eHealth Ontario
www.ehealthontario.on.ca

Information Security Policy

Document Identifier: 867

Version: 4.2

Ontario
eHealth Ontario

Table of Contents

1 Purpose / Objective

1.1 Purpose

The primary purpose of eHealth Ontario Agency (the Agency) is to provide reliable information management, information technology, and communications services to the Ontario health-care sector. Under the Personal Health Information Protection Act, 2004 (PHIPA) and Ontario Regulation 329/04, amended to O.Reg 447/08 (the Regulation) eHealth Ontario provides services under three distinctive roles:

- As a person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information
- As a health information network provider (HINP)
- As a third party retained by a HINP to assist in providing services to a health information custodian.

The security of those services and of the involved health-care information is critical to eHealth Ontario's success and the strategic objective of improving the efficiency and effectiveness of health-care in Ontario.

Loss of confidentiality, integrity, or availability of information or of the technology-based systems and services used for communications and information processing could adversely affect the achievement of goals and objectives and result in harm to eHealth Ontario, its clients, and other stakeholders.

Information security (frequently shortened to "security", below) is the discipline concerned with managing security-related risks to comply with laws and regulations, enable the achievement of objectives, and limit potential harm.

This Policy:

- defines enterprise objectives and strategy related to information security
- establishes principles for information security management
- specifies and assigns responsibilities for required elements and deliverables of the eHealth Ontario information security program
- grants authority to issue and enforce supporting governance documents
- specifies fundamental information security control requirements.

1.2 Objectives and Strategy

A key objective of this policy is to ensure that eHealth Ontario establishes accountabilities, and implements processes and controls that are consistent with the responsibilities placed on eHealth Ontario under the three roles that the Agency could play, as defined under the Personal Health Information Protection Act, 2004, and section 6.1 of Ontario Regulation 329/04 (as amended).

Information security is a means through which security-related risks can be managed to appropriate levels and the informed trust of relying parties can be gained and maintained. It is not possible or even desirable, to eliminate all risks. Information security serves the specific objectives of reducing the uncertainty and controlling the likelihood, nature, and consequences of potential unwanted events, thereby limiting harm, preserving existing value, and enabling enhanced value to be derived from information, information technology, and associated services.

Security mechanisms and practices will be implemented to appropriately protect information collected, used, stored, transmitted, disclosed or exchanged by eHealth Ontario, and to assure the continued delivery of services through the use of information systems.

To ensure consistent, effective management of security throughout the Agency, eHealth Ontario will implement an Information Security Management System (ISMS) in substantial compliance with ISO 27001:2005 and ISO 27002:2005. While responsibility for development and implementation of the ISMS lies with the Chief Privacy and Security Officer (CPSO), all organizational units must commit appropriate resources and adapt their processes to integrate, embrace, and support the ISMS.

2 Scope of Application

This Policy applies to the following:

- all organizational components of eHealth Ontario (divisions, departments, etc.)
- all eHealth Ontario personnel, including Executives, employees, consultants, and contract employees
- all information owned or controlled by eHealth Ontario or for which eHealth Ontario has stewardship or custodial responsibility
- all assets and facilities owned, leased, licensed, or managed by eHealth Ontario
- all services provided by eHealth Ontario, both internally and to clients
- all services provided to eHealth Ontario by public or private sector organizations and relied upon by eHealth Ontario for the conduct of its business

3 Management Principles

3.1 Integrated Approach

Information security controls, designed to defend against threats, preserve value, enable reliable delivery of quality services, and prevent harm, are implemented through the integrated application of people, process, and technology.

3.2 Risk Tolerance Defined by the Board

eHealth Ontario will manage its business such that residual, security-related business risks are consistent with the risk appetite and risk tolerance defined by the Board and cascaded to organizational units by Executive management.

3.3 Compliance with Legal and Regulatory Requirements

A reasonable standard of information security good practice, commensurate with perceived threats and risks, will be applied to achieve compliance with legal and regulatory requirements to protect the security of information.

