OIPC Guidance

# Reasonable Safeguards

## Purpose

This guidance is to assist public bodies subject to the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015) and custodians subject to the **Personal Health Information Act** (PHIA) in understanding their obligations to ensure reasonable safeguards are in place to protect the personal information and personal health information in their custody or under their control.

## Introduction

Meeting the standard of reasonable security set out in ATIPPA, 2015 and PHIA does not guarantee that privacy breaches will not occur. However, being able to demonstrate that reasonable security safeguards were in place at the time of a breach is a strong indicator of due diligence and compliance with the law. If an organization (public body or custodian) experiences a privacy breach, which later becomes the subject of an investigation by the Office of the Information and Privacy Commissioner (OIPC), one of the key considerations for any such investigation is what security measures were in place at the time of the breach, and whether those measures were reasonable in light of the contextual factors outlined below. In other words, an organization can experience a serious privacy breach and still be fully compliant with ATIPPA, 2015 or PHIA, but only if it can demonstrate that it met the reasonable safeguard requirements set out in the legislation.

## Reasonable Safeguards

Section 64(1) of ATIPPA, 2015 states:

> 64.(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that
>
> (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;
>
> (b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and
>
> (c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

Section 15(1) of PHIA states:

> 15.(1) A custodian shall take steps that are reasonable in the circumstances to ensure that
>
> (a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;
>
> (b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and

> (c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

## What is Reasonable?

Reasonableness refers to the appropriateness of the safeguards in a given circumstance and should be proportionate to the sensitivity of the information involved. Some considerations include:

- the impact a data breach would have on individuals;
- the volume of information;
- the type and level of risks involved;
- the cost of safeguards in relation to cost of system; or
- legacy system –when legacy systems are upgraded or modified, it may provide an opportunity to address privacy and security risks.

Commissioner Reports from this jurisdiction and other Canadian jurisdictions discuss the criteria used to determine if safeguards are reasonable. In Report P-2008-002, this Office identified four criteria it would consider when determining if reasonable safeguards were in place, including:

- the foreseeability of the privacy breach;
- the seriousness of potential harm;
- the cost of preventative measures; and
- the relevant standards of practice.

While this Report was issued after a privacy breach, the same criteria could be used in a proactive fashion to better ensure a breach does not happen.

The Office of the Information and Privacy Commissioner of British Columbia noted in Investigation Report F12-02 that:

> The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, how the costs of security are estimated, the relationship between the public body and the affected individuals and how valuable the information might appear to someone intending to misuse it.

British Columbia's Commissioner also noted in Investigation Report F06-01: "The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances."

Reasonableness applies throughout the life cycle of the information, from initial collection to secure destruction. Organizations should remember that what is considered reasonable may

also change over time. For example, you may collect additional information, new threats may emerge, or, for legacy systems, new features may become available.

## Types of Safeguards

Safeguards can be grouped into three categories: administrative, technical, and physical.

### Administrative Safeguards

Administrative safeguards are the policies, procedures, and practices in place to protect the privacy of personal information. Some common administrative safeguards include, but are not limited to:

- developing a Privacy Management Program;
- appointing a Privacy Officer;
- implementing privacy and security policies and procedures that address acceptable use of systems, respect for privacy, staff training, as well as the collection, use, disclosure, retention, and disposal of personal information;
- conducting regular training and awareness activities;
- ensuring there is a privacy breach and incident response plan that includes processes for containment, investigation, notification, and mitigation; or
- identifying required documentation, including privacy impact assessments, threat risk assessments, information sharing agreements, confidentiality oaths or affirmations, etc.

TIP: Determining what safeguards should be included in policies depends on a variety of factors, including the sensitivity of the information and whether the information is in hardcopy or electronic format. For example, a policy concerning information on an electronic system could inform staff about login requirements and passwords, as well as requirements to log out and not share passwords. In addition, if the electronic system is hosted or supported by a third-party provider, a policy should address requirements such as information sharing agreements.

### Technical Safeguards

Technical safeguards involve the use of technology to protect personal information. Common technical safeguards include, but are not limited to:

- encryption (consider the strength of encryption, as well as if data needs to be protected in transit and at rest);
- access controls to control access to systems and data (could include role-based access, strong authentication mechanisms like multi-factor authentication, and strong passwords);
- network security like firewalls, intrusion detection or prevention systems, and secure network configurations;

- regular updates and patch management;
- monitoring and logging of access to and use of personal information; or
- conducting regular audits.

