Our Vision
Better data. Better decisions. 
Healthier Canadians.

Our Mandate
To lead the development and 
maintenance of comprehensive 
and integrated health information 
that enables sound policy and 
effective health system management 
that improve health and health care.

Our Values
Respect, Integrity, Collaboration, 
Excellence, Innovation
## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-07-16</td>
<td>1.0</td>
<td>Document for approval</td>
<td>CISO and CPO</td>
</tr>
</tbody>
</table>

## Approval

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Approval authority</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-07-16</td>
<td>1.0</td>
<td>Senior Management Committee</td>
<td>Approved</td>
</tr>
</tbody>
</table>
# Table of contents

1 Introduction ................................................................................................................ ............ 5  
1.1 Overview .................................................................................................................. ... 5  
2 Alignment with Corporate Risk Management Framework ..................................................... 6  
3 Why PSRM? ................................................................................................................... ....... 7  
4 Risk management governance ......................................................................................... 8  
5 CIHI’s risk tolerance ............................................................................................................. 9  
6 PSRM methodology ........................................................................................................ 10
1 Introduction

1.1 Overview

Privacy and security risk management (PSRM) is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur.

This PSRM Framework provides an overview of PSRM at the Canadian Institute for Health Information (CIHI), including its alignment with CIHI’s Corporate Risk Management Framework, drivers for PSRM, the governance model, CIHI’s risk tolerance and the PSRM methodology.
2 Alignment with Corporate Risk Management Framework

This PSRM Framework has been designed to integrate and align with CIHI’s Corporate Risk Management Framework, shown below:

PSRM informs and aligns with corporate risk management activities through

- Adopting a similar methodology, terminology and governance structure; and
- Identifying privacy and security risks for potential inclusion on the Corporate Risk Register.
3 Why PSRM?

Effective management of privacy and security risks is essential for CIHI to achieve its strategic goals and is a core requirement for CIHI’s continued designated status under the *Personal Health Information Protection Act* (PHIPA) of Ontario.

Adopting an effective and robust PSRM program contributes to stakeholder and public trust by demonstrating CIHI’s commitment to protecting the personal health information that it maintains.

By implementing a continuous, proactive and systematic process to understand, manage and communicate privacy and security risks, CIHI can make sound strategic and tactical decisions based on real risk, cost and benefit.
4 Risk management governance

CIHI’s chief privacy officer (CPO) and chief information security officer (CISO) have primary responsibility for CIHI’s PSRM Program. CIHI has defined management responsibilities and a governance framework for effective PSRM, as shown in the figure below.

**Senior Management Committee (SMC)**
Accountable for privacy and security risk management
- Ensure PSRM is implemented enterprise-wide
- Support the PSRM Program
- Resolve escalated issues
- Provide oversight and direction for enterprise-level risks and treatments
Individually, members are responsible for PSRM within their area.

**Privacy, Confidentiality and Security Team**
Monitor and review PSRM Program
- Review and approve Privacy and Security Risk Register on a regular basis

**CPO and CISO**
Develop, implement, manage and coordinate PSRM Program

**CIHI’s Corporate Risk Management Program**

**Information Security Management System (ISMS) Risk Management Program**
5 CIHI’s risk tolerance

It is not always efficient or possible to eliminate risk due to the time, cost or effort that would be required, or because of other constraints. On the other hand, risks that are clearly inconsistent with CIHI’s vision, mandate and strategic goals may not be acceptable. On this basis, CIHI has developed a privacy and security risk tolerance statement that sets out the amount of residual risk it is willing to bear as part of normal management practice.

CIHI is willing to accept risk that

- May result in minor delays in achieving CIHI’s objectives;
- Does not lead to financial losses;
- May result in some potential for minor complaints, non-compliance issues or negative media coverage;
- May lead to some impact on public perception;
- May cause low stakeholder concern; and
- May lead to a potential minimal impact on service delivery.

The consequences of the risk event could be absorbed by normal activity or with minimal effort.
CIHI’s PSRM methodology is made up of the following 4 steps:

1. **Identify risk**: Risks are identified through a variety of sources and are entered into the Privacy and Security Risk Register.

2. **Assess risk**: Risk likelihood and impact are assessed in order to determine whether risk treatment is required. Risks that are within CIHI’s identified risk tolerance require no treatment.

3. **Treat risk**: Options for risk treatment are mitigating the risk, transferring the risk, avoiding the risk or accepting the risk.

4. **Monitor and review risk**: Risks and risk treatments must be continually monitored to ensure that CIHI’s assets are adequately protected.
Talk to Us

**CIHI Ottawa**
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860

**CIHI Toronto**
4110 Yonge Street, Suite 300
Toronto, Ontario M2P 2B7
Phone: 416-481-2002

**CIHI Victoria**
880 Douglas Street, Suite 600
Victoria, British Columbia V8W 2B7
Phone: 250-220-4100

**CIHI Montréal**
1010 Sherbrooke Street West, Suite 300
Montréal, Quebec H3A 2R7
Phone: 514-842-2226

**CIHI St. John’s**
140 Water Street, Suite 701
St. John’s, Newfoundland and Labrador A1C 6H6
Phone: 709-576-7006