

# eHealth Ontario Privacy Impact Assessment Policy

Document Identifier: 1002

Version: 2

Owner: Chief Privacy and Security Officer

## Document Control

The electronic version of this document is recognized as the only valid version

---

**Document Location:** I:\Privacy and Security\PRIVACY\Policies

---

**Review Frequency:** Every two years or with greater frequency at the discretion of the Chief Privacy and Security Officer

---

**Document Prime\*** Angelique Hamilton  
Senior Privacy Analyst

\*Enquiries relating to this document should be referred to the responsible Document Prime.

---

## Approval History

Approver(s)	Title	Approved Date
David Hallett	Chief Operating Officer	2009-08-13
Karen Waite	Chief Privacy and Security Officer	2009-08-13
Michael Power	VP, Privacy and Security	2008-11-12

## Revision History

Version No.	Version Date	Summary of Change	Changed By
2	2008-09-23	Revision as per VP, Privacy and Security Officer	Angelique Hamilton
1	2007-09-28	Final Draft	Sharan Dosanjh

---

## 1 Objective

---

The *eHealth Ontario Privacy Impact Assessment Policy* must be read in conjunction with the *eHealth Ontario Privacy and Data Protection Policy* and the *eHealth Ontario Privacy Impact Assessment Guide*. Together, these documents define the privacy and data protection principles, legislative requirements and policies which determine how eHealth Ontario conducts Privacy Threshold Assessments (PTAs) and Privacy Impact Assessments (PIAs). This policy and related tools and guidelines support the Agency's commitment to designing privacy into its products and operations by identifying and managing risks, and developing solutions which enable business processes that enhance the privacy of Personal Information (PI) and Personal Health Information (PHI).

---

## 2 Scope

---

This Policy applies to all eHealth Ontario Personnel, including contract employees. Applicable provisions of this policy must be addressed in eHealth Ontario's agreements with third party service providers as required. This policy applies to all ONE Product offerings and eHealth Ontario initiatives and corporate activities which may impact the privacy of Personal Information or Personal Health Information in the Agency's care.

---

## 3 Legislative Requirements

---

Section 6 of the Regulation to PHIPA requires that eHealth Ontario perform an assessment of the services it provides with respect to threats, vulnerabilities, and risks to the security and integrity of PHI, and how the services may affect the privacy of the individuals who are the subject of the information, when it acts in its capacity as a Health Information Network Provider (HINP). According to PHIPA, eHealth Ontario acts as a HINP when it provides services to two or more HICs and when the services are provided primarily to enable the HICs to use electronic means to disclose PHI to one another, whether or not eHealth Ontario is an agent of any of the HICs. The Regulation further requires that eHealth Ontario report its findings to all applicable HICs.

---

## 4 Policy

---

While eHealth Ontario is required to conduct PIAs under PHIPA when acting in its capacity as a HINP, as a matter of policy, the Agency will conduct privacy assessments wherever it undertakes a new or modified initiative involving a significant change in the way in which it handles Personal Information (PI) or Personal Health Information (PHI). In addition, eHealth Ontario will conduct PIAs on all ONE Products. Further, the results of such assessments will be provided to internal and/or external stakeholders, and identified privacy risks will be tracked and monitored for mitigation.

eHealth Ontario shall determine the scope and necessity of conducting PIAs by first conducting a Privacy Threshold Analysis (PTA) wherever the Agency is contemplating a new or modified activity which involves the collection, use, disclosure or other changes to the way in which it handles Personal Information (PI) or Personal Health Information (PHI). A PTA is a preliminary, standardized analysis utilized to determine whether or not a solution or initiative will require a full Privacy Impact Assessment. The result of the PTA process will determine whether a PIA will be required.

eHealth Ontario shall conduct PTAs and PIAs to assist in building privacy into the design and operation of its solutions and programs. PTAs and PIAs will also identify privacy risks, which shall be managed and mitigated by eHealth Ontario Executives responsible for the initiatives undertaken by their respective Divisions.

eHealth Ontario shall conduct PIAs:

- on new corporate initiatives that involve the collection, use, or disclosure of PI or PHI or that otherwise raise privacy issues;
- on existing corporate solutions or initiatives which eHealth Ontario proposes to modify in connection with the concepts, key business processes, functionality, access, or technology associated with such solutions;
- on new and existing ONE products and services to which eHealth Ontario proposes to make or makes changes in connection with the concepts, key business processes, functionality, access, or technology associated with such solutions;
- on all activities that involve data linkage or matching; and
- on any other initiative or solution which the Chief Privacy and Security Officer identifies as requiring analysis for determination of privacy risk.

eHealth Ontario's PIA assessments of the results ("PIA reports") shall consider and state the:

- scope of the assessment and any privacy risks, and limitations arising therefrom, for eHealth Ontario, its clients, Ontarians, and any other applicable stakeholders, insofar as eHealth Ontario can reasonably assess them;
- requirements for compliance with PHIPA and/ or the *Freedom of Information and Protection of Privacy Act* (FIPPA), the Regulations made under those Acts, eHealth Ontario's enabling regulation, and eHealth Ontario's Privacy and Data Protection policies; and
- strategies and solutions, including related timeframes, to be designed and implemented in order to mitigate and manage privacy risks.

