

Information Sharing Guideline

Updated July 2007

Prepared by: Information Sharing Working Committee
Alberta Children and Youth Initiative

Updated by: Information Sharing Advisory Committee
Information Sharing Training Initiative



Executive Summary

The Alberta Government is committed to ensuring that public services provided to individual Albertans are effective and well-coordinated. When various government ministries work together to provide a number of services to the same individual or family, they seek to collaborate to ensure those services are complimentary and harmonized. As such, public sector and service provider organizations that provide care and support to children, youth, adults and families need to be able to share personal and health information with each other in order to enhance, and more effectively deliver, those services in a collaborative and integrated approach. Service providers who work with individuals and families often express reluctance to share information regarding these individuals and families, with staff from other public sector and service provider organizations because they believe that existing privacy legislation prevents them from doing so.)

The Alberta Children and Youth Initiative (ACYI), is a collaborative partnership of government ministries working together on issues affecting children and youth. Children's issues cross many sectors and organizations, including government ministries. As such, these organizations providing care and support to children and their families need to be able to share personal and health information with other organizations in order to enhance and more effectively deliver those services in a collaborative and integrated fashion. Many staff working with children have expressed that they are reluctant to share information regarding these children with staff from other sectors because they perceive that existing privacy legislation prevents them from doing so.

A Government of Alberta cross-ministry Information Sharing Committee has examined barriers to information sharing among public sector and other service provider organizations regarding children, youth, and families, including those who are at risk or who pose a risk. A Guideline has been developed to articulate Government's support for sharing needed information to better serve individuals and their families. The concept of the Guideline and training tools were developed in consultation with cross-sector focus groups representing a mix of government, not-for-profit and private sector organizations who provide public services directly or under contract.

The delivery of services in an integrated or collaborative manner encounters the same issues, and follows similar processes whether the client groups are children, youth, adults or families; whether requiring supports due to disabilities, or issues facing their personal or family circumstances; or in need of services that cross sectors. The Guideline has been updated to incorporate the recognition that it has application to services being provided to adults as well as to children, youth and families. In addition, the proclamation and implementation of the *Personal Information Protection Act (PIPA)*, and the implementation of the training initiative are also dealt with in this updated version.

The vision of the Information Sharing Guideline (the Guideline) is to ensure that integrated planning and services for children, youth, adults and families are supported by appropriate cross-sector information sharing. The Guideline identifies the processes by which information can be shared between service providers (and others) who are providing services and supports to the same child, youth, adult and family. The guiding principles support this overall vision.

The purpose of the Guideline is to:

- enable the sharing of necessary information about children, youth, adults and families among service providers, and minimize barriers, perceived or real;
- support an integrated approach to service delivery, by strengthening the ability to share required information about children, youth, adults and families, based on consent; and
- enable effective coordination of supports and services by service providers, including the ability to collectively plan short- and long-term interventions.

The Guideline provides a foundation for the sharing of information among public sector and service provider organizations in the best interests of children, youth, adults and families.

Table of Contents

	Page
Executive Summary	i
I. Introduction.....	1
II. Purpose of a Guideline	2
III. Vision.....	3
IV. Principles.....	4
V. Information Sharing	5
VI. Guideline Directions	6
Direction #1—Integrated Service Approach	6
Direction #2—Consent-Based Approach.....	7
Direction #3—Training and Implementation	9
VII. Outcomes	12
VIII. Future Directions for the Guideline.....	13
Appendix 1: Background for the <i>Information Sharing Guideline</i>	14
1.0 BACKGROUND.....	14
2.0 LEGISLATION.....	14
3.0 CONTEXT	17
4.0 PARAMETERS.....	21
5.0 INFORMATION SHARING IN SUPPORT OF COMMON AND INTEGRATED PROGRAMS AND SERVICES	26
6.0 The Information Sharing Guideline for Integrated Service Delivery	29
7.0 Glossary of Terms	33
Appendix 2: Selected sections of the Freedom of Information and Protection of Privacy Act	36
Appendix 3: Selected Sections of the Health Information Act	40
Appendix 4: Selected Sections of the Personal Information Protection Act	53
Appendix 5: Selected Sections of the Personal Information Protection and Electronic Documents Act	58
Appendix 6: Selected Sections of the Privacy Act.....	60

I. Introduction

Public sector and service provider organizations, including custodians of personal health information, who provide care and support to children, youth, adults and families, need to be able to share personal and health information within their custody with other service providers. The sharing of personal and health information will assist organizations to enhance and more effectively deliver those services in a collaborative and integrated approach. The Alberta Children and Youth Initiative (ACYI) Deputy Ministers agreed to support a committee that would examine barriers to information sharing among public sector and service provider organizations regarding children and youth who are at risk or who pose a risk.

The ACYI¹ Information Sharing Committee was charged with the responsibility of developing a process that would remove barriers and enable the sharing of information about children and youth. The committee, co-chaired by Alberta Solicitor General and Alberta Learning (currently Alberta Education and Technology), included representatives from the ministries, boards, police services and agencies involved in the ACYI. The Office of the Information and Privacy Commissioner was represented in an advisory capacity.

¹ ACYI partners include the following ministries: Advanced Education and Technology, Children's Services, Education, Health and Wellness (including AADAC and the Alberta Mental Health Board), Employment Immigration and Industry, Justice and the Attorney General, Seniors and Community Supports, and Solicitor General and Public Security.

II. Purpose of a Guideline

The purpose of the Guideline is to identify the processes by which information can be shared between service providers who are providing services and supports to the same child, youth, adult or family.

Specifically, the Guideline is intended to:

- enable the sharing of necessary information about children, youth, adults and families among public sector and service provider organizations, and minimize real or perceived barriers to information sharing;
- support an integrated approach to service delivery by strengthening the ability to share information about children, youth, adults and families based on consent; and
- enable effective coordination of supports and services by public sector and service provider organizations, including the ability to collectively plan short- and long-term interventions.

III. Vision

Integrated planning and service delivery for children, youth, adults and their families are supported by appropriate cross-sector information sharing.

The information sharing vision is based on the following assumptions.

- Children, youth, adults and families benefit from an integrated approach to planning and service delivery.
- Children, youth, adults and families are involved, are informed and whenever possible, provide consent to plans and services that involve them.
- Legislation permits the sharing of information within certain guidelines and parameters.
- Children, youth, adults, families, and public sector and service provider organizations including government ministries and custodians of personal health information have access to clear, easy-to-understand guidelines for information sharing.

IV. Principles

The following principles provide direction for sharing information related to providing services and supports to children, youth, adults and families.

- **Respect for Privacy** — The right to individual privacy of children, youth, adults and families must be respected. Only the minimum amount of personal and health information necessary may be shared within the requirements of existing legislation.
- **Consent Based** — Informed consent from the individual or their parent/guardian where appropriate, is the preferred method of enabling the sharing of information among professionals and service providers.
- **Coordinated Services and Supports** — Children, youth, adults and families are better served when services and supports are provided in a holistic manner that considers the needs and resources required to meet those needs in an integrated approach, rather than in isolation.
- **Clarity** — Children, youth, adults and families must be helped to understand why and how their information will be shared and how services will be provided as a result of the information being shared.

V. Information Sharing

Public sector and service provider organizations, including custodians of personal health information, provide care and support to children, youth, adults, and their families. These organizations often need to share personal and health information within their custody with other service providers in order to enhance and more effectively deliver those services in a collaborative and integrated approach. The *Freedom of Information and Protection of Privacy Act* ([FOIP](#)), *Health Information Act* ([HIA](#)), *Personal Information Protection Act* ([PIPA](#)), *School Act*, *Child, Youth and Family Enhancement Act*, *Youth Criminal Justice Act* and other legislation are continuously reviewed to ensure the Guideline remains in compliance with legislated changes.

Although information sharing across ministries and mandates is complex, current privacy legislation allows for information sharing within clearly defined boundaries. Appendix 1 provides background and further information regarding legislation, and Appendices 2, through 6 contain relevant sections of the *Freedom of Information and Protection of Privacy Act*, the *Health Information Act*, the *Personal Information Protection Act (PIPA)*, the federal *Privacy Act*, and the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* respectively.

Enhancing collaborative and holistic service delivery to children, youth, adults and families in a community-based environment is the primary reason for the development of an Information Sharing Guideline. The Guideline not only supports the delivery of [integrated services](#) to meet the needs of children, youth, adults and families, it is also in compliance with the requirements of existing privacy legislation.

VI. Guideline Directions

There are three major directions that comprise this information sharing guideline.

Direction #1—Integrated Service Approach

Information sharing within an integrated service approach will facilitate the delivery of services to children, youth, adults and families.

Services to individuals are not always effective or complete when delivered in isolation from those delivered by other service providers, and without involvement of the family and their natural supports. Services and plans may at best be successful in dealing with only a portion of the child's/youth's/adult's needs. Those successes may not be sustainable in the long term if other issues are not addressed.

The following direction is based on the ability to share information within an integrated service approach. According to the definition in the FOIP Bulletin², "integrated" means that the program or service has several distinct components, each of which may be delivered separately, but when considered together, comprise the complete program or service.

Participants within an integrated service can share information, **with or without consent**, under FOIP. The FOIP Act allows for the disclosure of personal information to another public body if the disclosure is necessary for the delivery of an integrated program.

Organizations who need to share information on an ongoing basis (e.g. those who deliver the Student Health Initiative, Early Intervention Initiatives, Children and Youth with Complex Needs Initiative) are encouraged to formalize their involvement in an integrated service approach. Organizations not using this approach are not prevented from disclosing personal information on a case-by-case basis provided that such disclosure is made in accordance with the relevant privacy legislation or governing legislation.

Organizations that propose to facilitate the sharing of information within an integrated service approach need to ensure that their service provision incorporates the following elements:

1. Purpose — a statement of what the integrated service will be.
2. Authority — the authorities, policy, or legislation that authorize the disclosure or sharing of personal and health information.

² see [FOIP - Bulletin Number 8: Common Programs and Services](http://foip.gov.ab.ca/resources/publications/bulletin8.cfm)
(<http://foip.gov.ab.ca/resources/publications/bulletin8.cfm>)

3. Integrated Service Providers — which ministries, bodies or agencies will be providing the integrated service.
4. Statement of Use/Notification — this will outline how personal and health information will be used and shared by the service providers.
5. Records — a description of how personal and health information records will be kept and for how long.
6. Access — a process must be developed to allow individuals to access their own personal and health information.

Refer to [Appendix 1](#) for further details on these elements and a sample Terms of Reference for formalizing the process.

Direction #2—Consent-Based Approach

Services to children, youth, adults and families will incorporate a consent-based approach to information sharing whenever possible.

Privacy legislation in the public and private sectors imposes different legal obligations with respect to the collection and disclosure of personal information. Public bodies subject to the FOIP Act must be authorized to collect personal information. Government agencies should not exceed their mandates, although they can use and disclose personal information for other purposes with consent.

