

ESPIM Report

Operating Directive

Sensitivity: Unclassified

Document Identifier: 1,119

Version: 1.01

Owner: Bobby Singh, Director, Information Security

Contents

- 1 Introduction 1**
 - 1.1 Context 1
 - 1.2 Purpose 5
 - 1.3 Guiding International Standards 5
 - 1.4 Organization 6

- 2 Operating Directives 7**
 - 2.1 Governance 7
 - 2.2 Accountability 8
 - 2.3 Programmatic Directives 9
 - 2.4 Contracts and Service Level Agreements 12

- 3 Accountabilities and Responsibilities 12**

- Appendix 'A' References 17**

Document Control

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

Document Location:	eHealth Ontario Information Security Library
Review Frequency:	Two years from last approval date.
Document Prime*	Thomas Bernard
*Enquiries relating to this document should be referred to the responsible Document Prime.	Sr. IT Security Consultant

Approval History

Approver(s)	Title	Approved Date
Bobby Singh	Director, Information Security	30 November 2007

Revision History

Version No.	Version Date	Summary of Change	Changed By
1.01	11 September 2009	Changed classification from low to unclassified	Denise Shih
1.0	31 March 2008	Final version	Thomas Bernard
0.9	30 November 2007	Final draft	Thomas Bernard
0.1	26 October 2007	First draft	Bell Canada

1 Introduction

1.1 Context

1.1.1 Enterprise Security and Privacy Incident Management (ESPIM) Objectives

The objective of ESPIM is to develop an enterprise security and privacy incident management plan, process and capability that is distributed but integrated with other incident management plans and processes to effectively and efficiently identify, contain, triage, escalate and remedy security and privacy incidents.

1.1.2 ESPIM Tasks

The primary goals and objectives of the ESPIM plan are to maintain the integrity, confidentiality and availability of eHealth Ontario's security and privacy commitments including:

- The identification, analysis, resolution and reporting of security and privacy incidents and breaches to minimize risk to individuals, clients and eHealth Ontario (the Agency)
- Providing communications guidance regarding security and privacy incidents during the process of incident handling to ensure that the rights of individuals and eHealth Ontario are protected
- The restoration of in-service system operation to base-line service levels for security and privacy as defined in eHealth Ontario Service Level Agreements (SLAs)
- The minimizing of any adverse impact on eHealth Ontario business operations
- Timely escalation to ensure the proper resources are engaged to manage the situation
- The tracking and monitoring of security and privacy incidents with effective linkage to problem management to help provide early warning for potential exposures and
- The involvement of eHealth Ontario clients and stakeholders in decision-making relative to the identification, analysis, resolution and reporting of incidents and breaches.

1.1.3 Governance Framework

Legislation, regulations and eHealth Ontario's Memorandum of Understanding (MOU) with the Ministry of Health and Long-Term Care (MOHLTC) are drivers for information security and privacy at the Agency. The business requirements collected from stakeholders (internal and external) form a significant part of the framework.

The Agency's internal governance is provided in a tiered approach, rooted in enterprise policies, as shown in Figure 1 below. Each subordinate tier draws its authority from a higher tier. Subordinate tiers are intended to support the higher tiers, providing more detail but not establishing conceptually new principles, requirements or responsibilities. Section 9.1 of the Information Security Operating Directive (ISOD) makes provisions for the existence of other operating directives.

This ESPIM Operating Directive is supported by a framework of documents, which comprise the guideline area of Figure 1: The Policy Framework. Documents include a Strategy, Refined Best Practice Model, a Concept of Operations and Security and Privacy Incident Handling Procedures.