3.4 Accountability and Authority for Risk Decisions

Decisions on management of security-related business risks must be made by those with accountability and authority for accepting residual risks, allocating resources for risk mitigation, and recovering from potential adverse events. Risks will be reported and aggregated upward for review and strategic direction by line Executives, the Risk Management Committee and the Audit Committee of the Board.

3.5 Interdependencies Must Be Managed

Each division and department is responsible for managing security-related business risks that directly impact the achievement of the unit's objectives. The network of interdependent services provided by all of the organizational units must be managed such that security dependencies of one service on others are explicit, understood, and satisfied, and such that the overall system of security controls is architected and implemented to be effective, efficient, and robust.

3.6 Holistic Approach

Security of information and related business services will be addressed and analyzed in a holistic manner, with attention to people, process, and technology aspects throughout the information, information technology, and associated services lifecycles. Resources will be allocated using normal business management practices to ensure alignment of security capabilities and services with enterprise needs.

3.7 Building Trust and Confidence through Security

Trust and confidence in the appropriateness and effectiveness of information security attributes of eHealth Ontario internal and client-facing services will be gained and maintained through consistent application of robust processes for:

- determination of business security objectives and requirements
- development of architecture and designs that support objectives and meet requirements
- detailed service definition, including security commitments, rules of use and behaviour, and operational monitoring and reporting
- implementation and operation in accordance with design and service definition
- identification, tracking, and resolution of security issues
- validation through timely testing, threat and risk assessments, and independent security reviews
- formal Risk Profiling and formal acceptance of material risks, and sharing of this information with affected stakeholders and clients.

3.8 Progressive Development of Capabilities

Security strategies, mechanisms, and competencies will be progressively developed and leveraged to enhance service offerings and capabilities in aid of meeting business objectives. Performance metrics will be developed and applied, with reports on status and progress presented by the CPSO to the Executive Committee and the Board on a regular basis.

4 Policy

It is eHealth Ontario policy to:

- protect the confidentiality, integrity, and availability of information in accordance with legal obligations and the reasonable requirements of the parties that control the information, the information stewards, custodians, and authorized users;
- protect the integrity and availability of information technology-based services;
- hold individual users accountable for their unauthorized or inappropriate access to, use of, disclosure, disposal, modification of, or interference with sensitive information or services. Any eHealth Ontario staff member, consultant, or employee of a vendor who violates this policy could be subject to sanctions up to and including dismissal or termination of contract;
- establish accountabilities and implement processes and controls that ensure alignment and compliance with PHIPA, O.Reg 329/04, (amended to O.Reg 447/08) Section 6.1, and the Freedom of Information and Protection of Privacy Act (FIPPA) and other legislative, policy and operational requirements specific to eHealth Ontario business areas.

Information and associated services must be secured in line with legal and business requirements and throughout their life cycles, so as to optimize the combination of net value derived and risk incurred.

Information security shall be managed in accord with the following international standards:

- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management

4.1 Information Security Program

An information security program must be developed and managed to:

- provide information security leadership and expertise
- engage and coordinate participation of key actors and stakeholders
- develop, interpret, and implement comprehensive governance
- guide and promote security strategy and security architecture, aligned with business objectives, strategy, and requirements
- develop appropriate organizational and individual awareness, motivation, and capability
- report, and make recommendations for action or improvement, to Executive management and the Board on security posture, security incidents, and the status and effectiveness of the information security program.

4.1.1 Program Management

Primary responsibility for development and management of the information security program and information security management system (ISMS), including the necessary specialist staff resources, processes, and technology, is assigned to the CPSO.

4.1.2 Governance

As part of responsibilities for the information security program, the CPSO shall develop and maintain a comprehensive framework of policy documents and supporting guidelines, and related exception procedures.

- This Information Security Policy (ISP) must be reviewed every two years and updated as needed. The ISP must be approved by the President and CEO.
- Information Security Operating Directives (ISOD) shall support the ISP by defining the information security program and ISMS in greater detail, clarifying managerial accountabilities and responsibilities, and specifying the required outcomes of management of information security. The ISOD must be approved by the President and CEO on recommendation of the CPSO.
- Information Security Standard Practices (ISSP) shall support the ISODs and ISP by documenting specific responsibilities of individuals and/or

positions and specifying the uniform practices to be adopted at eHealth Ontario to achieve the outcomes specified in the ISOD. The ISSP must be approved by the CPSO on recommendation of the Director, Information Security.