Custodians subject to HIA can collect and disclose health information within an arena of health service providers, but generally require consent otherwise. Organizations subject to PIPA will normally require consent to collect, use or disclose personal information. Where contracts are involved, the legislation governing the principal will apply to personal information or health information in the custody of the service provider.

To facilitate delivery of an integrated program or service, program or service partners need to consider their own legal obligations as well as the obligations of their partners. Applying the relevant legislation within a formally coordinated program need not be unduly onerous. An approach based on

- A clear mandate to provide the program or service, or part of the integrated program or service
- Collection of personal information or health information only to the extent necessary for the program or service
- Notification of the purposes of the collection and of contact information for a personal who can provide information about the collection, and
- Informed consent of the client,

is likely to meet the most exacting requirements of all applicable legislation.

Where less exacting requirements for the collection of personal information are appropriate (for example, where program planners can anticipate difficulties in obtaining

consent), the partners need to plan more carefully to ensure compliance with their governing legislation.

The requirements for an informed consent will allow the individual to understand and agree to:

- **what** personal or [health information](#) will be shared;
- with **whom**;
- for **what** purpose; and
- for **how long** (consent can be withdrawn at any time).

Direction #3—Training and Implementation

The implementation of the Guideline includes cross-sectoral training of public sector and service provider organizations involved in the delivery of integrated services for children, youth, adults and families.

Cross-sector training is provided to staff of organizations who are involved in the delivery of services to children, youth, adults and families where the delivery of those services requires, or is enhanced by, participating in collaborative or integrated service delivery approaches. The training includes a review of the guidelines and how it can be applied to public sector and service provider organization to enhance information sharing practices. The purpose of the training is to ensure that all service providers, management and support personnel in the public sector and the service provider organizations that they work with, have the knowledge they need to make appropriate decisions on the sharing of personal and health information across sectors as they work with children, youth, adults and families.

A number of tools and training modules have been developed for use by organizations involved in such service delivery. These tools and modules are being implemented in the following manner:

Tools have been, and will continue to be, developed as required for use by staff from public sector and service provider organizations. These training tools include:

- The [Red Light/Green Light document](#): An overview document for use by delivery staff that provides a quick reference of when information can and cannot be shared from the perspective of the FOIP and HIA legislation along with a listing of support and resource contacts.
- The [PIPA Red Light/Green Light](#): A companion overview document for use by private sector delivery staff and their partners that provides a quick reference of when information can and cannot be shared from the perspective of PIPA legislation, along with a listing of support and resource contacts.
- Fact sheets pertaining to specific information sharing issues.
- A website that provides the Guideline, privacy legislation and related training tools for public sector and service provider organizations.

Training Modules have been developed that are being used in the delivery of information sharing training sessions to the target audiences. The modules are as follows:

EXECUTIVE OVERVIEW:

Provides an overview of the rationale for training, the areas to be covered, including privacy legislation, and seeks commitment by management teams to have their staff attend sessions.

Intended audiences include management teams of targeted organizations, and associations representing targeted professions or organizations.

UNDERSTANDING PRIVACY LEGISLATION: HOW IT ENABLES INFORMATION SHARING

Provides an overview of privacy legislation, including the *Freedom of Information and Protection of Privacy Act*, *Health Information Act*, *Personal Information Protection Act*, the federal *Privacy Act* and *Personal Information Protection and Electronic Documents Act*, and the relationship these have with other parent (program) legislation.

Outlines how privacy legislation allows for the appropriate sharing of personal and health information. Includes a background on family violence and the impacts of sharing information for the sake of prevention, and support to those who are impacted.

Intended audiences include staff of the various target organizations that work with children, youth, adults and families.

Provides the opportunity for staff to apply their learning by working through scenarios with their colleagues from other sectors or organizations.

ENGAGING OTHERS IN THE DELIVERY OF INTEGRATED/COLLABORATIVE PROGRAMS:

Provides an overview of strategies to use when working with staff from other organizations in order to cultivate collaborative relationships.

Assists in understanding how organizations from the various sectors have common goals, and how these goals enable service providers to establish collaborative relationships.

Intended audiences include staff of the various target organizations who work with children, youth, adults and families, and who are likely to work with staff from other organizations.

A **Training Unit** has been created under the umbrella of the Information and Privacy Office of Alberta Employment Immigration and Industry, acting on behalf of the partnering ministries. Funding for the operation of the training unit has been approved and provided in part by various members of the partnering ministries through the 2007-2008 fiscal year.

The target audiences for the training include, but are not limited to, the following:

GOVERNMENT DEPARTMENTS AND AGENCIES

- Advanced Education and Technology
- Children's Services
- Education
- Health and Wellness, including
 - AADAC,
 - Alberta Mental Health Board
- Employment Immigration and Industry
- Justice and Attorney General
- Seniors and Community Supports
- Solicitor General and Ministry of Public Security

REGIONAL AUTHORITIES

- Child and Family Services Authorities
- Family and Community Support Services
- First Nations, including Delegated First Nations Authorities
- Persons with Developmental Disabilities Community Boards
- Police Services including the RCMP and Military Police
- Regional Health Authorities
- School Jurisdictions

OTHER

- Community Based Service Agencies
- Professional Associations
- Service Provider Associations
- Private School Authorities

VII. Outcomes

It is intended that directions identified within the Guideline will achieve the following broad outcomes:

- appropriate and effective sharing of information for integrated planning of services and supports for children, youth, adults and families;
- greater understanding by delivery staff of their ability to share information related to service provision for the same individual;
- improved coordination of services and supports by cross-sector professionals and service providers, and enhanced capacity to collectively plan short- and long-term interventions; and
- greater participation and benefits experienced by children, youth, adults and their families in the coordination of services and supports.

VIII. Future Directions for the Guideline

Changes to privacy legislation will continue to occur. Regular reviews of FOIP, the HIA, and PIPA are scheduled. While the cross-ministry Alberta Children and Youth Initiative Information Sharing Committee no longer meets, there is an Information Sharing Advisory Committee (ISAC) that has taken its place. The ISAC reports or liaises on a regular basis with other related committees, including the ACYI Coordinating Committee and the Interdepartmental Committee on Family Violence and Bullying. ISAC will meet on a regular basis to review training materials and delivery, legislative or policy changes and any other issues that affect the Guideline.

Appendix 1: Background for the *Information Sharing Guideline*

1.0 BACKGROUND

The Alberta Children and Youth Initiative Information Sharing Committee was given the mandate of developing recommendations that would remove barriers and enhance the sharing of information about children, youth, and their families between public sector and service provider organizations who provide services to this client group. The focus was on making recommendations that would lead to the creation of an information exchange process that would then support an enhanced level of collaborative and integrated service delivery while protecting the privacy of the people who receive services.

It should be noted that the scope has been expanded to include services to adults as well, and the guideline and tools have been adjusted to reflect that.

The balance of this document provides an overview of the legislation that must be considered to share personal and health information as well as a process to achieve an integrated and collaborative information sharing process.

2.0 LEGISLATION

The current legislative privacy regime in Alberta consists of provincial and federal privacy legislation in both the public and private sectors, as outlined in the following chart:

LEGISLATION	SECTOR	SCOPE
<i>Freedom of Information and Protection of Privacy Act</i> (FOIP)	Public	Provincial: <ul style="list-style-type: none">• government organizations, including agencies boards and commissions• local public bodies
<i>Health Information Act</i> (HIA)	Public, some private	Provincial: <ul style="list-style-type: none">• health care custodians• health services providers (included if they bill the provincial health care plan, either directly or indirectly)• pharmacists/pharmacies

<i>Personal Information Protection Act (PIPA)</i>	Private sector	Provincial: <ul style="list-style-type: none"> • Organizations as defined under the act • Organizations under the Societies Act, etc. (see PIPA for specifics) are only covered in commercial transactions that involve personal information
<i>Privacy Act</i>	Public Sector	<ul style="list-style-type: none"> • Federal government organizations, including agencies boards and commissions (includes the RCMP in Alberta)
<i>Access to Information Act</i>	Public Sector	<ul style="list-style-type: none"> • Federal government organizations, including agencies boards and commissions (includes the RCMP in Alberta)
<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i>	Private Sector	<ul style="list-style-type: none"> • Private sector organizations • Alberta organizations only covered when collecting, using or disclosing personal information across provincial or national border • Only applies to employee information of federally regulated businesses

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* ([FOIP](#)) contains a set of requirements that a [public body](#) must abide by in collecting, protecting, using, disclosing and providing access to personal information in its custody and/or under its control. While the FOIP Act protects personal information by limiting the disclosure of personal information only for purposes specified in the act, these purposes cover many of the circumstances when public bodies need to share and disclose personal information. The act also provides a right of access to general information and an individual's own personal information, and allows for a right of correction of incorrect information.

FOIP continues to apply to information in the control of a public body, even when in the custody of a service provider. For example, when a private sector agency provides counseling services under contract to a government department, the personal information remains protected by the FOIP Act.

Health Information Act

The *Health Information Act* (HIA) applies to personal health information held by individuals and organizations who are health information [custodians](#) within the health care sector, and provides the rules for the collection, use, disclosure and protection of health information. The HIA is based on principles similar to FOIP, but differs from FOIP in several key areas. At the heart of the HIA is a firm understanding that health service providers require personal health care information in order to fulfill their service mandates. The concept of controlled sharing means that custodians are permitted to obtain and use the amount and type of health information that is necessary for them to perform their mandate. The HIA creates a “controlled arena” around those custodians who are subject to the HIA. Disclosure outside of this arena can only be made within very limited circumstances, including consent, and for health and safety reasons.

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) applies to personal information that an organization collects, uses or discloses within Alberta. The Act applies to corporations, unincorporated associations, partnerships, trade unions, and individuals acting in a commercial capacity. PIPA applies only to commercial activities of non-profit organizations, such as Societies. The Act normally requires consent for the collection, use, or disclosure of personal information, but there are exceptions to consent. PIPA provides a right of access to personal information and a right to request a correction of incorrect personal information.

Privacy Act (Federal)

The federal *Privacy Act* defines “government institutions”. It sets out the controls for the protection of personal information by these federal public sector organizations such as the RCMP and other federal government institutions. It sets out the requirements that government institutions must abide by in the management (including collection, protection, use, access to and disclosure of) of information and protection of the privacy of a third party’s personal information that is in its custody and/or under its control.

Access to Information Act (Federal)

The federal *Access to Information Act* applies to personal information held by government institutions such as the RCMP and other federal government organizations. The intent of the legislation is to allow individuals access to information under the control and custody of the federal government.

Personal Information Protection and Electronic Documents Act

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to personal information that a private-sector organization collects, uses and

discloses in provinces and territories without similar legislation. The act only applies within Alberta when an organization is involved in a commercial transaction that crosses a border, such as Internet sales. The act normally requires consent for the collection, use or disclosure of personal information with some exceptions. PIPEDA provides a right of access to personal information and a right to request a correction of incorrect information.

Other Legislative Impacts

Aside from legislation that focuses on privacy, as mentioned above, other legislation also specifically addresses confidentiality and disclosure of information collected in the administration of those Acts. Examples of legislation that are relevant to an information sharing process are discussed further below, in section 4.01.

