CONVERGE

REIMAGINING CANADA'S MENTAL HEALTH SYSTEMS – TOGETHER.

Alberta Specific Appendices

List of Alberta Specific Appendices for the Information Sharing Framework

This includes the following appendices.

Notes:

Appendix B is in landscape rather than portrait format.

The remaining appendices are contained in the Second Set (General), which do not reference or rely on specific jurisdictional legislation.

Appendix A: Applicable Legislation Back

Appendix A: Applicable Legislation - Alberta

References to legislation are to those listed and cited below. Note that there will be additional legislation that may have to be considered, depending in part on the areas being served. For example, Children's Services staff are also responsible for complying with the *Child, Youth and Family Enhancement Act*.

The following legislation is available at Alberta King's Printer (© Alberta King's Printer, 20__):

Alberta King's Printer: Laws Online/Catalogue

***Access to Information Act* (ATIA)**
A-1.4 2024 *(Current to June 11, 2025)*

Canadian Centre of Recovery Excellence Act
C-1.5 *(Current to June 11, 2025)*

Children First Act
C-12.5 2013 *(Current to June 11, 2025)*

Education Act
Chapter E 0.3, 2012 *(Current to June 11, 2025)*

Emergency Health Services Act
Chapter E-6.6, 2008 *(Current to June 11, 2025)*

***Health Information Act* (HIA)**
H-5 RSA 2000 *(Current to June 11, 2025)*

Health Information Regulation
70/2001 *(Current to December 20, 2024)*

Health Professions Act
H-7 RSA 2000 *(Current to May 15, 2025)*

***Personal Information Protection Act* (PIPA)**
P-6.5 2003 *(Current to June 11, 2025)*

Police Act
P-17 RSA 2000 *Current to July 2, 2025)*

***Protection of Privacy Act* (POPA)**
P-28.5 2024 *(Current to June 11, 2025*

Protection of Privacy Regulation
132/2025 *(Current to June 11, 2025)*

Protection of Privacy (Ministerial) Regulation
143/2025 *(Current to June 11, 2025)*

The following legislation is available on the Justice (Canada) Laws Website:

Consolidated Acts (justice.gc.ca)

***Personal Information Protection and Electronic Documents Act* (PIPEDA - Federal)**
S.C. 2000, c. 5

***Privacy Act* (Federal)**
R.S.C., 1985, c. P-21

Youth Criminal Justice Act (YCJA)
S.C. 2002, c. 1

Notes Re: Specific Legislative References Found in the Framework

Please note the sections listed below are excerpts from the applicable legislation, and are the ones identified as potentially appropriate for the circumstances of collaborative/integrated service delivery. As such, they may not be the complete sections, and it behooves organizations to conduct a thorough review to determine applicability to their circumstances.

1. Legislation that Might Apply to the Scenario (Back)

The *Protection of Privacy Act* (POPA), which could authorize disclosure by the School Board to the health services provider:

- For the purpose it was collected, [s.13(1)(b)]
- With consent, [s.13(1)(c)]
- To determine eligibility for a program or service, [s.13(1)(k)]
- To avert the risk of harm to a minor, [s.13(1)(cc)(i)]
- To avert the risk of imminent harm to a person, [s.13(1)(cc)(ii)] See also POPA Regulation 1(1)(b) definition of "imminent harm", or
- In the best interest of the minor [s.13(1)(ee)].

The *Access to Information Act* (ATIA), which could authorize disclosure by the School Board to the health services provider:

- To avert risk to the safety of the public, [s.37(1)]

The *Health Information Act* (HIA), which could authorize disclosure by the health services provider to the School Board:

- With consent, [s.34]

- To avert the risk of harm to a minor, [s.35(1)(m)(i)]
- To avert the risk of significant harm to a person [s.35(1)(m)(ii)], or
- To a person responsible for continuing treatment and care, [s.35(1)(b)].

The *Personal Information Protection Act* (PIPA) may apply if the social worker, psychologist, or other allied health professional is working independently, as a private sector entity. The act could authorize the disclosure by the social worker of psychologist to the school board:

- With consent, [s.7(1)]
- With provision of notice and appropriate time provided to respond, [s.8(3)]
- Where the disclosure is clearly in the best interests of the individual, but consent cannot be obtained in a timely way or is not likely to be withheld, [s.20(a)]

The *Children First Act*, which could authorize the disclosure of health information, without consent, about the child by the health services provider:

- to enable the planning and provision of services to a minor youth, if in the best interest of the minor [s.4(2)(b)].

