- Approves this Policy; and
- Oversees the Privacy Protection Program at eHealth Ontario.

5.2 Chief Executive Officer

- Recommends this Policy for approval;
- Fosters a culture of privacy protection;
- Ensures compliance with privacy requirements and enforces consequences of non-compliance; and
- Delegates privacy responsibility to the CPO, and ensures that the CPO is recognized as the privacy contact person.

5.3 Chief Privacy Officer

- Maintains this Policy;
- Implements and enforces this Policy;
- Is the ultimate authority for interpreting this Policy;
- Leads the design and operation of the Agency's Privacy Protection Program, including privacy-related governance bodies;
- Ensures privacy protective features are designed into Agency products, services and operations;
- Ensures transparency by making its privacy policies and practices and summaries of the results of relevant privacy assessments available;
- Provides advice, support and direction to eHealth Ontario managers, personnel and third party service providers about privacy matters applicable to their areas of responsibility;
- Provide tools and methods to support personnel and third party service providers in achieving their privacy objectives, including providing a privacy training program suitable to their privacy responsibilities;
- Ensures that the Agency's policies and practices protect individuals' privacy and the confidentiality of their PI/PHI and are transparent, comprehensive, aligned and complementary;
- Addresses privacy concerns from individuals, personnel and third party service providers; and
- Conducts privacy compliance reviews, maintain privacy-related performance metrics and regularly report to the Agency's Board of Directors, as required.

5.4 Chief Security Officer

- Supports this Policy; and
- Ensures that the Agency's policies and practices that protect individuals' privacy and the confidentiality of their PI/PHI are comprehensive, aligned and complementary.

5.5 Chief Administrative Officer

- Supports this Policy;

- Ensures personnel understand their privacy requirements prior to commencing work with eHealth Ontario;
- Implements procedures to enable personnel in achieving their privacy objectives; and
- Provides regular compliance reports to eHealth Ontario managers and to the CPO.

5.6 VP, Strategic Sourcing and Vendor Management

- Supports this Policy;
- Ensures third party service providers understand their privacy requirements prior to commencing work with eHealth Ontario;
- Implements procedures to enable third party service providers in achieving their privacy objectives; and
- Provides regular compliance reports to eHealth Ontario managers and to the CPO.

5.7 eHealth Ontario Managers

- Achieve and demonstrate compliance with privacy requirements in their areas of responsibility;
- Design, implement and operate aspects of the Privacy Protection Program applicable to their areas of responsibility and works collaboratively and proactively with the CPO;
- Ensure that privacy risks related to their areas of responsibility are identified, monitored, managed and subject to mitigation; and
- Ensure that personnel or third party service providers reporting to them meet their privacy objectives.

5.8 Privacy Office

- Supports the Agency's Privacy Protection Program, including conducting privacy assessments on new initiatives or changes to existing initiatives and developing and delivering privacy training to personnel and third party service providers; and
- Provides advice, support and direction on interpreting and applying this Policy.

5.9 eHealth Ontario Personnel

- Complies with this Policy, to the extent that it applies to their activities including supporting the Privacy Protection Program, designing privacy protection into Agency products, services and operations and completing privacy training; and
- Understands and agrees to their privacy obligations as defined in the eHealth Ontario Privacy and Security Acknowledgement and Agreement prior to commencing their work with the Agency.

6 Glossary

The following terminology and acronyms are associated with this Policy:

TERM	DEFINITION
Accountability	The obligation to answer for results and the manner in which responsibilities are discharged. Accountability cannot be delegated.

Data Protection	Legislation such as Ontario's PHIPA and FIPPA protect individuals' privacy in respect of their PHI and PI. The laws establish rules about the collection, use and disclosure of PHI/PI and rights for individuals, e.g. the right to access their PHI/PI. Protecting individuals' privacy in this way is also known as 'informational privacy' or 'data protection'. More broadly, privacy is recognized as a human right and the right to privacy is generally accepted as a precursor to sustaining freedom and democracy. For example, in R v O'Connor, Justice L'Heureux- Dube found that 'respect for individual privacy is an essential component of what it means to be "free"' and that the "essence of privacy… is that, once invaded, it can seldom be regained.'[3] The Agency's *Privacy and Data Protection Policy* reflects the fact that protecting privacy involves, but may not be limited to protecting PI/PHI.
eHealth Ontario managers	A manager is a person whose principal employment responsibilities consist of supervising or directing, or both supervising and directing, human or other resources. At eHealth Ontario, a manager may be the Chief Executive Officer, Senior Vice Presidents, Vice Presidents, Senior Directors, Directors, Managers, Supervisors, program leads, project managers or personnel who carry out managerial duties.
eHealth Services	One or more services to promote the delivery of health care services in Ontario that use electronic systems and processes, information technology and communication technology to facilitate electronic availability and exchange of information related to health matters, including personal information and personal health information, by and among patients, health care providers and other permitted users. (Enabling Regulation, s.1)
Enabling Regulation	Ontario Regulation 43/02, as amended from time to time, made pursuant to s.5 of the *Development Corporations Act* R.S.O. 1990, c. D. 10.
***Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA)**	A provincial privacy statute that provides a right to access information under the control of institutions in accordance with the principles that information should be available to the public; necessary exemptions from the right of access should be limited and specific; and decisions on the disclosure of government information should be reviewed independently of government. FIPPA also protects the privacy of personal information of individuals held by institutions. It provides individuals with a right of access to, and correction of, that information.
Governance	The processes and structures through which power and authority are exercised, including the decision-making processes.
Health Information Custodian (HIC)	Has the same meaning as defined in section 3 of *Personal Health Information Protection Act, 2004* (PHIPA) and generally means a person or organization that delivers healthcare services. Examples include: physicians, hospitals, pharmacies, laboratories, community care access centres and the Ministry of Health and Long-Term Care, but not eHealth Ontario.