3.0 CONTEXT

In order to determine the means by which information sharing can be best facilitated amongst the various organizations that provide support and other services to children, youth, adults and families, an analysis has to be undertaken of the possible barriers and means by which they can be mitigated, by organization type.

For the purpose of identifying the barriers and ways to support an information sharing process, organizations are categorized into six main groups:

01. Public bodies under FOIP
02. Custodians under the HIA
03. Organizations under PIPA
04. Federal government institutions
05. Other.

Note: Organizations and entities that have entered into contracts or agreements with public bodies or health information custodians to deliver services on their behalf may or may not be contractually bound to some or all of the requirements under FOIP or the HIA. Contractually binding an organization to FOIP or to the HIA will be dependent on several factors including the need for the public body to have access to the information collected by the contracted organization, the potential for individuals to have a right of access to their own personal information, and the nature of the service provided on behalf of the public body.

3.01 PUBLIC BODIES UNDER FOIP

The FOIP Act defines public bodies as:

- Government ministries
- Government agencies, boards and commissions listed in Schedule 1 of the FOIP regulation
- School boards, including charter schools
- Universities, public colleges and technical institutions

- Regional health authorities
- Alberta Cancer Board, Alberta Mental Health Board
- Nursing homes
- Municipalities
- Police services and commissions
- Public libraries
- Housing management bodies
- Drainage and irrigation districts
- Metis Settlements and the General Council.

Health authorities follow HIA for health information under that act, and FOIP for all other information (e.g. general information, employee information).

The ability to share and/or disclose personal information is restricted by the provisions of FOIP. There are, however, a number of enabling provisions that allow for the disclosure of personal information including:³

- disclosure for the purpose for which the information was collected or compiled, or for a use consistent with that purpose;
- if the individual the information is about has consented to the disclosure;
- disclosure to an [employee](#) of the public body if the information is necessary for the performance of the duties of the employee, (note that employee is defined to include a person who is acting on behalf of the public body);
- disclosure to an employee of a public body if it is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the employee or member to whom the information is disclosed, (allows for disclosure between public bodies);
- disclosure for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit; and
- disclosure for the purpose of complying with an enactment of Alberta or Canada, or with a treaty, arrangement or agreement under an enactment of Alberta or Canada.

It should be noted that any disclosures of personal information under section 40 of FOIP are limited to only that which is necessary for the stated purpose.

3.02 CUSTODIANS UNDER THE HIA

These include health care organizations such as Alberta Health and Wellness, the Regional Health Authorities, health service providers paid under the Alberta Health Care Insurance Plan, pharmacies and pharmacists. The provisions to share health information under the HIA differ from the provisions to share personal information under FOIP, particularly when sharing information with organizations or individuals who are not covered by privacy legislation.

³ For a full list of the enabling disclosure provisions, see section 40 of the FOIP Act (Appendix 2).

The ability to share personal health information under the HIA to an organization that is not a custodian is largely dependent on informed consent. Exceptions to the disclosure of health information without consent are specific and limited. However, they do need to be explored to determine the appropriateness of their use.

Examples include disclosure⁴:

- to someone who is responsible for providing continuing treatment and care of the individual that the information pertains to, (note that this provision includes persons other than health care providers),
- for health and safety reasons (i.e. to avert imminent harm),
- for audit purposes;
- to comply with another piece of legislation that requires or authorizes the disclosure; (includes provincial and federal legislation), and
- where the custodian reasonably believes that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, **AND** that the disclosure will protect the health and safety of Albertans. (allows disclosure of sufficient information to allow for a police service to seek a subpoena if deemed appropriate).

3.03 ORGANIZATIONS LEGISLATED UNDER PIPA

These include private sector organizations within Alberta that collect, use or otherwise manage the personal information of individuals. The act applies to:

- Corporations
- Unincorporated associations
- Trade unions
- A partnership, and
- An individual operating as a business

The act requires consent to collect, use and disclose personal information, except in specified circumstances. In each case the purposes for the collection, use or disclosure must be “reasonable” and only to the extent necessary to meet the purpose. For example, a business cannot collect personal information “just in case” or in anticipation of an event that is unlikely to occur.

Some of the relevant provisions that allow personal information to be disclosed without consent include⁵:

- the disclosure is clearly in the interest of the individual and consent cannot be obtained in a timely way
- legislation in Alberta or Canada requires or authorizes the disclosure to a public body authorized or required by an act of Alberta or Canada to collect the information
- to a public body or law enforcement agency to assist with an investigation in specified circumstances

⁴ For a full listing of the provisions regarding disclosure, see the relevant sections in HIA. (See also Appendix 3)

⁵ For a full listing of the provisions regarding disclosure, see the relevant sections in PIPA. (See also Appendix 4)

- if the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public..

While the Act applies to non-profit organizations, certain ones only need to comply with the rules protecting personal information when engaged in a commercial activity. The Act defined as “non-profit organizations” as organizations incorporated under the *Societies Act* or the *Agricultural Societies Act* or registered under Part 9 of the *Companies Act*. A Society would not be engaged in a commercial activity when accepting a registration fee for membership in a community league. A Society that offers addictions counselling on a fee for service basis, at rates competitive with the private sector (i.e. not just nominal rates) needs to comply with the act when collecting, using and disclosing its clients’ personal information. Private schools, colleges, and early childhood programs need to comply with the act for the personal information of clients and employees.

Note: Private sector organizations that fall under federal jurisdiction are governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA).⁶

3.04 FEDERAL GOVERNMENT INSTITUTIONS

Federal government institutions are defined under the *Privacy Act*, and include the RCMP. The Act sets out the parameters for the collection and use of personal information by government institutions, and restricts the ability to share and/or disclose personal information. There are, however, a number of enabling provisions that allow for the disclosure of personal information including:⁷

- if the individual the information is about has consented to the disclosure;
- disclosure for the purpose for which the information was obtained or compiled by the institution, or for a use consistent with that purpose, (may include the disclosure of information where there are collateral investigations taking place, or actions required that are subsequent to an investigation); and
- under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation, (may include disclosure from the RCMP acting under contract with Alberta for purposes related to the investigation).

OTHER

There are other organizations that do not fit neatly into one of the above categories:

⁶ For a full listing of the provisions regarding disclosure, see the relevant sections in PIPEDA. (See also Appendix 5)

⁷ For a full list of the enabling disclosure provisions, see section 8 of the Privacy Act (Appendix 6).

AADAC: While AADAC is a public body and subject to FOIP, AADAC’s legislation is paramount to FOIP with regard to the disclosure of client information. As a result, the ability to disclose personal information is very limited and requires client consent in most instances. As well, AADAC is exempt from the application of the HIA.

Aboriginal Agreements: First Nations are not subject to the FOIP Act or the federal Privacy Act, but some on reserve agencies may be subject to PIPEDA., A public body or custodian may retain control of personal or health information by contract in order to protect the information. Some services delivered by First Nations either directly or through contracted agencies may be covered under FOIP, for services provided through a contract or agreement with a public body. Any service arrangement needs to be examined in detail in order to determine how personal information can be protected.

Youth Criminal Justice Act (Canada): While Alberta Solicitor General and Public Security, and Alberta Justice and Attorney General are subject to FOIP, federal legislation including the *Youth Criminal Justice Act* is paramount to FOIP. This legislation is somewhat permissive in that it permits the disclosure of young offender records to other professionals (including school representatives) or persons involved in the care and supervision of the young person, in order “to facilitate the rehabilitation of the young person.” At the same time there are specific requirements identified on the management of the records that identify the “young person”. Note that any decision to share information must consider the obligations of the parties. For example, the RCMP are subject to the Privacy Act, whereas the Edmonton and Calgary police services are subject to FOIP.

4.0 PARAMETERS

Differing sets of rules guide the disclosure of personal and health information. The following lists several examples by which organizations can disclose or share personal and health information:

1. Parent (or Program) Legislation
2. Common Program/Integrated Services (with or without consent)
3. Consent-Based Disclosure.

4.01 PARENT (PROGRAM) LEGISLATION

The term ‘parent legislation’ or ‘program legislation’ refers to legislation that guides or provides the mandate for the different government organizations. Examples include:

<i>Alcohol and Drug Abuse Act</i>	AADAC
<i>Child and Family Services Authorities Act</i>	Alberta Children’s Services
<i>Child, Youth and Family Enhancement Act</i>	Alberta Children’s Services
<i>Hospitals Act</i>	Alberta Health and Wellness

<i>Income and Employment Supports Act</i>	Alberta Employment, Immigration and Industry
<i>Mental Health Act</i>	Alberta Mental Health Board/Alberta Health and Wellness
<i>Protection Against Family Violence Act</i>	Alberta Children's Services
<i>Protection of Children Involved in Prostitution Act</i>	Alberta Children's Services
<i>Regional Health Authorities Act</i>	Alberta Health and Wellness
<i>School Act/Student Record Regulation</i>	Alberta Education
<i>Youth Criminal Justice Act (Federal)</i>	Justice and Attorney General/Solicitor General and Public Security/RCMP

Legislation may include provisions that allow for, or compel, the production of personal and health information. It may also govern the ability to disclose such information, either in keeping with, or despite privacy legislation. Parent legislation may also impose some limitations on the ability to provide collaborative and integrated services with other organizations.

4.02 COMMON PROGRAMS/INTEGRATED SERVICES

FOIP allows for the disclosure of personal information for a number of reasons including “to another public body if the disclosure is necessary for the delivery of a common or integrated program or service”.

A “common program” is defined as a single program or service delivered by two or more public bodies.

Examples of common programs include programs such as the child protection and enhancement programs under the *Child Youth and Family Enhancement Act*. The ‘programs’ are similar across the province, but are delivered by different public bodies (CFSA’S). Similarly, Regional Health Authorities or individual Police Services would also run ‘programs’ that are common across the province.

- ***“Integrated” means a program or service which has several distinct components, each of which may be delivered separately, but when put together comprise a complete program or service.***

Examples of integrated programs include CARRT (Child At Risk Response Team) that involves both the police services and staff from the Child and Family Services Authority. Other examples include the Student Health Initiatives, and the Multi-Disciplinary Teams involved with the children and youth with complex needs.

In order to allow for disclosure under this provision, public bodies must be able to demonstrate the following:

- Involvement in a common program or integrated service

- Public bodies must be able to demonstrate evidence of a common or integrated program or service. Examples include terms of reference, agreements or a memorandum of understanding.
 - The working relationship between the public bodies involved in the program or service is identified.
 - Administrative processes are identified that support the operation of the program or service, including the management of common records, a process to respond to access requests and record retention schedules.
- Authority to collect information
 - Public bodies must be able to demonstrate they have the authority or mandate to collect personal information (linked to the services being delivered).
 - The collection of personal information is governed by section 33 of FOIP and is limited to only that which relates directly to and is necessary to allow for the program or service to be carried out.
- Manner of collection
 - Public bodies are limited by section 34 of FOIP to collect personal information directly from the individual it is about unless an exception applies. Examples of such exceptions include:
 - Information is necessary to determine eligibility for benefits and services.
 - Information is collected for the purpose of a law enforcement investigation.
 - Information is collected in a health and safety emergency.
- Limited disclosure
 - Disclosure of information is limited to that which is necessary to operate a common or integrated program or service in a reasonable manner.
 - Details of the disclosure are documented.