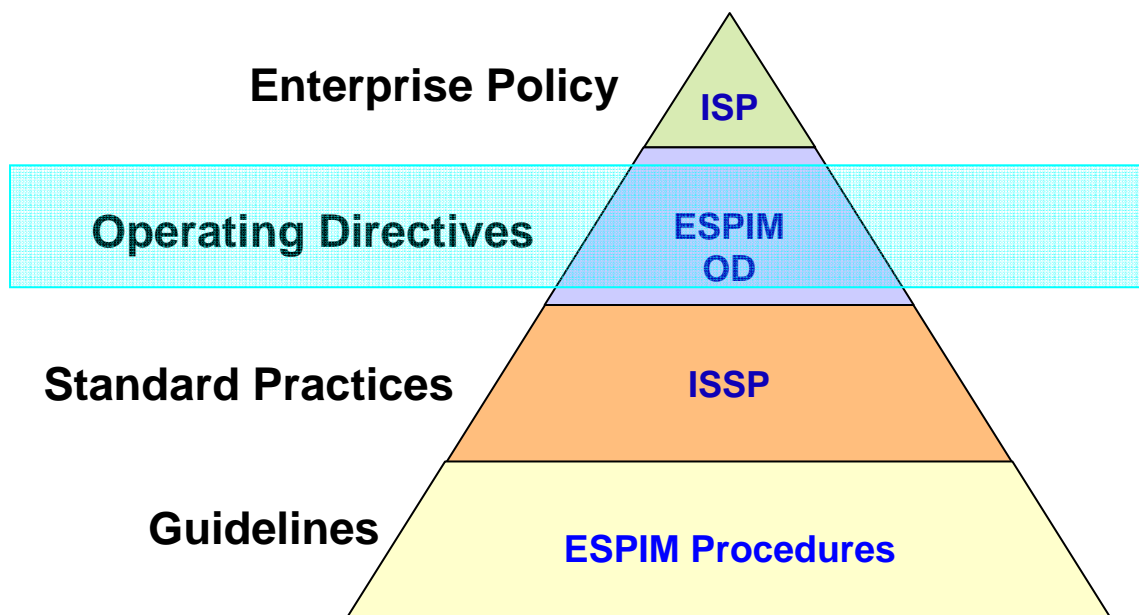


Figure 1: Policy Framework

1.1.4 Scope of Application

The scope of application, stated in Section 4 of the ISOD, also applies to this Directive. Additionally, this Operating Directive applies to clients and service providers, where a contract or service level agreement outlines the responsibilities of partners or clients.

1.1.5 Compliance

The processes, responsibilities and required outcomes specified in the ESPIM Operating Directive represent a target end-state that corresponds to a high level of capability and maturity for both security and privacy incident management within eHealth Ontario. Implementation and enforcement will be done incrementally, on the recommendation of the VP of Privacy and Security and the approval of the Information Security Program Steering Committee (ISPSC) for the ESPIM program.

The enforcement requirements, disciplinary action and appeals, (cited in Section 5 of the ISOD), apply for this Operating Directive.

1.1.6 Definitions

The ESPIM Glossary and Security and Privacy Incident Definition Matrices developed for the ESPIM initiative apply to this Directive.

Some key terms to note include:

Incident Management - All activities related to managing a security or privacy incident, beginning with the suspicion or confirmation of an incident occurring, through to and including post- incident activity such as identifying lessons learned, using incident data and evidence retention.

Privacy Incident - Unauthorized or illegal use, collection, disclosure or disposal of personal or personal health information.

Privacy Breach - When personal or personal health information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of FIPPA or MFIPPA.

Information Security – The preservation of the confidentiality, integrity and availability of sensitive information. Other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Information Security Incident – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Breach - An action by an authorized or unauthorized user that results in a negative impact or which causes interruption, disclosure, unauthorized access, modification, destruction or denial of service.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction or loss will cause perceptible damage to someone or something.

Notify - eHealth Ontario's legislated, regulatory or policy obligation to notify a personal or personal health information owner or custodian and other third parties regarding a privacy or security incident. Notification may be part of incident management.

Reporting - Mandatory communication to agencies regarding ESPIM incident occurrence, status and remedial actions.

1.2 Purpose

This Directive has been prepared to provide staff, clients and service providers with direction in those ESPIM-related activities approved by senior management. It also provides the upper level of the ESPIM Policy framework, from which subordinate security and privacy incident handling procedures can be developed and from which they will draw their authority.

1.3 Guiding International Standards

Two guiding International Standards were used as the primary basis for the policy direction of the ESPIM program: Information Technology Infrastructure Library (ITIL) and International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) Standard 17799 (2005) Code of Practice for Information Security Management.

1.3.1 Information Technology Infrastructure Library (ITIL)

eHealth Ontario has adopted Information Technology Infrastructure Library (ITIL) as its standard for IT Service Management. ITIL is a framework that documents industry best practices for the support and delivery of IT services. It provides proven methods for planning common processes, roles and activities.

Given the eHealth Ontario commitment to ITIL, this Directive also aligns ESPIM Full Operational Capability (FOC) processes and procedures with those required for effective execution of ITIL requirements.

1.3.2 ISO/IEC 17799: 2005 IT – Code of Practice for Information Security Management

Given the eHealth Ontario commitment to the International Organization for Standardization (ISO)/ International Electro-technical Commission (IEC) 17799 standard, this Directive also aligns the ESPIM FOC processes and procedures with those required for effective execution of the ISO/IEC 17799 requirements. The ISO/IEC18044 standard on Incident Management is also aligned in order to ensure that the 17799 requirement, (that incident management practice align with the18044 standard), is met.

