HIA Fact Sheet: Privacy impact assessments

The *Health Information Act* (HIA) includes requirements for privacy impact assessments.

Overview

A privacy impact assessment (PIA) is a due diligence assessment of privacy considerations. It helps custodians identify and address privacy risks in instances including but not limited to:

- implementing or changing administrative practices
- implementing or changing information systems
- participating in common or integrated programs or services (CIPS)
- becoming a sharing custodian of shared health information

The process helps custodians:

- ensure proposed actions are authorized by the HIA
- strengthen privacy and transparency by identifying how health information is collected, used, disclosed and protected
- manage risks related to health information in their custody or control
- meet compliance obligations under the HIA and regulations

A PIA documents these activities and supports informed decision-making about how to meet their obligations under the HIA. It can also identify high-risk issues and prompt consideration of alternative technologies, products or service designs. This may help prevent privacy breaches and reduce time and cost.

As a best practice, PIAs should be reviewed regularly and updated if there are significant changes.

When to complete a PIA

A PIA is required in several circumstances under the HIA. Each custodian is responsible for determining whether their projects, practices or systems meet the criteria.

This fact sheet outlines common requirements. Other situations may also require a PIA. For more information, contact the HIA Help Desk: HIAHelpDesk@gov.ab.ca.

General PIA requirements

A PIA is required:

- before implementing new administrative practices involving the collection, use or disclosure of individually identifying health information
- before making changes to administrative practices involving the collection, use or disclosure of individually identifying health information
- before implementing new information systems involving the collection, use or disclosure of individually identifying health information
- before making changes to information systems involving the collection, use or disclosure of individually identifying health information

Departmental custodians, ministerial custodians, provincial health corporations, provincial health agencies, Health Quality Alberta, and the Canadian Centre of Recovery Excellence are not required to complete a PIA for the collection, use or disclosure of health information among themselves for a purpose authorized under section 27(2), unless they are introducing a new information system or changing an existing one.

Other PIA Requirements

A PIA is also required:

- before becoming a sharing custodian
- before participating in a common or integrated program or service (CIPS)
- before performing data matching with other custodians or non-custodians

Submitting to the Information and Privacy Commissioner

Custodians must submit a PIA to the Information and Privacy Commissioner for review and comment before implementing an initiative.

If a PIA has already been prepared and submitted, custodians may amend the existing PIA to reflect changes instead of creating a new one.

PIA contents

A PIA should include enough detail to reflect:

- the level of risk
- the sensitivity of information
- the complexity of the initiative

Simple initiatives (for example, implementing a manual intake process) may require less detail than more complex initiatives (such implementing a new electronic medical record or participating in a CIPS).

All PIAs must set out each of the following in enough detail considering the complexity of the PIA:

- a summary of each type of health information involved and the purpose for its collection, use or disclosure
- the legal authority for collecting, using or disclosing the health information
- identified privacy risks and mitigation strategies
- administrative, physical and technical safeguards, including how health information will be securely transmitted, matched or linked
- relevant provisions of any agreements required under section 54 or 66
- any portions of a previously reviewed PIA that are incorporated, including any modifications

Specific PIA contents

Information systems

PIAs related to information systems must include all general contents and:

- identify and assess risks associated with the collection, use and disclosure of health information
- Identify measures that protect the privacy of the individuals who are the subjects of the health information; and
- address the security and confidentiality of health information

Common or integrated programs or services

PIAs related to CIPS must include all the general contents and describe the governance structure, including the roles of each custodian and public body involved.

Shared health information

PIAs for sharing custodians must include all the general contents and a description of the common policies and procedures that sharing custodians must adopt under section 4 of the Health Information (Ministerial) Regulation before making health information accessible to another sharing custodian or authorized user.

Data matching

PIAs for projects involving data matching must include all the general contents and:

- describe how the information used in data matching will be collected
- explain how information created through data matching will be used or disclosed

Related resources

- Fact Sheet: Common or Integrated Program or Service
- Fact Sheet: Shared Health Information
- Fact Sheet: Privacy Management Programs

Contact

HIA Help Desk provides general information about the HIA and health information privacy in Alberta.

- Phone: 780-427-8089 or Toll free: 310-0000 before the phone number (in Alberta)
- Email: hiahelpdesk@gov.ab.ca