Note that the above requirements should be applied to all three options identified under this section. As well, a common or integrated program or service can only involve public bodies; a common program cannot be established between a public body and a PIPA organization.

4.03 CONSENT-BASED INFORMATION SHARING

The application of the provision of FOIP for a [common program](#) or [integrated service](#) does not extend to health information collected pursuant to the HIA, organizations that are not covered by FOIP, nor information where other legislation prevents disclosure.

Consent-based information sharing has several requirements. In order for consent to be valid, the provisions outlined in the applicable legislation must be followed. Those provisions are outlined in the following chart.

LEGISLATION	SECTIONS	COMMENTS
FOIP	40(1)(d) Act; 6 Regulations	In writing, or oral or electronic if conditions are met to authenticate the consent, specifying to who the personal information may be disclosed and how it may be used.
HIA	34	Identifies that health information can be disclosed with consent and outlines requirements
PIPA	14, 20	In writing or orally. Express consent normally required for personal information sharing. Implied and opt-out consent permitted in some circumstances.
PIPEDA	7	In writing or orally. Express consent normally required for personal information sharing.
Privacy Act	7, 8(2)	Identifies that personal information can be disclosed without consent in the circumstances that are listed. (Note that this Act states under what circumstances personal information can be disclosed without consent rather than stating what can be disclosed with consent.

See Appendices 2 - 6 for the actual provisions listed above.

The individuals who are being asked to consent to the disclosure of their personal information must understand what information is to be disclosed, be advised how their information will be used and to whom it will be disclosed. Consent is an empowering tool that provides individuals with control over their personal information and results in them knowing:

- **what** information will be disclosed,
- to **whom** it will be disclosed,
- for **what** purpose it will be used, and
- for **how long** consent will remain in effect (consent can be withdrawn at any time).

The decision to pursue consent needs to be carefully considered. The decision to pursue consent needs to be carefully considered. A public body cannot rely on consent to collect personal information – it must have authority to collect because it is necessary for its program or activity or with other legislative authority.

A public body may need to pursue consent:

- to disclose personal information if the disclosure is not authorized under section 40 of the FOIP Act.
- to disclose personal information authorized by section 40, but in order to meet program objectives to ensure clients understand that their personal information will be shared
- to enable the collection of health information from a custodian
- to enable a custodian to collect health information from a public body or organization

In situations where individuals have a choice on whether or not they will allow the disclosure of their personal information, the options should be outlined for the individual. This requires that individuals be advised of the consequences of either providing or not providing their consent. The outcome of providing choice will mean that in some situations individuals will choose 'to repeat their story more than once.' In other situations it could mean that they will not be eligible for the programs or services they require, or that in some cases, services will be limited due to a refusal to provide consent and a lack of information to provide the service.

Consent also has to be considered in the context of minor children and their rights. Children are individuals in their own right, and as such may be able to agree or refuse to provide consent.

Section 84(1)(e) of FOIP deals with the ability of the guardian of a minor (an individual under the age of 18) to exercise the rights of the minor. This includes the right to give or refuse consent. The person requesting the consent from the parent or guardian must assess whether the exercise of this power by the parent or guardian would be an unreasonable invasion of the minor's privacy. A major factor in forming this opinion is to assess whether a particular minor child or youth is capable of providing informed consent. The ability to provide informed consent has to be judged on a number of factors for each child including his/her age, level of maturity, level of understanding, and the degree of involvement and influence of the guardians. The guardian must also be acting in the best interests of the child. The guardian cannot exercise the rights of the child in order to pursue the interests of the guardian or another individual.

Similarly, under HIA, section 35(1)(n) allows for the disclosure of individually identifying diagnostic, treatment and care information if the individual lacks the mental capacity to provide consent and the disclosure is deemed to be in the best interest of the individual. That presumes therefore, that the custodian needs to make a determination as to whether or not a child has the capacity to provide consent.

5.0 INFORMATION SHARING IN SUPPORT OF COMMON AND INTEGRATED PROGRAMS AND SERVICES

Services to individuals and their families are not always effective when delivered by a single human service organization in isolation of other service provider agencies that are dealing with the same individual.

The delivery of services to individuals and their families in a holistic community-based environment supports the development of an integrated information sharing service delivery process that not only meets the needs of the individuals and their families, but also complies with existing privacy legislation.

In order to develop an integrated service delivery process, it is important to recognize that services provided by various organizations are often incomplete. Services offered in isolation of other services, without a more comprehensive case-plan, or at least without knowledge of other case-plans and goals that have been developed in the other areas, may not always serve the best interests of the individual. Any small measures of success that are gained in such situations may not be maintainable to any degree in the long term if other issues are not addressed.

5.01 ENTRY POINTS

The rationale that supports the need for integrated services also supports the mechanisms by which individuals may be identified as potential clients of that process. This deals with the issue of determining how to refer someone to a service without knowing if it is the appropriate one.

There are at least three potential routes that can be taken:

1. Direct referral
 2. Initial screening/assessment/case conference
 3. Self-referral.
1. Direct referrals to the integrated services may be the appropriate process if the referral agent is aware of the services that would be available and determines that the child or youth would benefit from them. This process will work where there is a requirement for consent from the client to allow the disclosure of his/her information.

Organizations that are bound by the need for consent to disclose information could be captured in this process (e.g., custodians under the HIA, AADAC, private sector organizations).

2. The second process is a mechanism where there is an identified need based on an initial discussion regarding a potential client. In this case, a referral agent may not be comfortable in making the referral because of a lack of confidence in whether the service would be appropriate for the client. Public bodies under FOIP can use this

process to enter into preliminary discussions as to the appropriateness of the referral with other service providers involved in the integrated service.

Organizations (or programs, activities) that could potentially be captured in this process include those involved in the Student Health Initiative, Early Intervention Initiatives, and Enhanced Service Delivery Initiatives and are public bodies under FOIP or otherwise linked to them through some form of contract or agreement.

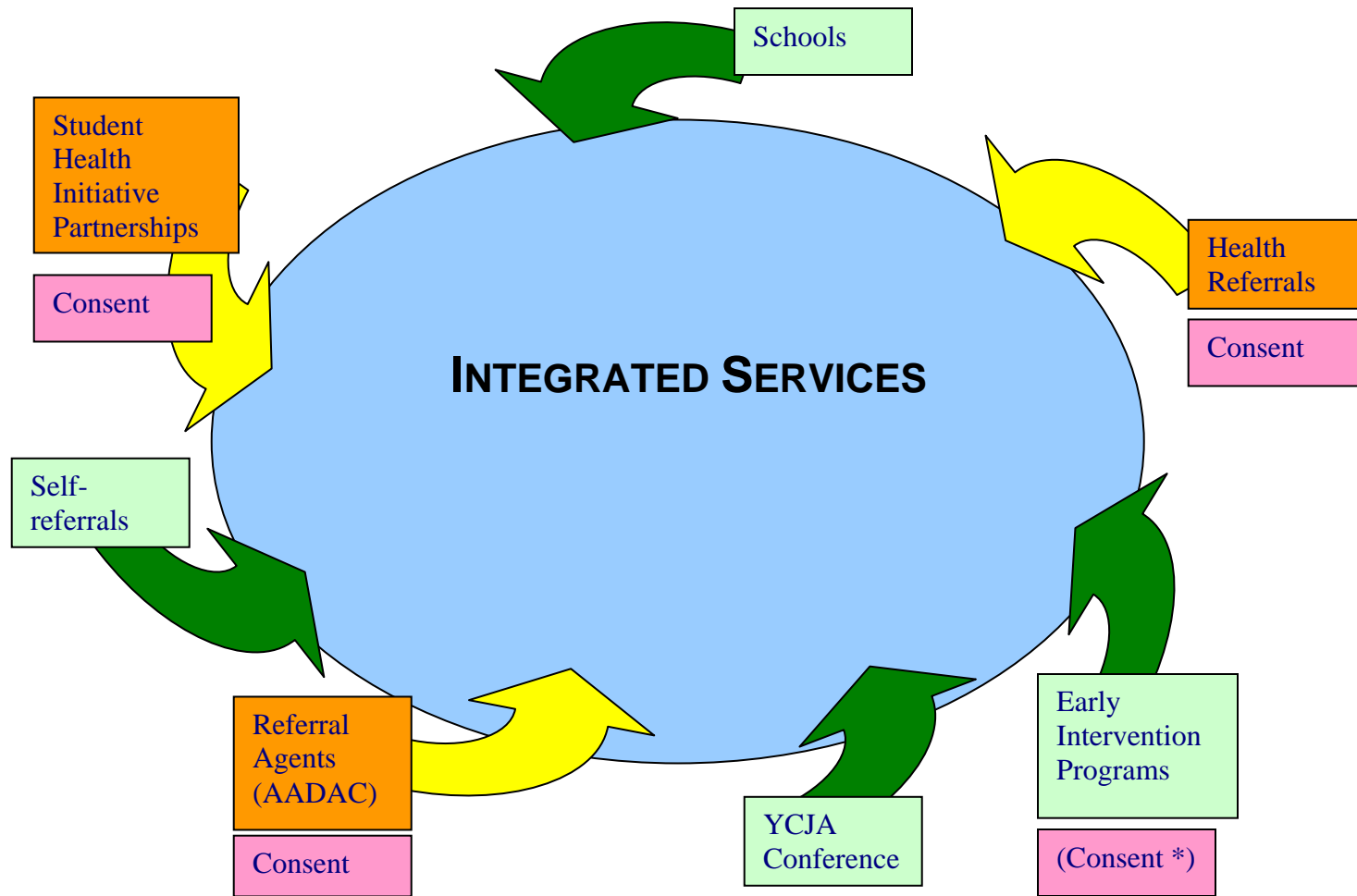
It should be noted however, that while there may not be a need for consent, it still should be considered as part of the process. If there is a decision to use this process for assessment, there then needs to be a further decision as to whether there will be a need for consent at a later point.

It should also be noted that service providers who are bound by the need for client consent to disclose information under the HIA or other legislation, are not necessarily restricted from participating in the initial assessment process for determining appropriateness (eligibility) of the referral where they have no prior knowledge or involvement with the child or the family, and where they are public bodies under FOIP.

3. The third process could deal with self-referrals.

(See Figure 1)

Entry Points (Figure 1)
(* consent may be required)



6.0 The Information Sharing Guideline for Integrated Service Delivery *(A Guide to assist Service Delivery Organizations to set up integrated services)*

In this context, integrated services have several distinct components. Each component may be delivered separately, but when viewed together comprise the complete program or service.