2. Provincial Public Sector Organizations (Back)

- In Alberta, public sector organizations are subject to the *Protection of Privacy Act* [s. 1(u)] and the *Access to Information Act* [s. 1(t)], which define a "public body" to mean:
  (i) a department, branch or office of the Government of Alberta,
  (ii) an agency, board, commission, corporation, office or other body designated as a public body in the regulations,
  (vi) the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, the Information and Privacy Commissioner, the Child and Youth Advocate or the Public Interest Commissioner, or
  (vii) a local public body,

  A "local public body" is defined to mean:
  (i) an educational body,
  (ii) a health care body, or
  (iii) a local government body;

3. Health Organizations (Back)

- In Alberta, health sector organizations and entities may be subject to the *Health Information Act* (HIA), which defines "custodians" to include among others:
  (i) the board of an approved hospital as defined in the *Hospitals Act* ...;
  (ii) the operator of a continuing care home as defined in the Continuing Care Act ...;
  (ii.1) an ambulance operator as defined in the *Emergency Health Services Act*;
  (iii) a provincial health corporation as defined in the *Provincial Health Agencies Act*;
  (ix) a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause;
  (xii) the Department;
  (xii.1) the Department of Mental Health and Addiction;

- The HIA Regulation designates the following health services providers as custodians: are designated as custodians: ([s. 2(2)]
  (a) regulated members of the Alberta College and Association of Chiropractors;
  (b) regulated members of the Alberta College of Optometrists;

(c) regulated members of the Alberta College of Pharmacists;
(d) regulated members of the Alberta Dental Association and College;
(e) regulated members of the College and Association of Registered Nurses of Alberta;
(f) regulated members of the College of Alberta Denturists;
(g) registered members of the College of Midwives of Alberta;
(h) regulated members of the College of Opticians of Alberta;
(i) regulated members of the College of Physicians and Surgeons of Alberta;
(j) regulated members of the College of Podiatric Physicians of Alberta;
(k) regulated members of the College of Registered Dental Hygienists of Alberta.

4. Private Sector Organizations Subject to Provincial/Territorial Legislation (Back)
   - Private Sector organizations in Alberta are subject to the *Personal Information Protection Act* (PIPA). This does not include nonprofit agencies unless they are managing personal and health in the course of a commercial activity, in which case the information managed under that activity is subject to PIPA; or when managing personal and health information on behalf of an organization that is (e.g. for an institution under a contract or agreement).
   - 4(1) Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information.

     Note: The act and regulations go on to indicate that it does not apply in a number of areas, including where other privacy legislation applies, and to the information about an individual managed by themselves.

5. Private Sector Organizations Subject to PIPEDA (Back)
   - PIPEDA does not apply to private sector organizations in jurisdictions where substantially similar legislation applies, including Alberta. However, the Act could apply in situations where personal information flows across jurisdictional borders.
   - PIPEDA s. 4(1) Except as provided in this Act and subject to the regulations, this Act applies to every organization and in respect of all personal information.
     1(1) (i) "organization" includes
     (i) a corporation,
     (ii) an unincorporated association,
     (iii) a trade union as defined in the Labour Relations Code,
     (iv) a partnership as defined in the Partnership Act, and
     (v) an individual acting in a commercial capacity, but does not include an individual acting in a personal or domestic capacity;

6. Federal Institutions (Back)
   - Privacy Act s.3 In this Act, government institution means
     (a) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and
     (b) any parent Crown corporation, and any wholly owned subsidiary of such a corporation, within the meaning of section 83 of the Financial Administration Act;

7. Organizations Not Generally Subject to Privacy Legislation (Back)
   - Where there is potential to involve organizations that are not subject to any oversight legislation as members of a collaborative partnership, a set of minimum standards should be established that mirror the expectations placed on other member organizations through their applicable legislation. Such organizations would be required to demonstrate how they meet those minimum requirements, and assistance to those who are not at the

required level could be offered if their involvement is desired. A recommendation is to require the organizations to commit to aligning their policies and practices such that they would comply with private sector privacy legislation in their jurisdiction. In Alberta this would mean aligning with PIPA.

8. Collection (Back)

- HIA s.18 No custodian shall collect health information except in accordance with this Act.
- HIA s. 20 A custodian may collect individually identifying health information
  (a) if the collection of that information is expressly authorized by an enactment of Alberta or Canada, or
  (b) if that information relates directly to and is necessary to enable the custodian to carry out a purpose that is authorized under section 27.
- See also Note 11 – Use, below.

- PIPA s.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.
- S.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 authorized or required by
    (i) a statute of Alberta or of Canada,
    (ii) a regulation of Alberta or a regulation of Canada,
    (iii) a bylaw of a local government body, or
    (iv) a legislative instrument of a professional regulatory organization;
  (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 information to the organization;
  (d) the collection of the information is reasonable for the purposes of an investigation or a legal proceeding;
  (h) the information may be disclosed to the organization without the consent of the individual under section 20;

- POPA s.4 No personal information may be collected by or on behalf of 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, including a common or integrated program or service.