1.4 Organization

This section addresses the Agency's organizational approach, structures and assigned responsibilities for management oversight relative to security and privacy incident management. Utilizing existing structures and adjusting terms of reference, as required, is the preferred approach. The following sub-sections define the roles and responsibilities of bodies that will be involved in the ESPIM plan.

The ESPIM Stakeholder Working Group

There is a need to establish a working-level body of stakeholders that includes eHealth Ontario, its clients and service providers to achieve and maintain alignment of ESPIM with similar capability that exists within its client and service provider organizations.

The members of such a group would logically be individuals with management responsibility for information security and privacy within their respective government and non-government organizations across the health sector. The onus to establish this stakeholder group would be on the VP of Privacy and Security at eHealth Ontario or his/her delegate(s).

The mandate of the ESPIM Stakeholder working group will include:

- Developing a shared understanding of the security and privacy incident management-related responsibilities of each organization within the complex legal and governance framework and within the complex business arrangements that exist between eHealth Ontario, its clients and service providers who may be serving either eHealth Ontario or its clients
- Coordinating, aligning and integrating security and privacy incident management approaches among the various organizations and
- Facilitating the achievement of a timely and effective process to handle security and privacy incidents.

The ESPIM Team

The roles and responsibilities for the ESPIM Team will be elaborated on in the Concept of Operations (CONOP). On an on-going basis these individuals will maintain skills and knowledge of the ESPIM process flows and procedures in their individual areas of responsibility. For the most part, they will all have other non-incident related duties to perform.

The ESPIM Incident Response Team

The specific roles of this team will be elaborated on in the ESPIM CONOP. Depending on the type of incident that must be handled, an Incident Response Team Lead will be selected and other team members will be drawn from a variety of groups within the organization and outside eHealth Ontario as appropriate, in order to respond to the detected security or privacy incident. They will follow the ESPIM process and procedures in handling the incident.

2 Operating Directives

The following must be applied in order to maintain an effective ESPIM plan and capability:

2.1 Governance

- A governance structure consisting of the organizational components cited in Section 1.4 of this Directive
- An ESPIM documentation framework, consisting of a Strategy, an Operating Directive, a Concept of Operations, a Communications Plan that includes an escalation process, a Training Plan and Incident Handling Procedures that are all mutually supportive and consistent and
- A glossary and standardized incident definition(s) for both security and privacy that will create a common understanding for the cooperative handling of security and privacy incidents among the various health sector partners.

2.2 Accountability

- The assignment of accountabilities to eHealth Ontario Executives for the management of ESPIM. Refer to Section 3 of this Directive for additional details.
- The identification of shared accountabilities between eHealth Ontario accountable executives as well as between eHealth Ontario and its clients and partners, where appropriate, to ensure effective incident resolution and decision making and
- The identification of roles and responsibilities and their assignment to eHealth Ontario managers and ESPIM team members. The ESPIM Concept of Operations further details the team structure, roles and responsibilities of the ESPIM Team.

2.3 Programmatic Directives

2.3.1 Security and Privacy Incident and Event Monitoring and Logging

- Monitoring is to be conducted in accordance with eHealth Ontario corporate policy, directives and/or standards of practice for both security and privacy and only by those personnel who have been authorized by accountable executives or their delegates to conduct such activities.
- Audit logs of security-related events on eHealth Ontario computing, networking and application systems must be produced and maintained to assist in future investigations and to monitor network and system access.
- Event and audit logs must comply with corporate monitoring and logging policy or Information Security Operating Directives (ISODs). The storage, retention and archiving requirements stated in relevant eHealth Ontario policies apply. If a system is subject to any legal, contractual or regulatory requirement that logs be retained for stated periods, then that requirement will apply.
- Appropriate access control levels must be employed to preserve log integrity. Logs must be secured so that they cannot be modified and log access must be restricted to authorized persons. Such logs may need to be encrypted, depending on the assessed risk.
- During system audits, log reviews need to be performed by an independent person other than the system administrator. This may also be identified during a risk assessment as a requirement for certain systems at all times. In these situations, a separation of roles between the system administrator and the person(s) undertaking the independent review must be established.

2.3.2 ESPIM Incident Handling

- Data produced during the handling of a security and privacy incident must be provided with appropriate security, particularly where personally identifiable information and personal health information are concerned.
- Wherever practical, common protocols will be used to handle security and privacy incidents.
- Any collection of identifiable personal information or personal health information in support of ESPIM activities must conform to legislative and regulatory requirements for privacy and with Enterprise Privacy Policy PSO 002 Section 6.4.
- The authority to disconnect clients from eHealth Ontario Services will require the approval of the accountable Executive of Infrastructure Services, in consultation with the CEO, and with Legal and Client Services guidance as appropriate. Any client requesting to be disconnected must be properly identified and authenticated to avoid eHealth Ontario liability.