The following elements should be included in the terms of reference (and/or the information being made available to the client) that guide integrated service delivery. This could include processes that are delivered individually, but are agreed to by the participating organizations as necessary to the delivery of services in a holistic and collaborative manner.

Purpose

Services to children, youth, adults and families are more effective when integrated or when collaboration occurs between the involved service providers. This template sets out the requirements by which information can be shared within an integrated service model. (See sample Terms of Reference.)

Integrated Service Providers

The integrated service providers need to be identified to all potential clients in order to inform the potential clients as to who may be accessing their information and providing services to them. In addition to the listing of agencies, the reason for their involvement must also be available. In situations where agencies are providing services under contract to a public body or a health information custodian, that relationship should also be identified. Contracts of this nature must contain conditions governing the access to the records by the public body; limits on collection; use; disclosure; and the disposition of personal and health information and records as well as consequences for failing to comply with these conditions. Finally, the privacy legislation by which they are bound should also be identified so that the client knows under what conditions their personal and health information is protected.

Authority

A statement outlining the authority for the integration of services must be made. This may be a mandate statement for the integrated group of organizations, authorities for each of the participants or both. A separate document that briefly outlines the background and services offered for each of the integrated service providers should be added.

Statement of Use/Notification

A clear statement must be made regarding the type of personal and health information that will be collected, and the manner in which it will be used and disclosed in the integrated services program. This should also state who will have access to the information, and include a limitation statement that indicates that use of the information will be limited to the defined purposes. Any further disclosure would be subject to the consent of the individual to whom it pertains or limited by law (and in compliance with

the appropriate privacy legislation). Given the premise that individuals have a right to know how their information is used, all disclosures must be documented.

Consent

Informed consent not only serves as a mechanism that allows the sharing or disclosure of information, but also serves as a means of empowering clients by giving them control of their personal and health information. In situations where there are no provisions for sharing without consent, as defined by the legislation and the relationship with the integrated service providers, it should be clearly stated that consent is a requirement prior to the disclosure of the personal and health information, other than where required by law or as a condition of receiving service.

Records

A description of the types of records that will be created through the integrated services should be provided. Records may be kept on an individual program/service file basis or there may be a rationale for the creation of common records. A statement as to the life expectancy of such records will inform the clients as to the retention schedule of their records.

Access

Individuals whose personal and health information is collected and used generally have a legislated right of access to that information. A process should be outlined that can be easily followed by individuals seeking access to their information. Consideration should be given to the identification of one source where individuals can make their request for access.

Sample Terms of Reference—Integrated Service

Purpose Statement

The organizations listed below have developed an integrated process to deliver certain services in support of children, youth, adults and families. These services, while capable of being delivered independently, are seen as more likely to achieve success for the client if delivered in collaboration with each other.

The services that are offered through this approach include _____, or will focus on _____.

Authority

The membership in this integrated service system has been determined to be appropriate and will operate in a manner that recognizes the value in delivering _____ services in a collaborative approach. Individually the members derive their authority from the specific legislation that they operate under, or by virtue of being a program or activity of the governing organization in order to collect, use as well as disclose client information to other integrated service providers on a [need-to-know](#) basis.

Integrated Service Providers/Partners (examples)

Core Service Providers

- CFSA
- Health Authority
- Separate School Board
- Public School Board
- Mental Health Board

Extended Service Providers

- AADAC
- Church
- Boys and Girls Club
- Agency
-

Note: For details on the membership, including authorities, see individual partnership data sheets.

Statement of Use

Personal and health information that is collected by the core service providers will be used only for the purpose of providing (E.g.) counseling and intervention services. The focus of these services will be to assist the individual and his/her family to _____.

Services will be delivered primarily by the integrated service providers. Where services need to be delivered by extended service providers, information will only be disclosed to them with consent. Information will not be used for any other purpose, unless required by law, and will only be disclosed to external parties with the consent of the individual to whom it pertains.

The services that are seen to be necessary will be identified through an assessment process that will build on the case- or educational-plans already in place. Where there is no such plan, one will be developed with the input of the individual and his/her family. As part of the case-plan, a case manager will be identified. That person may serve as the main point of contact.

Records and Access

Information that is collected by the member participants will be maintained individually, other than the common registration and assessment form. That particular form will serve as the basis for the integrated services and will be maintained by _____, for a period not to exceed ___ years following the closure of the client file. Individual program records may be created and maintained by the partner organizations.

In order to obtain access to the records that relate to the integrated services, _____ the case manager should be the initial point of access. Records that are held by the individual partners need to be accessed through their normal channels.

7.0 Glossary of Terms

Affiliate	Defined under the Health Information Act includes an employee, volunteer, appointee or person under contract or in an agency relationship with the custodian.
Age of Consent	The age at which children and youth can give consent may be specified in legislation and takes into consideration the age of the child, maturity level and sensitivity of the information. (See the Appendix for further information.)
Common Program	A single program or service delivered by two or more public bodies. The delivery of these under a formalized arrangement is recommended wherever appropriate.
Continuity of Care	A person's/persons' responsibility for the ongoing care, medical or otherwise, for a child.
Custodians	Defined under the <i>Health Information Act</i> to include organizations and health service providers that are fully/partially, directly/indirectly funded under the Alberta Health Care Insurance Plan. Custodians have the authority to collect, use and disclose health information and are responsible for ensuring the protection of this health information. For a full definition, refer to the HIA.
Employee	Defined under the <i>Freedom of Information and Protection of Privacy Act</i> to include individuals and agencies who provide services on behalf of the public body that they have contracted or entered into an agreement with. (Note: This definition of employee is solely for the purposes of FOIP.) Contractual obligations should include the necessary clauses to ensure that the provisions of FOIP are properly addressed.
FOIP	<i>Freedom of Information and Protection of Privacy Act</i>
HIA	<i>Health Information Act</i>
Imminent Danger	A situation in which any individual or group of individuals may be at immediate risk of harm to their health and/or safety.
Integrated Service	A program or service that has several distinct components, each of which may be delivered separately, but when considered together comprises the complete program or

service.

Need to Know

Only the minimum amount of personal and health information necessary may be shared where existing legislation provides for disclosure in order to respect the rights to individual privacy of children, youth, adults and their families.

PIPA

Personal Information Protection Act

Public Body

Defined under FOIP to include government organizations such as departments, boards and agencies. (**Note:** This does not refer to contracted agencies, such as service providers.)

Additional HIA Definitions

Continuing Treatment and Care

Section 35(1)(b) of HIA permits the disclosure of individually identifying diagnostic, treatment and care information without the individual's consent to the person providing continuing treatment and care to the individual. For example, if the individual is discharged from the hospital and returning home, the disclosure may be necessary so that appropriate home care can be provided. The person the health information is disclosed to need not be a formal health service provider.

Health Information

Section 1(1)(k) of HIA states that "health information" means any or all of the following:

- diagnostic treatment and care information (see also 1(1)(i));
- health and services provider information (see also 1(1)(o));
- registration information (see also 1(1)(u)).

Imminent Danger

Section 35(1)(m) of HIA states that a custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person. In order to determine whether an imminent danger to the health or safety of any person exists, you must determine whether the following three criteria of "imminent danger" exist:

1. Clarity—The intended victim or group of victims must be

- ascertainable or sufficiently identifiable.
2. **Danger**—The danger to the victim must be serious bodily harm or death.
 3. **Imminence**—The risk must be serious and a sense of urgency must be created by the threat of danger. The risk could be a future risk but must be serious enough that a reasonable person would be convinced that the harm would be carried out.

Each of these three criteria must be considered in the context of each situation and in view of the surrounding circumstances. There must be a clear and imminent threat of serious bodily harm or death to an identifiable group or person that creates a sense of urgency. If the custodian (or affiliate) believes on reasonable grounds that the disclosure will avert or minimize an imminent danger to the health or safety of any person, the information may be disclosed to the police pursuant to section 35(1)(m) of HIA.

Least Amount of Information

Sections 57 and 58 of the HIA requires custodians to collect, use, or disclose the least amount of information at the highest anonymity, based on the need to know. Only the amount of health information that is essential to enable the custodian to carry out the intended purpose must be collected, used or disclosed. Not all health information created and maintained by the custodian is relevant or necessary to carry out a certain purpose or to address a certain disclosure request.

Need to Know

Only the minimum amount of personal and health information necessary to meet the purpose for which the information is being shared may be shared where existing legislation provides for disclosure in order to respect the rights to individual privacy of children, youth, adults and their families.

Appendix 2: Selected sections of the Freedom of Information and Protection of Privacy Act

Request under section 7 deemed to be a request under HIA

15.1(1) If a request is made under section 7(1) for access to a record that contains information to which the Health Information Act applies, the part of the request that relates to that information is deemed to be a request under section 8(1) of the Health Information Act and that Act applies as if the request had been made under section 8(1) of that Act.

(2) Subsection (1) does not apply if the public body that receives the request is not a custodian as defined in the Health Information Act.

Purpose of collection of personal information

33 No personal information may be collected by or for a public body unless

(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,

(b) that information is collected for the purposes of law enforcement, or

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

Protection of personal information

38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

1994 cF-18.5 s36;1996 c28 s21

Division 2: Use and Disclosure of Personal Information by Public Bodies

Use of personal information

39(1) A public body may use personal information only

(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.

(2) Despite subsection (1), but subject to subsection (3), a post-secondary educational body may use personal information in its alumni records for the purpose of its own fund-raising activities.

(3) A post-secondary educational body must, when requested to do so by an individual, discontinue using that individual's personal information under subsection (2).

(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

1994 cF-18.5 s37;1999 c23 s24

Disclosure of personal information

40(1) A public body may disclose personal information only

(a) in accordance with Part 1,

- (b) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17,
- (c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
- (d) if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure,
- (e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,
- (f) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,
- (g) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information,
- (h) to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member,
- (i) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,
- (j) for the purpose of enforcing a legal right that the Government of Alberta or a public body has against any person,
- (k) for the purpose of
 - (i.) collecting a fine or debt owing by an individual to the Government of Alberta or to a public body, or to an assignee of either of them, or
 - (ii.) making a payment owing by the Government of Alberta or by a public body to an individual,
- (l) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,
- (m) to the Auditor General or any other prescribed person or body for audit purposes,
- (n) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem,
- (o) to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry,
- (p) to the Provincial Archives of Alberta or to the archives of a public body for permanent preservation,
- (q) to a public body or a law enforcement agency in Canada to assist in an investigation
 - (i.) undertaken with a view to a law enforcement proceeding, or
 - (ii.) from which a law enforcement proceeding is likely to result,
- (r) if the public body is a law enforcement agency and the information is disclosed
 - (i.) to another law enforcement agency in Canada, or
 - (ii.) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,
- (s) so that a spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted, (Amended by s.38 of the Adult Interdependent Relationships Act, 2002, in force June 1, 2003)
- (t) in accordance with section 42 or 43,
- (u) to an expert for the purposes of section 18(2),
- (v) for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party,

- (w) when disclosure is by the Minister of Justice and Attorney General or an agent or lawyer of the Minister of Justice and Attorney General to a place of lawful detention,
 - (x) for the purpose of managing or administering personnel of the Government of Alberta or the public body,
 - (y) to the Director of Maintenance Enforcement for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act,
 - (z) to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer,
 - (aa) for the purpose of supervising an individual under the control or supervision of a correctional authority,
 - (bb) when the information is available to the public,
 - (bb.1) if the personal information is information of a type routinely disclosed in a business or professional context and the disclosure
 - (i.) is limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number and e-mail address, and
 - (ii.) does not reveal other personal information about the individual or personal information about another individual,
 - (cc) to the surviving spouse or adult interdependent partner or a relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy, (Amended by s.38 of the Adult Interdependent Relationships Act, 2002, in force June 1, 2003)
 - (dd) to a lawyer or student-at-law acting for an inmate under the control or supervision of a correctional authority,
 - (ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person, or
 - (ff) to the Administrator of the Motor Vehicle Accident Claims Act or to an agent or lawyer of the Administrator for the purpose of dealing with claims under that Act.
- (4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner.

