eHealth Ontario

Privacy Policy on the Responsibilities of Third Party Service Providers

Privacy Office

Document ID: 2489

Version: 3.2

Owner: Chief Privacy Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

1 Purpose / Objective 1
2 Scope 1
3 Legislative Requirements 1
4 Policy 2
4.1 Privacy Responsibilities of Third Party Service Providers 2
4.2 Agreements with Third Party Service Providers 2
4.3 Logging and Document Retention 2
5 Responsibilities 3
6 Glossary 3
7 References and Associated Documents 5
8 Interpretation 5

Tables

Table 1: Privacy Policy on the Responsibilities of Third Party Service Providers Policy: Glossary 4
Table 2: Privacy Policy on the Responsibilities of Third Party Service Providers Policy: References and Associated Documents 5

1 Purpose / Objective

This Policy describes the expectations and responsibilities, as they relate to privacy, of third party service providers which eHealth Ontario retains in the course of carrying out its business.

The *eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers* must be read in conjunction with the *eHealth Ontario Privacy and Data Protection Policy*, *Personal Health Information Privacy Policy and Personal Information Privacy Policy*. Together, these documents define the privacy and data protection principles, legislative requirements and policies which determine the privacy roles and responsibilities of eHealth Ontario in relation to the protection of personal information (PI) and personal health information (PHI).

2 Scope

This Policy applies to all eHealth Ontario personnel and third party service providers whom it has retained to support the delivery of its operations and services.

Applicable provisions of this Policy must be addressed in eHealth Ontario's agreements with third party service providers as required. This Policy applies to eHealth services which may impact the privacy of PI/PHI in the Agency's care.

Third party service providers have the same meaning as suppliers.

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 Legislative Requirements

eHealth Ontario may act in a number of capacities, as described in the *Personal Health Information Protection Act, 2004* (PHIPA) and its regulation: under section 6.2 of Ontario Regulation (O. Reg.) 329/04, section 6 of O. Reg. 329/04 as a health information network provider (HINP), an electronic service provider (ESP), an agent or as a service provider to a HINP. Each role is focused around eHealth Ontario's relationship to one or more health information custodians (HICs).

Section 6 and section 6.2 of the O.Reg. 329/04 to PHIPA requires eHealth Ontario to ensure that any third party it retains to assist it in providing services related to its roles under PHIPA agrees to comply with the restrictions and conditions that are necessary to enable eHealth Ontario to comply with all these requirements.

eHealth Ontario is an "institution" as defined in Ontario's *Freedom of Information and Protection of Privacy Act*, 1990, S.O. 2004, c. F.31 ("FIPPA"), as amended and is subject to its provisions. eHealth Ontario is committed to protecting PI subject to FIPPA and extending privacy protection practices to its handling of PI where that information may not be subject to privacy laws or regulations.

4 Policy

The Chief Privacy Officer (CPO) at eHealth Ontario is responsible for leading the design and operation of the Agency's privacy program, including entering 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.

4.1 Privacy Responsibilities of Third Party Service Providers

eHealth Ontario shall not provide PI/PHI to a third party service provider if other information, namely de-identified and/or aggregate information will serve the purpose, and shall not provide more PI/PHI than is reasonably necessary to meet the purpose.

In some cases third party service providers retained by eHealth Ontario will not come into direct contact with PI/PHI in the course of their duties. In other cases, when third party service providers require access to PI/PHI in order to fulfill their job duties, eHealth Ontario shall ensure that they are subject to the same expectations and requirements as eHealth personnel regarding the protection of PI/PHI.

4.2 Agreements with Third Party Service Providers

eHealth Ontario shall enter into agreements with all third party service providers which it retains as a condition of the engagement. These agreements shall set out expectations regarding compliance with relevant legislation and eHealth Ontario policies and procedures, and responsibilities for the protection and safeguarding of PI/PHI at eHealth Ontario.