The CPSO shall set up and chair a Steering Committee, with representatives from major Agency divisions, that will provide business directions and tactical priorities for the Security Program.

4.1.3 Strategy and Plans

The CPSO shall provide leadership and expertise, and work with the other Executives, to plan and implement enterprise strategic architecture and initiatives, designed to help achieve security objectives and/or provide required security infrastructure services.

4.1.4 Capability Development

The information security program must include elements to develop appropriate organizational and individual awareness, motivation, and capability.

4.1.5 Assurance and Oversight

The information security program must incorporate monitoring, metrics, regular reporting, and management review and direction to track and progressively improve both the program and its outcomes.

The Director, Information Security must complete a periodic review of the program and its implementation across eHealth Ontario to assess the adequacy and effectiveness of the program and verify compliance with requirements of this and other related policies.

The information security program will be subject to an external audit at least once every five years.

4.2 Processes

Consistent execution of well defined processes will be an indicator of organizational capability and maturity regarding information security. The ISOD and ISSP will define processes and standard practices that all divisions, departments, and employees must apply in the development and delivery of secure services and to ensure appropriate security of information.

Where feasible and efficient, information security processes will leverage and be integrated into other business processes such as: development of business strategies and plans, risk management, opportunity assessment, new product introduction, requirements analysis, architecture, design, development, quality assurance, project management, information

management, asset management, service management, client management, procurement, contract management, personal development, and performance management.

The Director, Information Security will support Executive Leads in the development, revision (as necessary), progressive introduction in their divisions, and monitoring of the efficiency and effectiveness of these information security processes and standard practices.

4.3 Controls

The system of security controls protecting an asset or service must be designed and operated such that:

- all governance and business security requirements are met
- there is diversity and redundancy in the security controls so that unexpected failure of any given control mechanism will not result in significant harm
- the harm resulting from a security failure is limited and contained, with minimal potential to expand beyond predetermined bounds
- the control framework provides evidence / assurance of its own effectiveness, and includes mechanisms for correction of deficiencies
- residual, security-related risks are consistent with risk tolerance and risk appetite guidance cascaded from the Board.

The system of security controls and individual control mechanisms must be assessed and tested prior to use and periodically thereafter. Involved technology, products, or tools must be properly configured and operated to ensure that all security controls are effective.

The ISOD and ISSP shall define specific control requirements and practices in each of the following areas, as deemed appropriate to meet security objectives:

- internal control – defined responsibility and delegation of authority, process controls, segregation of duties, and independent reviews
- asset management – identification, stewardship, classification, labeling, security rules and requirements, and inventory
- service management – definition, responsibility, alignment with business requirements, and service integration
- contractual controls, including outsourcing
- personnel controls – screening, employment terms and conditions, compliance agreements, awareness, training, supervision, incentives, and consequences for full time and part time staff, contractors and vendors' personnel
- access control and accountability – identification, authentication, authorization, session control, non-repudiation, and audit
- physical, environmental, premises, utilities, and housekeeping controls
- cryptographic controls – protocols, algorithms, key and certificate management, and products
- planning, architecture, development, acquisition, acceptance, and maintenance

- zones and gateways – physical and network security, and remote access
- operations controls – IT service management, operating procedures, system integrity, monitoring and reporting, intrusion detection, and incident management
- assurance controls – assessment, testing, independent review, and audit.

4.4 Business Continuity

Business continuity management processes must be implemented to identify and limit to acceptable levels the business risks and consequences associated with major failures or disasters, considering both the disruption of eHealth Ontario services and the capability and time to resume essential operations.

The potential consequences of disasters, security failures, and service disruptions must be analyzed to determine the criticality of services and supporting IT infrastructure components. Integrated plans must be developed, implemented, and tested to ensure that all critical business services are maintained or can be restored on a prioritized basis, to an acceptable level and within the required time-scales, in the event of failure. Business continuity commitments for critical services must be incorporated into Service Level Agreements with clients. Disaster Recovery plans should be tested annually.