1994 cF-18.5 s38;1995 c17 s12;1996 c28 s21;1999 c23 s25

Consistent purposes

41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

- (a) has a reasonable and direct connection to that purpose, and
- (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

1994 cF-18.5 s39;1999 c23 s26

Disclosure for research or statistical purposes

42 A public body may disclose personal information for a research purpose, including statistical research, only if

- (a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Commissioner,
- (b) any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest,
- (c) the head of the public body has approved conditions relating to the following:
 - (i.) security and confidentiality,

- (ii.) the removal or destruction of individual identifiers at the earliest reasonable time, and
- (iii.) the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body, and
- (d) the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

1994 cF-18.5 s40

Appendix 3: Selected Sections of the Health Information Act

29 A custodian that collects information described in section 1(1)(i), (o) or (u) that is not written, photographed, recorded or stored in some manner in a record may use the information only for the purpose for which the information was provided to the custodian.

1999 cH-4.8 s29

Use of personal health number by non-custodian

30 A person who is authorized to require an individual to provide a personal health number pursuant to section 21(1)(b) may use that information only for the purpose for which the information was collected.

1999 cH-4.8 s30

Part 5—Disclosure of Health Information

Division 1: General Disclosure Rules

Prohibition re disclosure of health information

31 No custodian shall disclose health information except in accordance with this Act.

1999 cH-4.8 s31

Disclosure of non-identifying health information

32(1) A custodian may disclose non-identifying health information for any purpose.

(2) If a disclosure under subsection (1) is to a person that is not a custodian, the custodian must inform the person that the person must notify the Commissioner of an intention to use the information for data matching before performing the data matching.

1999 cH-4.8 s32

Disclosure of information to individual who is subject of information

33 A custodian may disclose individually identifying health information to the individual who is the subject of the information or to a person referred to in section 104(1)(c) to (i) who is acting on behalf of that individual.

1999 cH-4.8 s33

Disclosure of individually identifying health information to be with consent

34(1) Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure.

(2) A consent referred to in subsection (1) must be provided in writing or electronically and must include

(gg) an authorization for the custodian to disclose the health information specified in the consent,

- (hh) the purpose for which the health information may be disclosed,
 - (ii) the identity of the person to whom the health information may be disclosed,
 - (jj) an acknowledgment that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent,
 - (kk) the date the consent is effective and the date, if any, on which the consent expires, and
 - (ll) a statement that the consent may be revoked at any time by the individual providing it.
- (3)** A disclosure of health information pursuant to this section must be carried out in accordance with the terms of the consent.
- (4)** A revocation of a consent must be provided in writing or electronically.
- (5)** A consent or revocation of a consent that is provided in writing must be signed by the person providing it.
- (6)** A consent or revocation of a consent that is provided electronically is valid only if it complies with the requirements set out in the regulations.

1999 cH-4.8 s34

Disclosure of diagnostic, treatment and care information

35 (1) A custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information

- (a) to another custodian for any or all of the purposes listed in section 27(1) or (2), as the case may be,
 - (a.1) to the government of Canada or of another province or territory of Canada for that government's use for health system planning and management and health policy development where
 - (i) the individual is a resident of that other province or territory, or
 - (ii) that government is otherwise responsible for payment for health services provided to the individual,
- (b) to a person who is responsible for providing continuing treatment and care to the individual,
- (c) to family members of the individual or to another person with whom the individual is believed to have a close personal relationship, if the information is given in general terms and concerns the presence, location, condition, diagnosis, progress and prognosis of the individual on the day on which the information is disclosed and the disclosure is not contrary to the express request of the individual,
- (d) where an individual is injured, ill or deceased, so that family members of the individual or another person with whom the individual is believed to have a close personal relationship or a friend of the individual can be contacted, if the disclosure is not contrary to the express request of the individual,
 - (d.1) where an individual is deceased, to family members of the individual or to another person with whom the individual is believed to have had a close personal relationship, if the information relates to circumstances surrounding the death of the individual or to health services recently received by the individual and the disclosure is not contrary to the express request of the individual,

- (e) to an official of a penal or other custodial institution in which the individual is being lawfully detained if the purpose of the disclosure is to allow the provision of health services to the individual,
- (f) to a person authorized to conduct an audit of the information if the person agrees in writing
 - (i) to destroy the information at the earliest opportunity after the audit is concluded, and
 - (ii) not to disclose the information to any other person, except as required to accomplish the audit or to report unlawful or improper conduct by the custodian or a health services provider,
- (g) to a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the *Alberta Evidence Act*,
- (h) for the purpose of a court proceeding or a proceeding before a quasi-judicial body to which the custodian is a party,
- (i) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information,
- (j) repealed 2006 c18 s5;
- (k) to another custodian where the custodian disclosing the information has a reasonable expectation that disclosure will detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada,
- (l) to an officer of the Legislature if the information is necessary for the performance of the officer's duties,
- (m) to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person,
- (n) if that individual lacks the mental capacity to provide a consent and, in the opinion of the custodian, disclosure is in the best interests of the individual,
- (o) to a descendant of a deceased individual, a person referred to in section 104(1)(c) to (i) who is acting on behalf of the descendant or a person who is providing health services to the descendant if, in the custodian's opinion,
 - (i) the disclosure is necessary to provide health services to the descendant, and
 - (ii) the disclosure is restricted sufficiently to protect the privacy of the deceased individual,
- (p) if the disclosure is authorized or required by an enactment of Alberta or Canada,
- (q) to its successor where
 - (i) the custodian is transferring its records to the successor as a result of the custodian
 - (A) ceasing to be a custodian, or
 - (B) ceasing to provide health services within the geographic area in which the successor provides health services,

and

- (ii) the successor is a custodian,
- (r) for the purpose of obtaining or processing payment for health services provided to the individual by a person that is required under a contract to pay for those services for that individual, or
- (s) to the College of Physicians and Surgeons of Alberta for the purpose of administering the Triplicate Prescription Program.

(2) A committee to which health information is disclosed pursuant to subsection (1)(g) must not disclose the information to any other person except in accordance with subsection (3).

(3) A committee referred to in subsection (2) may disclose non-identifying health information to another committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the *Alberta Evidence Act*.

(4) A custodian may disclose individually identifying diagnostic, treatment and care information to a health professional body for the purpose of an investigation, a discipline proceeding, a practice review or an inspection if

- (a) the custodian has complied with any other enactment authorizing or requiring the custodian to disclose that information for that purpose, and
- (b) the health professional body agrees in writing
 - (i) not to disclose the information to any other person except as authorized by or under the Act governing the health professional body, and
 - (ii) repealed 2006 c18 s5.

RSA 2000 cH-5 s35;2003 c23 s2;2006 c18 s5

Disclosure of registration information

36 A custodian may disclose individually identifying registration information without the consent of the individual who is the subject of the information

- (a) for any of the purposes for which diagnostic, treatment and care information may be disclosed under section 35(1) or (4),
- (b) to any person for the purpose of collecting or processing a fine or debt owing by the individual to the Government of Alberta or to a custodian, or
- (c) to a person who is not a custodian if the disclosure is in accordance with the requirements set out in the regulations.

1999 cH-4.8 s36

Disclosure of health services provider information

37 (1) A custodian may disclose individually identifying health services provider information without the consent of the individual who is the subject of the information

- (a) to a health professional body that requests the information for the purpose of an investigation, a discipline proceeding, a practice review or an inspection relating to the health services provider, or
- (b) if the disclosure is authorized or required by an enactment of Alberta or Canada.

(2) A custodian may disclose the health services provider information described in section 1(1)(o)(i) to (iii), (vii), (xiv), (xv), (xviii), (xix) and (xx), other than home address,

telephone number and licence number, to any person for any purpose without the consent of the individual who is the subject of the information, unless the disclosure

- (a) would reveal other information about the health services provider, or
- (b) could reasonably be expected to result in
 - (i) harm to the health services provider's mental or physical health or safety, or
 - (ii) undue financial harm to the health services provider.

(3) Subsection (2) does not apply where the disclosure is to a police service or the Minister of Justice and Attorney General under section 37.1, 37.2 or 37.3.

RSA 2000 cH-5 s37;2006 c18 s6

Disclosure to prevent or limit fraud or abuse of health services

37.1 (1) A custodian may disclose individually identifying health information referred to in subsection (2) without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes

- (a) that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and
- (b) that the disclosure will detect or prevent fraud or limit abuse in the use of health services.

(2) A custodian may disclose the following information under subsection (1):

- (a) the name of an individual;
- (b) the date of birth of an individual;
- (c) the personal health number of an individual;
- (d) the nature of any injury or illness of an individual;
- (e) the date on which a health service was sought or received by an individual;
- (f) the location where an individual sought or received a health service;
- (g) the name of any drug, as defined in the *Pharmaceutical Profession Act*, provided to or prescribed for an individual and the date the drug was provided or prescribed.

(3) If a custodian discloses individually identifying health information about an individual under subsection (1), the custodian may also disclose health services provider information about a health services provider from whom that individual sought or received health services if that information is related to the information that was disclosed under subsection (1).

(4) Health services provider information may be disclosed under subsection (3) without the consent of the health services provider who is the subject of the information.

2006 c18 s7

Disclosure to prevent or limit fraud or abuse of health services by health services providers

37.2 (1) A custodian may disclose individually identifying health information referred to in subsection (2) without the consent of the health services provider who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes

- (a) that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada by the health services provider, and

(b) that the disclosure will detect or prevent fraud or limit abuse in the provision of health services.

(2) A custodian may disclose the following information under subsection (1):

- (a) the name of the health services provider;
- (b) the business address of the health services provider;
- (c) the date on which the health services provider provided a health service;
- (d) the description of a health service provided by the health services provider;
- (e) the benefits that were paid or charged in relation to a health service provided by the health services provider.

(3) If a custodian discloses information under subsection (1) about a health service, the custodian may also disclose individually identifying health information about the individual who received that health service if that information is related to that health service.

(4) Individually identifying health information may be disclosed under subsection (3) without the consent of the individual who is the subject of the information.