2.3.3 Computer Forensics

- As the ESPIM program matures, business owners, in consultation with the ESPIM Program Manager, will explore scenarios and a process for the conducting of computer forensics.
- The ESPIM team will identify, during the triage analysis stage, where computer forensics is required and then escalate to the accountable executive(s) for approval on proceeding and the extent of law enforcement involvement.

- As ESPIM matures, involved business areas within eHealth Ontario will make provisions for audit trails and other such electronic journals to support the collection of evidence.

2.3.4 Communications

- A communications plan (notification and reporting) and guidance will be developed for the handling of privacy and security incidents.
- Disclosures of sensitive information, internal or external, by the ESPIM Incident Response Team (IRT) Lead will require the approval of the accountable executive(s) if shared accountability exists and with coordinated input from Legal, Communications and the business as appropriate.
- Communications on security and privacy incidents and/or breaches must comply with the approved ESPIM Communications Plan and escalation process.
- The ESPIM Incident Response Team Lead will consult established ESPIM protocols for reporting and notification and consult appropriate corporate offices such as Communications and Legal for their guidance.
- Each eHealth Ontario employee, contractor and eHealth Ontario service provider shall be informed of his or her obligation to immediately report any security or privacy incident to the Contact Centre. Employees must also be provided with a means of anonymously reporting privacy and security incidents. A user must promptly report to his or her supervisor any damage to or loss of computer hardware, software or information entrusted to the user.

2.3.5 Post-Incident Analysis

- The ESPIM Incident Response Team Lead will oversee post-incident analysis and the preparation of a report that will address root-cause analysis, the need for change as well as communication to all involved stakeholders including how, when and where the incident was detected and information to assist in characterizing the incident.
- The release of a post-incident report will follow the ESPIM Communications Plan protocol.
- On an annual basis, the ESPIM Program Manager shall produce a report detailing the following:
 - Types and volume of security and privacy incidents
 - Estimated cost to recover from each type of incident and
 - Identification of areas where additional controls could be used to limit the frequency, damage from and cost of future occurrences.
- The ESPIM Program Manager will ensure that eHealth Ontario Business Continuity Planning is advised of valuable outputs from the ESPIM program.

2.3.6 Testing and Training

- An annual test of the ESPIM process will be conducted to ensure the proper operation and handling of security and privacy incidents.
- A training program for primary and alternate eHealth Ontario team members and the team lead, (that is reflective of their roles and responsibilities within the ESPIM process), will be developed for ESPIM maintenance and updating.

2.4 Contracts and Service Level Agreements

- Contracts and Service Level Agreements (SLAs) with service providers and clients respectively, must reflect the application of eHealth Ontario's ESPIM plan or alignment with eHealth Ontario ESPIM requirements where equivalent client or service provider incident management processes are being applied, to ensure that incidents or breaches are handled in an efficient and effective manner.
- The notification and reporting requirements of security and privacy incident status to clients and personal or personal health information owners or custodians must be covered in eHealth Ontario's MOUs, SLAs or other appropriate formal agreements and must include both eHealth Ontario and client actions.
- Formal arrangements must reflect a line of demarcation for records retention, access to logs and other elements for criminal investigations with clients and service providers who might be implicated in a security or privacy incident or breach.

3 Accountabilities and Responsibilities

This section outlines the accountabilities and responsibilities of key eHealth Ontario stakeholders in the ESPIM process. More details on specific roles and responsibilities can be found in the ESPIM Concept of Operations. Executive leads and subordinate managers who will carry ESPIM responsibilities include:

1. The Vice-President, Privacy and Security
2. The Directors of Privacy and Information Security
3. The ESPIM Program Manager
4. The Vice-President of Client Services and the Directors of Business Delivery or Portfolios
5. The Director(s) of Internal and External Communications
6. The Vice-President of Operations and the Directors of Operations and Service Management
7. The Vice-President of Strategic Planning and
8. The Vice-President of Human Resources and the Director of Human Resources.