The terms of the agreement will vary depending on the nature of the service provider's engagement with eHealth Ontario:

- Third party service providers assisting in the provision of eHealth Ontario's services, whether working on eHealth Ontario's premises or remotely, who manage or come into contact with PI/PHI, shall be subject to the same expectations regarding conduct and practices as Agency personnel.
- Third party service providers assisting in the provision of eHealth Ontario's services through the development of systems that store and allow for the management of PI/PHI in an environment external to eHealth Ontario shall be subject to the same expectations regarding their conduct and practices as Agency personnel. These third party service providers shall also be expected to implement additional controls and safeguards that assure eHealth Ontario that PI/PHI that is not in its direct care is being managed by the third party service provider in a manner which enables eHealth Ontario to comply with its requirements under applicable privacy law.

Third party service providers must satisfy the requirements for additional controls through the development and submission of:

- privacy and security architecture that specify detailed safeguards and controls on PI/PHI;
- information management guidelines; and
- joint operational management procedures between the service provider and eHealth Ontario that address or contribute to the protection of PI/PHI.

Third party service providers which eHealth Ontario enters into agreements with shall describe safeguards for the secure retention and destruction of data, as applicable.

4.3 Logging and Document Retention

With guidance from the CPO, the Vice President, Strategic Sourcing and Vendor Management shall maintain standard content about privacy for agreements with third party providers. The CPO and Vice President, Strategic

Sourcing and Vendor Management shall periodically review and update the standard content to ensure it is up-to-date and accurate.

The Vice President, Strategic Sourcing and Vendor Management shall maintain an agreement management system which flags which third party service providers have access to PI/PHI and the date on which the PI/PHI in the care of the third party service provider will be securely disposed of or returned to eHealth Ontario. The CPO shall follow-up with the third party service provider to ensure PI/PHI is disposed of or returned in a secure manner, in accordance with eHealth Ontario policies and procedures.

All documentation relating to the privacy responsibilities of third party service providers retained by eHealth Ontario are securely retained in accordance with eHealth Ontario's policy and procedures.

5 Responsibilities

eHealth Ontario shall define and implement privacy and security compliance requirements that set out expectations of third party service providers retained by eHealth Ontario, where required.

Safeguards and access controls form a significant portion of eHealth Ontario's compliance monitoring program, and shall be embodied in all relevant agreements with third party service providers.

The CPO is considered the ultimate authority for interpreting, implementing, enforcing and maintaining this Policy, including providing third party service providers with training as required.

Compliance with this Policy will be reviewed as directed by the CPO.

6 Glossary

The following terminology and acronyms are associated with this Policy:

TERM	DEFINITION
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)
***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.
Personal Health	Has the meaning set out in section 4 of the *Personal Health Information Protection Act,*

Information (PHI)	*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.
***Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3. (PHIPA)**	A provincial health privacy statute that establishes rules for the management of PHI and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.
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.
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. .

Table 1: Privacy Policy on the Responsibilities of Third Party Service Providers Policy: Glossary

7 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 Privacy and Data Protection Policy	www.ehealthontario.on.ca/privacy
eHealth Ontario Personal Health Information Privacy Policy	www.ehealthontario.on.ca/privacy
eHealth Ontario Personal Information Privacy Policy	www.ehealthontario.on.ca/privacy
eHealth Ontario Privacy Complaints and Inquiries Policy and Procedure	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Privacy Incidents and Breach Management Policy	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Privacy and Security Standard of Conduct for Service Providers	http://www.ehealthontario.on.ca/privacy
eHealth Ontario Electronic Health Record Privacy Policies	http://www.ehealthontario.on.ca/en/initiatives/resources

Table 2: Privacy Policy on the Responsibilities of Third Party Service Providers Policy: References and Associated Documents

8 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 other eHealth Ontario privacy policy, the *eHealth Ontario Privacy and Data Protection* Policy takes precedence.