Contingency plans must provide for:

- the timely restoration of service disrupted by a failure within a system, process, or function
- the emergency recovery of service at an alternate location in the event of a disaster or prolonged outage at the primary site
- limited recovery of critical services in the event of major loss of staff.

4.5 Security Infrastructure Services

Certain security controls are best implemented by leveraging centrally managed services that are implemented and operated by staff with specialized security expertise and segregated duties.

The following security infrastructure services, to be defined in greater detail in the ISOD and ISSP, are required to support the achievement of enterprise security objectives and the delivery of secure services to clients:

- Identity Management, Authentication, and Privilege Management
- Cryptographic Infrastructure – key and certificate management
- Intrusion Detection and Incident Management
- Security Status Tracking and Reporting
- Security Assurance.

Requirements, strategy, architecture, and design for these services must be developed by, or with close involvement of, Information Security Department. Careful consideration must be given to segregation of duties in the delivery of these services.

5 Responsibilities

5.1 Audit Committee of the Board

Provide guidance and oversight for security risk management program.

5.2 President and CEO

Review and approve the Information Security Policy, on the recommendation of CPSO.

Review and approve the Information Security Operating Directives, on the recommendation of CPSO.

5.3 Senior VP, Corporate Services and Privacy

Provide business directions and confirm business priorities

Maintain relationship with the Board and communicate Board's directions with regard to risk tolerance and security risk management expectations.

Ensure that the security program is coordinated with, and has business objectives consistent with the privacy program

Approve adequate funding and resources for the security program.

Provide leadership and guidance related to employee incentives and discipline.

5.4 Executive Leads

Provide direction and oversight for management of security-related business risks within their areas of responsibility.

Commit appropriate resources and adapt processes to integrate, embrace, and support the ISMS.

Ensure that all business operations and service delivery are in accordance with this Policy, the ISOD, and ISSP.

Ensure that adequate procedures and training and awareness programs are implemented to make all employees, contractors and vendors' personnel aware of their obligations under

PHIPA and The Regulation, and that they sign an Acknowledgement of Confidentiality which clearly states their obligations in relation to access to Personal Information, and Personal Health Information, as required by sections 6 and 6.1 of the Regulation.

5.5 CPSO

Develop and manage information security governance, the information security program, the ISMS, and the necessary specialist staff resources, processes, and technology.

Champion and maintain enterprise-wide business continuity processes and plans.

Commission external audits of the information security program.

5.6 Director, Information Security

Develop and maintain information security governance documents: ISP, ISOD, ISSP, and supporting guidelines.

Develop and maintain policies and practices in accordance with section 6(3)5 of the Regulation with respect to assessment of threats, vulnerabilities and risks to security and integrity of Personal Health Information as a result of eHealth Ontario services, and support the disclosure and reporting requirements established by the Regulation.

Manage progressive development of capability and introduction of the processes and practices defined in the ISOD and ISSP, and monitor their efficiency and effectiveness to identify opportunities for improvement.

Provide expert security advice and independent security review and assessment services to assist Executive Leads and their organizations, projects, and initiatives.

Develop a security awareness program which will ensure that all employees, contractors and vendors' personnel have adequate awareness of common security threats, consequences of security incidents, and controls to safeguard information and information technology, as necessitated by their job function.

Monitor, track, and prepare regular reports on information security posture, issues, and risks across eHealth Ontario.

Complete an annual review of the information security program and its implementation across eHealth Ontario.