ESPIM-related responsibilities for these executives and managers are detailed in the following sections along with the responsibilities of other individuals at eHealth Ontario.

eHealth Ontario's Board of Directors

The eHealth Ontario's Board of Directors is responsible for the following:

- In that the ESPIM plan will contribute to the efficient and effective resolution of incidents involving security and privacy, eHealth Ontario's Board will be responsible for the oversight of eHealth Ontario's capability for security and privacy incident management.
- Communications with the eHealth Ontario CEO on security and privacy incidents, where appropriate.

eHealth Ontario's Chief Executive Officer (CEO)

The eHealth Ontario's Chief Executive Officer is responsible for the following:

- With delegated authority from the Board of Directors, eHealth Ontario's CEO will provide leadership and direction, as required, for eHealth Ontario's security and privacy incident management capability.
- Delegation of responsibility to his/her executive leads for implementing this Operating Directive within their respective areas of responsibility

- Delegation of authority to the ESPIM Incident Response Team Lead, through the VP, Privacy and Security, to take those steps deemed necessary to successfully resolve privacy and security incidents
- Delegation of authority to the VP, Privacy and Security for maintaining and monitoring compliance with ESPIM guidelines and ensuring the ESPIM program is effective in resolving privacy and security incidents throughout eHealth Ontario and
- Where ESPIM requirements are extended by virtue of contracts or service level agreements, the CEO has the authority to require his executive leads to work with clients and third party service providers to ensure that security and privacy incidents are satisfactorily resolved within their business areas.

eHealth Ontario Executives

eHealth Ontario Executives are responsible for the following activities:

- Participating in those Risk Management Committee (RMC) activities that relate to ESPIM
- Ensuring that their delegates to the Management Council are supported as required for ESPIM issues
- Ensuring that when their area engages a vendor or service provider, that the contract addresses ESPIM requirements, including the protection and disclosure of sensitive information and the relevant security and privacy training and
- Participating in security and privacy incident handling, where their action is required for the incident escalation process.

Subordinate Managers

Subordinate Managers are responsible for enforcing this Operating Directive within their respective areas of responsibility. More precisely, they are responsible for:

- Participating as required in the handling of security and privacy incidents and breaches where their action is required for the incident escalation process
- Participating as required in the ESPIM stakeholder working group and
- Ensuring that the individuals working in their respective areas of responsibility are adequately prepared to carry out their ESPIM functions and designating individuals to participate in the ESPIM incident response teams as needed. The ESPIM CONOP provides additional details on specific ESPIM Team roles and responsibilities.

ESPIM Program Manager

The ESPIM Program Manager will be responsible for the following:

- Assisting the VP, Privacy and Security with the execution of the ESPIM plan
- Acting as a single point of contact for ESPIM plan inquiries
- Maintaining the accuracy of the ESPIM process model and procedures
- Ensuring that ESPIM team training is updated as adjustments in the ESPIM plan are implemented
- Creating ESPIM incident handling teams as needed and assigning members as appropriate, to the teams
- Holding post-incident analysis and lessons-learned meetings and overseeing the preparation of reports
- Maintaining the ESPIM incident information repository
- Maintaining an ESPIM registry of action items raised during post-incident analysis

- Regularly auditing the configuration of security devices and sensors to ensure that they are adequately tuned to detect security and privacy incidents
- Regularly conducting threat environment scanning for newly identified threats to eHealth Ontario and
- Preparing reporting and metrics on key performance indicators (KPIs) of the ESPIM Team, as defined in the ESPIM Strategy.

ESPIM Team Members

ESPIM Team Members will:

- Carry out their roles and responsibilities as members of the ESPIM Team when called upon to address security and privacy incidents. Specific roles are defined in the ESPIM CONOP.
- Attend ESPIM training to ensure their skills and understanding will permit them to carry out their assigned roles within the ESPIM plan.

ESPIM Partners – Clients and Third Party Service Providers

ESPIM Partners – Clients and Third Party Service Providers will:

- Participate as required in the ESPIM stakeholder working group, (cited in Section 1.5 of this Directive)
- Participate in the resolution of security and privacy incidents or breaches as stipulated in their contract or service level agreement with either eHealth Ontario or an eHealth Ontario client and
- Conduct equivalent security and privacy incident management programs within their respective areas so that interactions and exchanges with eHealth Ontario and its partners/clients will be achievable without jeopardizing security or privacy.

Appendix 'A' References

The following documents are relevant to this Operating Directive:

- 1) Person Health Information Protection Act (PHIPA), 2004, S.O. 2004, c.3, Schedule A, Reg 329/04
- 2) Freedom of Information and Protection of Privacy Act (FIPPA), R.S.O. 1990, as amended
- 3) Information Security Policy, Version 3.0
- 4) Information Security Operating Directive (ISOD), Version 1.0
- 5) ESPIM Strategy, Version 1.0
- 6) ESPIM Concept of Operations, Version 1.0
- 7) ESPIM Incident Handling Procedures, Version 1.0
- 8) Enterprise Privacy Policy PSO-002, December 2005