2006 c18 s7

Disclosure to protect public health and safety

37.3 (1) A custodian may disclose individually identifying health information referred to in subsection (2) without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes

- (a) that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and
- (b) that the disclosure will protect the health and safety of Albertans.

(2) A custodian may disclose the following information under subsection (1):

- (a) the name of an individual;
- (b) the date of birth of an individual;
- (c) the nature of any injury or illness of an individual;
- (d) the date on which a health service was sought or received by an individual;
- (e) the location where an individual sought or received a health service;
- (f) whether any samples of bodily substances were taken from an individual.

(3) If a custodian discloses individually identifying health information about an individual under subsection (1), the custodian may also disclose health services provider information about a health services provider from whom that individual sought or received health services if that information is related to the information that was disclosed under subsection (1).

(4) Health services provider information may be disclosed under subsection (3) without the consent of the health services provider who is the subject of the information.

2006 c18 s7

Disclosure for purpose of storage

38 A custodian may disclose individually identifying health information without the consent of the individual who is the subject of the information to the Provincial Archives of Alberta or to any other archives that is subject to this Act or the *Freedom of Information and Protection of Privacy Act*, for the purposes of permanent preservation

and historical research if, in the opinion of the custodian, the information has enduring value.

1999 cH-4.8 s38

Disclosure by Minister and Department

39 (1) The Minister or the Department may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information to another Minister of the Government of Alberta for the purpose of developing public policy.

(2) The Minister or the Department may enter into an agreement with

- (a) another Minister of the Government of Alberta or a Minister of the Government of Canada or of any other province or territory, or
- (b) a person or entity in accordance with the regulations made pursuant to the *Alberta Health Care Insurance Act*,

respecting the disclosure to the person referred to in clause (a) or (b), as the case may be, of individually identifying registration information without the consent of the individual who is the subject of the information.

1999 cH-4.8 s39

Disclosure to Minister

40 A custodian other than the Minister may disclose individually identifying health information to the Minister without the consent of the individual who is the subject of the information if the disclosure is necessary or desirable in the opinion of the custodian to enable the Minister to carry out the duties of the Minister.

1999 cH-4.8 s40

Maintaining certain disclosure information

41 (1) Subject to subsection (1.1), a custodian that discloses a record containing individually identifying diagnostic, treatment and care information under section 35(1) or (4) must make a note of the following information:

- (a) the name of the person to whom the custodian discloses the information;
- (b) the date and purpose of the disclosure;
- (c) a description of the information disclosed.

(1.1) The requirement to make a note under subsection (1) does not apply to a custodian that discloses a record containing individually identifying diagnostic, treatment and care information under section 35(1)(a) by permitting access to the information stored in the computer database of the custodian if, when the information is accessed, the database automatically keeps an electronic log of the following information:

- (a) the user identification of the custodian that accesses the information;
- (b) the date and time that the information is accessed;
- (c) a description of the information that is accessed.

(2) The information referred to in subsections (1) and (1.1) must be retained by the custodian for a period of 10 years following the date of the disclosure.

(3) An individual who is the subject of information referred to in subsection (1) or (1.1) may ask a custodian for access to and a copy of the information, and Part 2 applies to the request.

RSA 2000 cH-5 s41;2006 c18 s8

Notification of purpose of and authority for disclosure

42 (1) A custodian that discloses individually identifying diagnostic, treatment and care information must inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is made.

(2) Subsection (1) does not apply where the disclosure is

- (a) to another custodian under section 35(1)(a),
- (b) to the Minister or the Department under section 46,
- (c) to another custodian under section 47,
- (d) to a police service or the Minister of Justice and Attorney General under section 37.1, 37.2 or 37.3, or
- (e) to the individual who is the subject of the information.

RSA 2000 cH-5 s42;2006 c18 s9

Disclosure of health information by affiliate

43 An affiliate of a custodian must not disclose health information in any manner that is not in accordance with the affiliate's duties to the custodian.

1999 cH-4.8 s43

Confidentiality of non-recorded information

44 A custodian that collects information described in section 1(1)(i), (o) or (u) that is not written, photographed, recorded or stored in some manner in a record may disclose the information only for the purpose for which the information was provided to the custodian.

1999 cH-4.8 s44

Duty of custodian

45 A custodian that discloses health information must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information.

1999 cH-4.8 s45

Disclosure to Minister or Department

46 (1) The Minister or the Department may request another custodian to disclose individually identifying health information for any of the purposes listed in section 27(2)

- (a) if the Minister or the Department, as the case may be, is authorized by an enactment of Alberta or Canada to obtain the information from the other custodian, or
- (b) if the information requested relates to a health service provided by the other custodian and
 - (i) the health service is fully or partially paid for by the Department or is provided using financial, physical or human resources provided, administered or paid for by the Department, or
 - (ii) the information is prescribed in the regulations as information the Minister or the Department may request under this section.

(2) If the requirements of subsection (1) are met, the custodian must disclose the information to the Minister or the Department, as the case may be.

(3) On receipt of information under this section, the Minister or the Department, as the case may be, may disclose the information to a custodian referred to in section 1(1)(f)(iii), (iv) or (vii) for any of the purposes listed in section 27(2).

(4) Individually identifying health information may be disclosed under this section without the consent of the individual who is the subject of the information.

(5) Where health information is requested under subsection (1)(b), the Department

- (a) must prepare a privacy impact assessment describing how disclosure of the health information may affect the privacy of the individual who is the subject of the information, and submit the privacy impact assessment to the Commissioner for review and comment, and
- (b) must consider the comments of the Commissioner, if any, made in response to the privacy impact assessment before disclosing the health information under subsection (3).

RSA 2000 cH-5 s46;2006 c18 s10

Disclosure to other custodians

47 (1) A custodian referred to in section 1(1)(f)(iii), (iv) or (vii) may request another custodian to disclose to the requesting custodian individually identifying health information for any of the purposes listed in section 27(2)

- (a) if the requesting custodian is authorized by an enactment of Alberta or Canada to obtain the information from the other custodian, or
- (b) if the information requested relates to a health service provided by the other custodian
 - (i) that is fully or partially paid for by the requesting custodian, or
 - (ii) that is provided using financial, physical or human resources provided or administered by the requesting custodian.

(2) Where a request relates to information described in subsection (1)(b), the custodian receiving the request may refuse to disclose the information if disclosure could reasonably be expected

- (a) to result in immediate and grave harm to the mental or physical health or safety of the individual who is the subject of the information,
- (b) to threaten the mental or physical health or safety of another individual, or
- (c) to pose a threat to public safety.

(3) If a custodian refuses to disclose information in accordance with subsection (2),

- (a) the custodian must provide the requesting custodian with non-identifying health information in the form requested by that custodian, and
- (b) the requesting custodian may ask for a review of that refusal by the Commissioner.

(4) In making a decision on a review under subsection (3)(b), the Commissioner must, if the custodian is a member of a health professional body, inform the health professional body of the review and provide an opportunity for that body to make comments to the Commissioner relating to the review.

(5) On receipt of information under this section, the requesting custodian may disclose the information

- (a) to a custodian referred to in section 1(1)(f)(iii), (iv) or (vii),
- (b) to the Minister, and
- (c) to the Department

for any of the purposes listed in section 27(2).

(6) Individually identifying health information may be disclosed under this section without the consent of the individual who is the subject of the information.

1999 cH-4.8 s47

Definition

48 In this Division, “health information” means individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

1999 cH-4.8 s48

Research proposal

49 A person who intends to conduct research may submit a proposal to a research ethics board for review by that board.

RSA 2000 cH-5 s49;2006 c18 s11

Role of research ethics board

50 (1) The research ethics board must

- (a) consider whether the researcher should be required to obtain consents for the disclosure of the health information to be used in the research from the individuals who are the subjects of the information, and
- (b) assess whether, in the opinion of the research ethics board,
 - (i) the proposed research is of sufficient importance that the public interest in the proposed research outweighs to a substantial degree the public interest in protecting the privacy of the individuals who are the subjects of the health information to be used in the research,
 - (ii) the researcher is qualified to carry out the research,
 - (iii) adequate safeguards will be in place at the time the research will be carried out to protect the privacy of the individuals who are the subjects of the health information to be used in the research and the confidentiality of that information, and
 - (iv) obtaining the consents referred to in clause (a) is unreasonable, impractical or not feasible.

(2) In making an assessment under subsection (1)(b), the research ethics board must consider the degree to which the proposed research may contribute to

- (b) identification, prevention or treatment of illness or disease,
- (c) scientific understanding relating to health,
- (d) promotion and protection of the health of individuals and communities,
- (e) improved delivery of health services, or
- (f) improvements in health system management.

(3) The research ethics board must prepare a response setting out

- (a) its recommendation under subsection (1)(a),
- (b) its assessment of the matters set out in subsection (1)(b), and
- (c) any conditions that the research ethics board considers should be imposed on the researcher.

(4) The research ethics board must send a copy of the response required in subsection (3) to the Commissioner.

Publication of response

50.1 If the response of the research ethics board sent to the Commissioner under section 50(4) indicates that the research ethics board is satisfied as to the matters referred to in section 50(1)(b), the Commissioner may publish the response in any manner the Commissioner considers appropriate.

2006 c18 s13

Bar to research

51 If the research ethics board is not satisfied as to any of the matters referred to in section 50(1)(b), the researcher may not apply to a custodian under section 52.

RSA 2000 cH-5 s51;2006 c18 s14

Application for disclosure of health information

52 If the research ethics board is satisfied as to the matters referred to in section 50(1)(b), the researcher may forward to one or more custodians

- (a) the response of the research ethics board to the researcher's proposal, and
- (b) a written application for disclosure of the health information to be used in the research.

RSA 2000 cH-5 s52;2006 c18 s14

Conditions and consents

53 (1) A custodian who has received the documents referred to in section 52 may, but is not required to, disclose the health information applied for.

(2) If the custodian decides to disclose the health information,

- (a) the custodian
 - (i) must impose on the researcher any conditions suggested by the research ethics board, and
 - (ii) may impose other conditions on the researcher,
- and
- (b) the researcher must obtain the consents referred to in section 50(1)(a), if recommended by the research ethics board, prior to the disclosure.

RSA 2000 cH-5 s53;2006 c18 s14

Agreement between custodian and researcher

54 (1) If the custodian decides to disclose health information to a researcher, the researcher must enter into an agreement with the custodian in which the researcher agrees

- (a) to comply with
 - (i) this Act and the regulations made under this Act,
 - (ii) any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information, and
 - (iii) any requirement imposed by the custodian to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information,
- (b) to use the health information only for the purpose of conducting the proposed research,

- (c) not to publish the health information in a form that could reasonably enable the identity of an individual who is the subject of the information to be readily ascertained,
- (d) not to make any attempt to contact an individual who is the subject of the health information to obtain additional health information unless the individual has provided the custodian with the consent referred to in section 55,
- (e) to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the enactments, conditions and requirements referred to in clause (a), and
- (f) to pay the costs referred to in subsection (3).