At the earliest possible stage, eHealth Ontario shall commence and complete PTAs, and PIAs as required, prior to the provision of the services to HICs, or prior to deployment of a corporate solution or initiative.

For existing corporate solutions and ONE products and services, eHealth Ontario shall perform PTAs and PIAs as required prior to the implementation of any changes and where possible, at the design stage. eHealth Ontario shall review and update PIAs at the discretion of the Chief Privacy and Security Officer.

eHealth Ontario shall maintain supporting tools and procedures to enable it to conduct PTAs and PIAs. eHealth Ontario shall integrate PTAs and PIAs into the Agency's project management, development lifecycle, and risk management processes. PTA and PIA reports will be managed in a central location and any privacy risks identified through the assessment process will be entered into a Privacy and Security Risk Register, and shall be tracked and monitored for implementation of mitigation strategies.

eHealth Ontario shall:

- Provide to each applicable HIC a written copy of the results of the Agency's ONE product PIA summaries in advance of providing services to that HIC; and
- Ensure it has provided current PIA summaries to its clients.

In order to maintain a high level of accountability and transparency, eHealth Ontario shall make its PIA summaries available to the public by publishing them on the eHealth Ontario website. However, eHealth Ontario does not provide or make available any information which could reasonably be expected to compromise the security of its ONE products or services, or the confidentiality of PHI or PI.

Any person may contact the Chief Privacy and Security Officer for more information about this Policy, or eHealth Ontario's PIA processes, reports and summaries.

---

## 5 Responsibilities

---

The Chief Privacy and Security Officer, is responsible for:

- ensuring that PTAs and/or PIAs are conducted as required on eHealth Ontario's products, services and corporate initiatives;
- approving completed PIAs; and
- ensuring appropriate risk mitigation and management strategies are in place.

The Director, Privacy is responsible for:

- determining how the PTA or PIA will be completed;
- maintaining a template for PTA and PIA reports and summaries;
- ensuring that PTAs and/or PIAs are conducted, as required, on eHealth Ontario's products, services and corporate initiatives;
- approving completed PTAs;
- collaborating with eHealth Ontario managers to ensure privacy risks are appropriately managed and mitigated;
- ensuring that privacy risks are entered into a privacy and security risk register as required; and
- ensuring PIA summaries are published and distributed as appropriate.

The Privacy Analyst is responsible for:

- collecting the required information and documentation, documenting data flows and identifying privacy risks;
- documenting this analysis in a PTA or PIA Report;
- entering the risks identified through the PTA or PIA process into a privacy risk register;
- monitoring the implementation of mitigation strategies to address identified privacy risks; and
- briefing the Director, Privacy and the Chief Privacy and Security Officer on PTAs and PIAs as required.

The eHealth Ontario Executive sponsor of the project or initiative is responsible for:

- ensuring the Director, Privacy is informed of new products, services or corporate initiatives that may require a PTA or PIA;
- ensuring that responsible parties allocate sufficient time and funds in their project plans to conduct the PTA and/or PIA;
- ensuring the availability and cooperation of sufficient personnel to facilitate information collection by the privacy analyst (or external privacy consultant) in provision of relevant, pertinent information and documentation pertaining to the solution or initiative under analysis; and
- implementing PTA and/or PIA recommendations.

eHealth Ontario shall provide a copy of this Policy to its clients when it provides ONE products and services and shall make the policy available to the public on its website. The Chief Privacy and Security Officer shall review and update this policy every two years, or more frequently at his or her discretion. The Chief Privacy and Security Officer is the ultimate authority for interpretation of this Policy.

The Chief Privacy and Security Officer is responsible for implementing and enforcing this Policy, including providing personnel with training as required. eHealth Ontario management shall assist the Chief Privacy and Security Officer as required.

Where there is a discrepancy or gap between this Policy and PHIPA, the regulations made under PHIPA, with FIPPA, the regulations made under FIPPA, or with eHealth Ontario's enabling regulation, the legislation or regulation shall take precedence. Where there is a discrepancy or gap between this Policy and the *eHealth Ontario Privacy and Data Protection Policy*, the latter shall take precedence.

## 6 References and Associated Documents

---

This policy uses or refers to the following references and associated documents:

- *eHealth Ontario Privacy and Data Protection Policy*
- *eHealth Ontario Privacy Impact Assessment Guide*