

Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) requires that custodians take steps that are reasonable in the circumstances to ensure that:

1. Personal health information in their custody or control is protected against theft, loss and unauthorized access, use or disclosure;
2. Records containing personal health information in their custody or control are protected against unauthorized copying or modification; and
3. Records containing personal health information in their custody or control are retained, transferred and disposed of in a secure manner.

The implication of this requirement is that custodians must implement information security controls to protect the personal health information in their custody or control. Custodians must regard personal health information in their custody or control as being perhaps the most sensitive information there can be about an individual and must manage the information with due diligence and take appropriate measures to safeguard it from injury.

The contents of this document are intended to serve as a very brief introduction to information security and to some of the aspects of information security that custodians of personal health information may need to consider in order to fulfill their responsibilities and obligations under PHIA.

Information Security is a Process

Information security is simply the process by which information confidentiality, integrity, and availability are safeguarded and ensured. No one product, process or technology alone can provide for every information security issue faced by a custodian; rather, effective information security requires the successful integration of:

- **Physical** security controls, such as door locks, alarm systems and segregated working areas;
- **Administrative** security controls, such as policies, procedures and guidelines documents; and,
- **Technological** security controls, such as firewalls, intrusion detection systems and encryption applications.

Controls of all three types must be developed to work in concert with one another in order to create an effective information security framework.

Personal health information must be safeguarded according to baseline security requirements and continuous security risk management. Continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

Information Security Management – Key Practices

The following is a list of key information security practices that custodians of personal health information should consider when implementing their information security program. These practices have been derived from the internationally-recognized ISO 27002 information security standard published by the International Organization for Standardization (ISO), and represent the different aspects that comprise a comprehensive information security management program.

It should be noted that while addressing each of the following practices will result in a comprehensive security framework, custodians may not need to address certain of the following, depending on the nature and scope of their operations. These practices should be read as being guidelines to inform the development and implementation of an information security management framework: rather than being a comprehensive list of things that custodians *must* do, these practices should be viewed as being a list of things that custodians should consider the necessity of, in the context of their particular work, line of business and / or operations.

Common Information Security Practices

1. Security Policy Management

- 1.1. Establish a comprehensive information security policy

2. Corporate Security Management

- 2.1. Establish an internal security organization
- 2.2. Control external party use of your information

3. Organizational Asset Management

- 3.1. Establish responsibility for your organization's assets
- 3.2. Use an information classification system

4. Human Resource Security Management

- 4.1. Emphasize security prior to employment
- 4.2. Emphasize security during employment
- 4.3. Emphasize security at termination of employment

5. Physical and Environmental Security Management

- 5.1. Use secure areas to protect facilities
- 5.2. Protect your organization's equipment

6. Communications and Operations Management

- 6.1. Establish procedures and responsibilities
- 6.2. Control third party service delivery
- 6.3. Carry out future system planning activities
- 6.4. Protect against malicious and mobile code
- 6.5. Establish backup procedures
- 6.6. Protect computer networks
- 6.7. Control how media are handled
- 6.8. Protect exchange of information
- 6.9. Protect electronic commerce services
- 6.10. Monitor information processing facilities

7. Information Access Control Management

- 7.1. Control access to information
- 7.2. Manage user access rights
- 7.3. Encourage good access practices
- 7.4. Control access to network services
- 7.5. Control access to operating systems
- 7.6. Control access to applications and systems
- 7.7. Protect mobile and tele-working facilities

8. Systems Development and Maintenance

- 8.1. Identify information system security requirements
- 8.2. Make sure applications process information correctly
- 8.3. Use cryptographic controls to protect your information
- 8.4. Protect and control your organization's system files
- 8.5. Control development and support processes

9. Information Security Incident Management

- 9.1. Report information security events and weaknesses
- 9.2. Manage information security incidents and improvements

10. Business Continuity Management

- 10.1. Use continuity management to protect your information

11. Compliance Management

- 11.1. Comply with legal requirements
- 11.2. Perform security compliance reviews
- 11.3. Carry out controlled information system audits

12. Risk Assessment

- 12.1. Threat and risk assessment and identification

12.2. Risk mitigation

Implementation of Information Security Program

Information security management is generally considered to be a specialized field for subject-matter experts in Information Management and Information Technology. Custodians of personal health information should consult with internal or external subject-matter experts when developing and implementing their information security management strategies.