[3] R v O'Connor [1995] 4 S.C.R. 411 at paragraph 119

Personal Information (PI)	Has the meaning set out in section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) as: recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.
Personal Health Information (PHI)	Has the meaning set out in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA), and generally means identifying information about an individual in oral or recorded form pertaining to that person's health or health services provided to the individual.
Personnel	Collectively, the following: current and former Employees; current Suppliers; and current and former Appointees. Where: • Employee: A person whom through the execution of a contract of service, has entered into an employment relationship with eHealth Ontario and is classified in one of the following categories, as defined by the eHealth Ontario Human Resources Department: Full-Time Regular Employee, Full-Time Temporary Employee, Part-Time Regular Employee or student. • Supplier: Also referred to as a third party service provider. An individual who or entity that supplies goods or services to eHealth Ontario, and is paid through the eHealth Ontario accounts payable system. • Appointee: An individual appointed by the Lieutenant Governor in Council as a member of the board of directors of eHealth Ontario under Ontario Regulation 43/02, "eHealth Ontario", made under the *Development Corporations Act*, *1990*, as amended from time to time.
Privacy default	A solution design that automatically protects privacy (i.e. the individual whose PI/PHI is involved needs to take no action to protect his/her privacy.)
Responsibility	The obligation to assume a role or take specific action(s). Responsibility may be delegated or conferred by mutual agreement, depending on the relationship.
Risk	The chance of something happening that will impact on the achievement of objectives.
Risk assessment	Evaluation of risk with regard to the risk's likelihood and potential impact using qualitative and quantitative methods.

Risk management	A comprehensive, structured and continuous process, in which risks are identified, evaluated and accepted or mitigated within approved risk tolerances.

Table 1: Privacy and Data Protection Policy: Glossary

7 Subordinate Policies

The subordinate policies of the *eHealth Ontario Privacy and Data Protection Policy* are:

REFERENCE	LOCATION
eHealth Ontario Personal Health Information Privacy Policy	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Personal Information Privacy Policy	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Privacy Impact Assessment Policy	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy Incidents and Breach Management Policy	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Privacy Complaints and Inquiries Policy and Procedure	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Freedom of Information and Protection of Privacy Access Request Policy	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy Risk Management Policy and Procedure	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers	http://www.ehealthontario.on.ca/privacy

Table 2: Privacy and Data Protection Policy: Subordinate Policies

8 References and Associated Documents

The following are legislative references and eHealth Ontario policies associated with this Policy:

REFERENCE	LOCATION
Freedom of Information and Protection of Privacy Act (FIPPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.

	htm
Personal Health Information Protection Act, 2004 (PHIPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm
eHealth Ontario Directory of Records	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Statement of Information Practices	http://www.ehealthontario.on.ca/en/privacy
eHealth Ontario Privacy and Security Standard of Conduct for Employees	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Privacy and Security Standard of Conduct for Service Providers	http://emerge/spaces/privacy/Documents/Forms/AllItems.aspx
eHealth Ontario Information Security policies and procedures	http://emerge/spaces/security/Documents/Forms/AllItems.aspx
Information and Privacy Commissioner, Ontario Privacy by Design	http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
eHealth Ontario Electronic Health Record Privacy Policies	http://www.ehealthontario.on.ca/en/initiatives/resources

Table 3: Privacy and Data Protection Policy: References and Associated Documents

9 Contact Information

For further information about this Policy, kindly contact:

Privacy Office

eHealth Ontario

P.O. Box 148

777 Bay Street, Suite 701

Toronto, ON

M5G 2C8

Fax: (416) 586-4937 or 1 (866) 831-0107

Email: privacy@ehealthontario.on.ca

Telephone: (416) 946-4767 or 1 (888) 411-7742 ext 64767

10 Interpretation

Policy requirements preceded by:

- 'shall' are compulsory actions;
- 'may' are options; and
- 'should' are recommended actions

If there is a discrepancy between this Policy and *FIPPA* or *PHIPA*, the regulations made under those Acts, or with the Agency's Regulation, the legislation or regulation takes precedence.

If there is a discrepancy between this Policy and any subordinate eHealth Ontario privacy policy, this Policy takes precedence.