6 Glossary

Term	Definition
Accountability	The property that ensures that the actions of an individual may be traced uniquely to the individual, who may then be held responsible for his / her actions.
Agent	"agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated;
Assurance	The result of evidentiary processes through which one achieves confidence that objectives, commitments, and obligations are being met.
Auditability	The property that enables reliable determination of actions and qualities by tracing them, through records, to their origins or sources as they existed at a particular time.
Authentication	The process of establishing the validity of a claimed identity.
Authorization	The process of granting or denying permission for different types of access or activity, possibly with specified constraints or conditions
Availability	The property of assets and services that ensures they can be accessed and used as required, without undue delay.
CAO	Chief Administration Officer
CEO	Chief Executive Officer
Certification	Comprehensive evaluation of the technical and non-technical security features and safeguards of a technology-based service, made in support of the approval / accreditation process, to establish the extent to which the service meets specified security requirements and commitments
Compliance	Meeting the requirements of laws, regulations, policies, and standards
Confidentiality	The property that information is available or disclosed only to authorized individuals, entities, or processes.
CPSO	Chief Privacy and Security Officer
Cryptography	The art or science concerning principles, means, and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.

Harm	Loss of or damage to an organization's or a person's right, property, business, reputation, or physical or mental well-being.
Health Information Custodian	A person or organization described in the Personal Health Information Protection Act, 2004, (the Act) Section 2, who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the Act.
Identification	The process that enables unique recognition of one entity by another, generally by the use of names (e.g. user names, system names).
Identity	The set of characteristics, including physical, personal, behavioral, contextual, and/or relational characteristics, by which a person or thing is definitively recognizable or known.
Information	Consistent meaning derived from records; that which increases certainty of knowledge. Information is the meaning of the representation of a fact (or of a message) for the receiver.
Information Integrity	The property that information is valid (authentic, consistent, complete, unmodified, and fit for purpose) and can be relied upon to remain valid over time.
Information Management	Direction and control of production, use, transformation, exchange, protection, and disposal of information by an organization.
Information Security	The subject concerned with concepts, processes, and measures to manage risks and limit harm related to potential or actual, deliberate or accidental compromise of the confidentiality, integrity, or availability of information or information technology services.
Information Technology (IT)	Information technology (IT) or information and communication technology (ICT) is the computer, communications, input/output, and software technology created and used to acquire, store, combine, extract, transform, validate, protect, exchange, access, and dispose of information.
ISMS	Information Security Management System
ISOD	Information Security Operating Directives
ISSP	Information Security Standard Practices
Personal Information	Recorded information about an identifiable individual as defined in the Freedom of Information and Protection of Privacy Act, 1990, as amended, Section 2.
Personal Health Information	Identifying medical health information about an individual in oral or recorded form, as described in the Personal Health Information Protection Act, 2004, (the Act) Section 4.
Risk	Combined likelihood distribution of potential unwanted events and the

	harm they cause or their adverse affect on the achievement of objectives.
Risk Appetite	The amount of risk, on a broad level, an entity is willing to accept in pursuit of value and achievement of objectives.
Risk Assessment	Process of analyzing threats, vulnerabilities, event scenarios, and potential consequences to identify, characterize, and estimate risks and to understand the sensitivity of risks to potential business actions or environmental changes.
Risk Management	Coordinated direction and control of activities to ensure that risks are understood and appropriate, consistent with goals and objectives.
Risk Tolerance	Qualitative and quantitative acceptability bounds (upper and lower) on risks and associated potential harm or consequences to the achievement of objectives.
Threat	A potential cause of an unwanted event or incident, which may result in harm to a person or organization or impede achievement of objectives.
Vulnerability	A deficiency or weakness of an asset, process, or service that could be exploited by a threat.

7 References and Associated Documents

Reference	Location
Risk Management Policy	eHealth Ontario Enterprise Policy Document Library
Privacy and Data Protection Policy	eHealth Ontario Enterprise Policy Document Library

8 Appendix A – ISMS Architecture

This Policy is based on ISO Standards ISO27001 and ISO 17799. Together, these standards define the requirements for a comprehensive Information Security Management Systems (ISMS), which is aligned with business objectives and receives management approval for security risk management.

While the description of the ISO standards is beyond the purpose and scope of this Policy, the following figure shows the conceptual architecture for an Information Security Management Systems as defined by the standards. This Policy addresses only one component of the Governance Framework required by the standards. Additional governance, process and control documentation must be developed based on the principles and accountabilities set forth in this policy.