- PIPEDA s. 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.

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

9. Notice (Back)

Generally, refers to the need to inform the individual to whom the information relates what information is required, how it will be used, and to whom it may be disclosed, as well as the contact information of someone/position who can answer the individual's questions about the collection.

- HIA s.22(3) When collecting individually identifying health information about an individual directly from the individual, the custodian must take reasonable steps to inform the individual
  (a) of the purpose for which the information is collected,
  (b) of the specific legal authority for the collection, and
  (c) of the title, business address and business telephone number of an affiliate of the custodian who can answer the individual's questions about the collection.

- PIPA s.7 (3) Notwithstanding section 7(1), an organization may collect, use or disclose personal information about an individual for particular purposes if
  (a) the organization
    (i) provides the individual with a notice, in a form that the individual can reasonably be expected to understand, that the organization intends to collect, use or disclose personal information about the individual for those purposes, and
    (ii) with respect to that notice, gives the individual a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for those purposes,
  ...
- s.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
  (a) as to the purposes for which the information is collected, and
  (b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

- POPA s.5(2) Subject to subsections (3) and (4), a public body that collects personal information that is required by subsection (1) to be collected directly from the individual the information is about must give notice to the individual, at the time of collection, of
  (a) the purpose for which the information is collected,
  (b) the specific legal authority for the collection,
  (c) the email address, telephone number or other contact information to which the individual may direct the individual's questions about the collection, and
  (d) the public body's intention, if any, at that time to input the information into an automated system to generate content or make decisions, recommendations or predictions.
  (3) Subsections (1) and (2) do not apply if, in the opinion of the head of the public body concerned, it could reasonably be expected that the information collected would be inaccurate.
  (4) Subsection (2) does not apply where a public body previously gave notice to an individual under that subsection and the public body continues to collect personal information from that individual for the same purpose and under the same specific legal authority as identified in the notice.

- PIPEDA s. 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
  (a) as to the purposes for which the information is collected, and
  (b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.
  (3) Before or at the time personal information about an individual is collected from another organization without the consent of the individual, the organization collecting the personal information must provide the organization that is disclosing the personal information with sufficient information regarding the purpose for which the personal information is being collected in order to allow the organization that is disclosing the personal information to make a determination as to whether that disclosure of the personal information would be in accordance with this Act.
  (4) Subsection (1) does not apply to the collection of personal information that is carried out pursuant to section 8(2).
- PIPEDA SCHEDULE 1 (Section 5) 4.2.3
  The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

- Privacy Act s. 5 (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.

10. Indirect Collection (6.3.3) refers to Manner of Collection. Relevant legislative provisions may include:
    - HIA s.22(1) A custodian must collect individually identifying health information directly from the individual who is the health information from a person other than the individual who is the subject of the information in the following circumstances:
      (a) where the individual who is the subject of the information authorizes collection of the information from someone else;
      (b) where the individual who is the subject of the information is unable to provide the information and the custodian collects the information from a person referred to in section 104(1)(c) to (i)who is acting on behalf of that individual;
      (c) where the custodian believes, on reasonable grounds, that collection from the individual who is the subject of the information would prejudice
      (i) the interests of the individual,
      (ii) the purposes of collection, or
      (iii) the safety of any other individual,
      or would result in the collection of inaccurate information;
      (d) where collection from the individual who is the subject of the information is not reasonably practicable;
      (g) where disclosure of the information is authorized under Part 5;
      (h) where disclosure of the information is authorized by an enactment of Alberta or Canada.

    - PIPA s. 7 (1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,

(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,

- s.12 An organization may without the consent of the individual collect personal information about an individual from a source other than that individual if the information that is to be collected is information that may be collected without the consent of the individual under section 14, 14.1, 15 or 22.

- POPA s.5(1) Subject to subsection (3), a public body must collect personal information directly from the individual the information is about unless
  (a) another method of collection is authorized by
    (i) that individual,
    (ii) another Act or a regulation under another Act, or
    (iii) the Commissioner under section 27(1)(h),
  (b) the information may be disclosed to the public body under Division 2 of this Part,
  (c) the information is collected in a health or safety emergency where
    (i) the individual is not able to provide the information directly, or
    (ii) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person,
  (d) the information concerns an individual who is designated as a person to be contacted in an emergency or other specified circumstances,
  (g) the information is collected for the purpose of law enforcement,
  (i) the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority,
  (k) the information is necessary
    (i) to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of Alberta or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or
    (ii) to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Government of Alberta or a public body and is collected for that purpose,
  (l) the information is collected for the purpose of informing the Public Trustee or a Public Guardian about clients or potential clients,
  (o) the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people, or
  (p) the information is necessary to plan, administer, deliver, manage, monitor or evaluate a common or integrated program or service.

