Ontario Health

Information Security Compliance Assurance

Prepared by: Information Security Office

November 2022

Introduction

Ontario Health's information management is subject to:

- Ontario's Personal Health Information Protection Act, 2004 (PHIPA) and corresponding regulations;
- Ontario's Freedom of Information and Protection of Privacy Act (FIPPA); and
- Connecting Care Act.

Ontario Health is designated as an "institution" under FIPPA in respect of "personal information" (PI); as a "prescribed entity," "prescribed person" (in respect of the Ontario Cancer Screening Registry and CorHealth); and as a "prescribed organization," "health information network provider," and "agent" under PHIPA in respect of PHI, depending on the context of its operation.

The collection, use, and disclosure of PI and PHI under Ontario Health's stewardship and the provisioning of information technology solutions to Health Information Custodians (as defined under PHIPA) are authorized and regulated by law. Ensuring the security of Ontario Health's information assets and the PI and PHI involved is a legal requirement that is essential to the organization's mission and objectives.

Reports on OH status as a PO, PE and PP are available from the IPC's website at: https://www.ipc.on.ca/decisions/three-year-reviews-and-approvals/three-year-reviews-and-approvals-documentation/

Ontario Health complies with the requirements of PHIPA, FIPPA, Connecting Care Act, and all regulations thereunder and

any other applicable laws for PHI, PI, and other records in OH's custody or control.

The Information Security program at OH:

- Ensures the necessary written agreements are executed and maintained where required under law or as a best practice;
- Ensures an audit trail of all accesses to PHI;
- Performs assessments of the threats, vulnerabilities, and risks to the confidentiality, integrity, and availability of the information assets, services, or other resources dealing with PHI and on request, making available a written copy of the summary of assessments to Health Information Custodians that provide PHI to Ontario Health; and
- Describes the administrative, technical, and physical safeguards relating to the confidentiality, integrity, and availability of the PHI as appropriate.

Information Security Program

Governance

The Ontario Health Board of Directors holds accountability for Information Security governance practices in support of Ontario Health's mission. Information Security risks (including the results of and recommendations arising from security audits and the status of implementation of the recommendations) along with other information technology and digital risks, are reported to the Ontario Health Board of Directors and/or the Innovation and Transformation Committee (ITC) of the Board on a quarterly basis.

Authority for the establishment of Information Security within the organization comes from the Chief Executive Officer (CEO), who is ultimately accountable for ensuring the security of all information, including personal health information, and for ensuring that Ontario Health Employees and Agents comply with the security policies, procedures and standards implemented.

The CEO appoints the Digital Excellence in Health Executive who directly reports to the CEO and is accountable for leading the digital strategy, integrating Information Security into this strategy, and ensuring the required resources.

The VP of Enterprise Products & Services and the VP of Innovations for Connected Health report to the Digital Excellence in Heath Executive. These VPs are accountable to support the implementation of the strategy through the development, operation, and improvement of the Information Security Program at an operational level. Their teams participate in, and are supported by, various formal committees including the Cyber Security Steering Committee (CSSC).

The Digital Leads Table (DLT) receives reporting on a monthly basis.

Information Security governance establishes the authority, organization structure and processes to ensure that reasonable and appropriate actions are taken to protect Ontario Health's information resources, in the most effective and efficient manner, in pursuit of its business goals. Governance is not a one-time event, but rather an ongoing process.

Monitoring and Reviewing the Information Security Program

Information Security Risk Management, Metrics & Reporting involves the ability to capture and manage an organization's key cyber security risks and compliance and report this to senior management when agreed metrics are exceeded. This ensures cyber security risks are appropriately understood and mitigation is timely and effective.

The Information Security Office and Cyber Security Defense prepare an Ontario Health Cyber Security Board Report quarterly, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework's five functions[1]: Identify, Protect, Detect, Respond, and Recover.

Security Risk Register reporting includes a log of all Security Audits. The Security Risk Register is reviewed on a weekly basis by the Information Security Office and reported quarterly to Senior Management of the Information Security Office.

The Digital Excellence in Health (DxH) Portfolio Risk Lead reviews the Security Risk Register quarterly and applies the risk prioritization and escalation criteria. Security risks with potentially enterprise-wide implications are escalated to the Digital Excellence in Heath Executive, the Enterprise Risk Management Program Office, and the Enterprise Risk Management Oversight Committee to be assessed for inclusion in the Enterprise Risk Register.

The Ontario Health Cyber Security Board Report is communicated by the VP, Enterprise Products & Services and the VP, Innovations for Connected Health to the Digital Excellence in Heath Executive who then communicates the Report to the CEO and Enterprise Risk Management Program Office.

The Ontario Health Cyber Security Board Report is presented to the Ontario Health Board of Directors and/or the ITC of the Board in person by the Vice Presidents of Enterprise Products & Services and Innovations for Connected Health and the Directors of Cyber Security Defense and Enterprise Information Security Office on a quarterly basis.

[1] https://www.nist.gov/cyberframework/online-learning/five-functions

Information Security Audit and Testing

Ontario Health implements an Information Security audit, testing and compliance program for the continuous assessment and verification of the effectiveness of Ontario Health's Information Security Program at managing OH's Information Security Risks.

The program includes the following required audits/assessments:

Compliance & Conformance Audits

Purpose:

The assessment of compliance with laws, regulations and/or contractual obligations; the assessment of conformance to security policies, procedures and practices implemented by OH.

Types:

- IPC Triennial Review
- Annual Financial Audit
- IT General Control (ITGC) Audit
- Cyber Insurance Control Attestations
- Canada Health Infoway (CHI) Certification
- Security Controls Assessments (audit of policies, standards, and procedures)

Frequency:

- Typically annually
- Every 3 years from effective date for policies / standards / procedures

Security Risk Assessments

Purpose:

The safeguarding of OH's Assets through evaluation and improvement of Information Security processes, including security risk management, Control selection and governance processes

Types:

- Threat and Risk Assessments (TRAs)
- Vulnerability Assessments (VAs)
- Security Assessments
- EHR Assessments for HSPs

• Penetration Testing / Ethical Hacks • Code reviews	• Audit of Sensitive Assets

Frequency:

- Within 5-7 years of the last security risk assessment of an existing core system / service
- Otherwise ad hoc or as established in the annual Operating Plan in accordance with section 2.2.2 Criteria Triggering a Risk Assessment

Operational Auditing

Purpose:

Real-time feedback for management to ensure that systems and Controls have been operating as designed and transactions are processed appropriately

Types:

• Reviews of system control and audit logs	• Continuous monitoring and auditing

Frequency:

- Continuous, i.e. at the normal operating frequency of the Control(s) being monitored and audited
- As required, as part of Incident investigation, troubleshooting, or system improvements
- As required, when Vulnerabilities are published by vendors