Organizations should monitor technology changes and threats to ensure they keep technical safeguards current. Keeping up with technology changes and threats may be difficult with the rapid pace of this environment. Some organizations monitor technological changes and threats through efforts such as:

- relationship building and networking with peers in similar industries or positions;
- monitoring media stories, industry publications, and similar resources; and
- staying current with alerts and updates issued by entities such as the Canadian Centre for Cyber Security.

Organizations relying on third-party information managers or information security contractors should ensure they have clear contract language in place setting out expectations for the security of the information being protected.

TIP: When looking at upgrading or replacing a legacy system, it should not be assumed that what was accepted as reasonable in the past will be accepted as reasonable today. For example, many older systems lacked robust audit capabilities. Currently, vendors have recognized the importance of such audit capabilities and offer improved options.

### Physical Safeguards

Physical safeguards are steps taken to protect physical access to buildings and assets where personal information is stored or handled. Common physical safeguards include, but are not limited to:

- restricting access to buildings, including locks, card readers, video surveillance or security personnel;
- protecting assets that store or handle personal information, like servers, using locks, cable management, or secure storage areas; or
- protecting assets against environmental threats, such as fire and temperature extremes.

## Conclusion

A reasonable safeguard is one that is risk-based and considers the sensitivity and volume of the information involved. It is fact-specific, contextual, and must consider the totality of circumstances of the particular case. If a breach occurs, organizations must assess the risk of personal information being inappropriately accessed or disclosed, focusing on the potential impact to the individual and put in place measures to reduce the risk of future incidents. In general, an organization should use layers of technical, administrative, and physical safeguards to ensure that it is in compliance with the requirements established in ATIPPA,

2015 and PHIA. Safeguards should be regularly reviewed to ensure they remain reasonable in light of evolving threats, changes in standards or laws, and technological advancements.

For public bodies and custodians looking for additional resources, Appendix A contains a non-exhaustive list of some international guidelines and frameworks that may assist with their understanding of what is considered reasonable.

## Resources

Office of the Information and Privacy Commissioner of Newfoundland and Labrador

Office of the Chief Information Officer Cyber Security Guidance

Access to Information and Protection of Privacy Office ATIPPA, 2015 Resources

Department of Health and Community Services PHIA Resources

Securing Personal Information: A Self-Assessment Tool for Public Bodies and Organizations
Office of the Information and Privacy Commissioner for Alberta, Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia

Office of the Information and Privacy Commissioner of Nova Scotia's Reasonable Security Checklist for Personal Information

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
https://www.oipc.nl.ca

# Appendix A: Frameworks and Guidelines

The following is in alphabetical order, is for reference purposes only, and is not intended to be an endorsement.

For public bodies and custodians looking for additional resources, here is a non-exhaustive list of some international guidelines and frameworks.

Canadian Centre for Cyber Security (CCCS)

CCCS has a number of resources, including a Security Audit Program, which is part of a series of tools for auditors to use to assess the cyber security status of organizations.

International Organization for Standardization (ISO)

ISO has a number of standards that may be considerations, including:

- ISO/IEC 27001: standard for Information Security Management Systems (ISMS); and
- ISO/IEC 27002: guidance focused on cybersecurity, offering best practices and control objectives, to establish, implement and improve an ISMS.

National Institute of Standards and Technology (NIST)

NIST has a number of frameworks that may be considerations, including:

- Privacy Framework: assists organizations manage privacy risks and protect individuals' personal information;
- Risk Management Framework: offers a structured process for managing risk to organizational operations and assets; and
- Cybersecurity Framework: provides guidelines for improving cybersecurity practices in organizations, focusing on identification, protection, detection, response, and recovery.

Open Worldwide Application Security Project (OWASP)

OWASP is a nonprofit foundation that works to improve the security of software; they provide a top ten list for privacy risks in web applications and related countermeasures.

Organization for Economic Co-operation and Development (OECD)

The OECD has guidelines on the protection of privacy and transborder flows of personal information.

Privacy by Design (PbD)

PbD incorporates seven principles designed to anticipate and prevent privacy invasive events before they occur.