(2) When an agreement referred to in subsection (1) has been entered into, the custodian may disclose to the researcher the health information requested under section 52

- (a) with the consent of the individuals who are the subjects of the information, where the research ethics board recommends that consents should be obtained, or
- (b) without the consent of the individuals who are the subjects of the information, where the research ethics board does not recommend that consents be obtained.

(3) The custodian may set the costs of

- (a) preparing information for disclosure,
- (b) making copies of health information, and
- (c) obtaining the consents referred to in section 55,

which must not exceed the actual cost of providing that service.

(4) If the researcher contravenes or fails to meet the terms and conditions of an agreement under this section, the agreement is cancelled.

RSA 2000 cH-5 s54;2006 c18 s14

Consent for additional information

55 If the researcher wishes to contact the individuals who are the subjects of the information disclosed under section 54(2) to obtain additional health information, the custodian or an affiliate of the custodian must first obtain consents from those individuals to their being contacted for that purpose.

1999 cH-4.8 s55

Court order

56 (1) If a researcher refuses to allow a custodian to access or inspect its premises in accordance with the agreement referred to in section 54, the custodian may apply to the Court of Queen's Bench by notice of motion for an order under subsection (2).

(2) If the Court is satisfied that there are reasonable and probable grounds to believe that access to premises or the production or removal of documents is necessary for the purpose of determining whether an agreement referred to in section 54 is being complied with, the Court may make any order it considers necessary to enforce compliance with the agreement.

(3) Where authorized to do so by an order under subsection (2), a custodian may

- (a) enter and search any premises of the researcher where the research is conducted,

- (b) operate or cause to be operated any computer system of the researcher to search any data contained in or available to the system and produce a document from the data, and
- (c) seize and make copies of any documents of the researcher that are or may be relevant to the investigation.

(4) An application for an order under this section may be made ex parte unless the Court orders otherwise.

(5) The custodian must return any documents seized pursuant to a court order within 60 days after the conclusion of the investigation that gave rise to the seizure, including any hearing or appeal.

(6) In this section, “document” includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine readable record or other material or thing, regardless of physical form or characteristics.

1999 cH-4.8 s56

Appendix 4: Selected Sections of the Personal Information Protection Act

Standard as to what is reasonable

2. Where in this Act anything or any matter is described, characterized or referred to as reasonable or unreasonable, or is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner, the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

2003 cP-6.5 s2

Consent required

7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual, collect that information unless the individual consents to the collection of that information, collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source, use that information unless the individual consents to the use of that information, or disclose that information unless the individual consents to the disclosure of that information.

(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

(3) An individual may give a consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.

2003 cP-6.5 s7

Limitations on collection

11(1) An organization may collect personal information only for purposes that are reasonable.

(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.

2003 cP-6.5 s11

Notification required for collection

13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally as to the purposes for which the information is collected, and of the name of a person who is able to answer on behalf of the organization the individual's questions about the collection.

Collection without consent

14. An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:

- (a) a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- (b) the collection of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the collection;
- (c) the collection of the information is from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the personal information to the organization;
- (d) the collection of the information is reasonable for the purposes of an investigation or a legal proceeding;
- (e) the information is publicly available;
- (f) the collection of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;
- (g) the information is collected by a credit reporting organization to create a credit report where the individual consented to the disclosure to the credit reporting organization by the organization that originally collected the information;
- (h) the information may be disclosed to the organization without the consent of the individual under section 20;
- (i) the collection of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;
- (j) the organization collecting the information is an archival institution and the collection of the information is reasonable for archival purposes or research;
- (k) the collection of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

2003 cP-6.5 s14

Limitations on Use

16(1) An organization may use personal information only for purposes that are reasonable.

(2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.

Use without consent

17. An organization may use personal information about an individual without the consent of the individual but only if one or more of the following are applicable:

- (a) a reasonable person would consider that the use of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

- (b) the use of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the use;
- (c) the information was collected by the organization from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the information to the organization;
- (d) the use of the information is reasonable for the purposes of an investigation or a legal proceeding;
- (e) the information is publicly available;
- (f) the use of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;
- (g) a credit reporting organization was permitted to collect the information under section 14(g) and the information is not used by the credit reporting organization for any purpose other than to create a credit report;
- (h) the information may be disclosed by an organization without the consent of the individual under section 20;
- (i) the use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;
- (j) the use of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;
- (k) the organization using the information is an archival institution and the use of the information is reasonable for archival purposes or research;
- (l) the use of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

2003 cP-6.5 s17

Limitations on disclosure

19(1) An organization may disclose personal information only for purposes that are reasonable.

(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.

2003 cP-6.5 s19

Disclosure without consent

20. An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:

- (a) a reasonable person would consider that the disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- (b) the disclosure of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the disclosure;

- (c) the disclosure of the information is to a public body and that public body is authorized or required by an enactment of Alberta or Canada to collect the information from the organization;
- (d) the disclosure of the information is in accordance with a provision of a treaty that
 - (i) authorizes or requires its disclosure, and
 - (ii) is made under an enactment of Alberta or Canada;
- (e) the disclosure of the information is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information;
- (f) the disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation
 - (i) undertaken with a view to a law enforcement proceeding, or
 - (ii) from which a law enforcement proceeding is likely to result;
- (g) the disclosure of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;
- (h) the disclosure of the information is for the purposes of contacting the next of kin or a friend of an injured, ill or deceased individual;
- (i) the disclosure of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;
- (j) the information is publicly available;
- (k) the disclosure of the information is to the surviving spouse or adult interdependent partner or to a relative of a deceased individual if, in the opinion of the organization, the disclosure is reasonable;
- (l) the disclosure of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;
- (m) the disclosure of the information is reasonable for the purposes of an investigation or a legal proceeding;
- (n) the disclosure of the information is for the purposes of protecting against, or for the prevention, detection or suppression of, fraud, market manipulation or unfair trading practices and the organization that is disclosing the information or to which the information is being disclosed is permitted or otherwise empowered or recognized under an enactment of Alberta or Canada or of another province of Canada to carry out any of those purposes;
- (o) the organization is a credit reporting organization and is permitted to disclose the information under Part 5 of the Fair Trading Act;
- (p) the organization disclosing the information is an archival institution and the disclosure of the information is reasonable for archival purposes or research;
- (q) the disclosure of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

2003 cP-6.5 s20

Non-profit organizations

56(1) In this section,

- (a) "commercial activity" means
 - (i) any transaction, act or conduct, or
 - (ii) any regular course of conduct, that is of a commercial character and, without restricting the generality of the foregoing, includes the following:
 - (iii) the selling, bartering or leasing of membership lists or of donor or other fund-raising lists;
 - (iv) the operation of a private school or an early childhood services program as defined in the School Act;
 - (v) the operation of a private college as defined in the Post-secondary Learning Act;
- (b) "non-profit organization" means an organization
 - (i) that is incorporated under the Societies Act or the Agricultural Societies Act or that is registered under Part 9 of the Companies Act, or
 - (ii) that meets the criteria established under the regulations to qualify as a non-profit organization.

(2) Subject to subsection (3), this Act does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization.

(3) This Act applies to a non-profit organization in the case of personal information that is collected, used or disclosed by the non-profit organization in connection with any commercial activity carried out by the non-profit organization.

- (4) The Lieutenant Governor in Council may make regulations
- (a) establishing, for the purposes of subsection (1)(b)(ii), the criteria to be met by an organization to qualify as a non-profit organization;
 - (b) establishing the criteria to be met by non-profit organizations to qualify as non-profit organizations that are restricted or otherwise limited in the scope of their operations and exempting those non-profit organizations from the operation of subsection (3);
 - (c) governing the coming into force of this Act or any provision of this Act with respect to a non-profit organization;
 - (d) providing that this Act or any provision of this Act commences to apply to a non-profit organization at a date that is later than January 1, 2004;
 - (e) providing for and governing any transitional matter relating to the application of this Act to a non-profit organization.

(5) Any regulation made under this section may be general or specific in its application.

2003 cP-6.5 s56;2005 c29 s4

Appendix 5: Selected Sections of the Personal Information Protection and Electronic Documents Act

Collection without knowledge or consent

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if
- (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
 - (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
 - (c) the collection is solely for journalistic, artistic or literary purposes; or
 - (d) the information is publicly available and is specified by the regulations.

Use without knowledge or consent

- (2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if
- (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;
 - (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
 - (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the
 - (c.1) it is publicly available and is specified by the regulations; or
 - (d) it was collected under paragraph (1)(a) or (b).

Disclosure without knowledge or consent

- (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
- (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;
 - (b) for the purpose of collecting a debt owed by the individual to the organization;

- (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
- (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
 - (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
 - (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
 - (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;
- (d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization
 - (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
 - (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
- (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;
- (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;
- (g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;
- (h) made after the earlier of
 - (i) one hundred years after the record containing the information was created, and
 - (ii) twenty years after the death of the individual whom the information is about;
- (h.1) of information that is publicly available and is specified by the regulations;
- (h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or
- (i) required by law.

Appendix 6: Selected Sections of the Privacy Act

Collection of personal information

4. No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

1980-81-82-83, c. 111, Sch. II "4".

Personal information to be collected directly

5. (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).

Individual to be informed of purpose

(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

Exception

(3) Subsections (1) and (2) do not apply where compliance therewith might

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

1980-81-82-83, c. 111, Sch. II "5".

Use of personal information

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

Disclosure of personal information

8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

- (c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
- (d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;
- (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
- (f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;
- (g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;
- (h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;
- (i) to the National Archives of Canada for archival purposes;
- (j) to any person or body for research or statistical purposes if the head of the government institution
 - (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
 - (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;
- (k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;
- (l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and
- (m) for any purpose where, in the opinion of the head of the institution,
 - (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
 - (ii) disclosure would clearly benefit the individual to whom the information relates.

Copies of requests under paragraph (2)(e) to be retained

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to

the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.

Notice of disclosure under paragraph (2)(m)

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.

Record of disclosures to be retained

9. (1) The head of a government institution shall retain a record of any use by the institution of personal information contained in a personal information bank or any use or purpose for which that information is disclosed by the institution where the use or purpose is not included in the statements of uses and purposes set forth pursuant to subparagraph 11(1)(a)(iv) and subsection 11(2) in the index referred to in section 11, and shall attach the record to the personal information.

Limitation

(2) Subsection (1) does not apply in respect of information disclosed pursuant to paragraph 8(2)(e).

Record forms part of personal information

(3) For the purposes of this Act, a record retained under subsection (1) shall be deemed to form part of the personal information to which it is attached.

Consistent uses

(4) Where personal information in a personal information bank under the control of a government institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not included in the statement of consistent uses set forth pursuant to subparagraph 11(1)(a)(iv) in the index referred to in section 11, the head of the government institution shall

- (a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and
- (b) ensure that the use is included in the next statement of consistent uses set forth in the index.

1980-81-82-83, c. 111, Sch. II "9"; 1984, c. 21, s. 89.