- PIPEDA s. 12 An organization may without the consent of the individual collect personal information about an individual from a source other than that individual if the information that is to be collected is information that may be collected without the consent of the individual under section 14, 14.1, 15 or 22.

- Privacy Act s. 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).
  (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.

(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.

11. Use (Back)

- PIPA s. 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.

- HIA s.27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:
  (a) providing health services;
  (b) determining or verifying the eligibility of an individual to receive a health service;
  (c) conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline;
  (d) conducting research or performing data matching or other services to facilitate another person's research
    (i) if the custodian or researcher has submitted a proposed research protocol to a research ethics board in accordance with section 49,
    (ii) if the research ethics board is satisfied as to the matters referred to in section 50(1)(b),
    (iii) if the custodian or researcher has complied with or undertaken to comply with the conditions, if any, suggested by the research ethics board, and
    (iv) where the research ethics board recommends that consents should be obtained from the individuals who are the subjects of the health information to be used in the research, if those consents have been obtained;
  (e) providing for health services provider education;
  (f) carrying out any purpose authorized by an enactment of Alberta or Canada;
  (g) for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

- POPA s. 12(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 under section 13, 15 or 16.

- PIPEDA s. 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.

- Privacy Act s. 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).

12. Consistent Purpose (Back)

- HIA s.27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:
  (a) providing health services;
  (b) determining or verifying the eligibility of an individual to receive a health service;
  (c) conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline;
  (d) conducting research or performing data matching or other services to facilitate another person's research
    (i) if the custodian or researcher has submitted a proposed research protocol to a research ethics board in accordance with section 49,
    (ii) if the research ethics board is satisfied as to the matters referred to in section 50(1)(b),
    (iii) if the custodian or researcher has complied with or undertaken to comply with the conditions, if any, suggested by the research ethics board, and
    (iv) where the research ethics board recommends that consents should be obtained from the individuals who are the subjects of the health information to be used in the research, if those consents have been obtained;
  (e) providing for health services provider education;
  (f) carrying out any purpose authorized by an enactment of Alberta or Canada;
  (g) for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

- POPA s. 14 For the purposes of sections 12(1)(a) and 13(1)(b), 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 or common or integrated program or service of, the public body that uses or discloses the information.

- Privacy Act s.9(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.

13. Health and Safety (Back)

- HIA s. 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
  (m) to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize

(i) a risk of harm to the health or safety of a minor, or
(ii) a significant risk of harm to the health or safety of any person,

- POPA s. 13(1) A public body may disclose personal information only
(cc) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize
(i) a risk of harm to the health or safety of a minor, or
(ii) an imminent danger to the health or safety of any person.
- Protection of Privacy Regulation: s. 1(1) For the purposes of the Act,
(b) "imminent danger" includes a situation in which the head of a public body believes, on reasonable grounds, that
(i) there is a significant risk of harm to the health or safety of a person, and
(ii) disclosure of personal information is necessary to protect the health or safety of the person

- PIPA s. 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;
(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;

- PIPEDA s.7 (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
(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;
(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.1).

- Privacy Act s.8 (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
(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.

14. Disclosure (Back)

- HIA s.31 No custodian shall disclose health information except in accordance with this Act.
- S.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.
- S.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,
(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,
(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 or continuing treatment and care to the individual,
(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,
(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
    (i) a risk of harm to the health or safety of a minor, or
    (ii) a significant risk of harm 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,
(p) if the disclosure is authorized or required by an enactment of Alberta or Canada,

- PIPA s.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.
- s.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 authorized or required by
      (i) a statute of Alberta or of Canada,
      (ii) a regulation of Alberta or a regulation of Canada,
      (iii) a bylaw of a local government body, or
      (iv) a legislative instrument of a professional regulatory organization;
  (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;

(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;
(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, and the information is disclosed to or by
(i) an organization that is permitted or otherwise empowered or recognized to carry out any of those purposes under
(A) a statute of Alberta or of Canada or of another province of Canada,

- POPA s.13(1) A public body may disclose personal information only
(a) if the disclosure would not be an unreasonable invasion of personal privacy under section 20 of the Access to Information Act,
(b) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
(c) if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure,
(d) 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,
(e) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,
(f) 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,
(g) 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,
(h) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service and for the performance of the duties of the officer, employee or member to whom the information is disclosed,
(k) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,
(p) 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,
(q) 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,
(r) so that the spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted,

(s) 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,
(t) in accordance with section 15 (*research purposes)* or 16,
(y) to an officer of the Legislature if the information is necessary for the performance of the duties of that officer,
(z) for the purpose of supervising an individual under the control or supervision of a correctional authority,
(aa) to a lawyer or student at law acting for an inmate under the control or supervision of a correctional authority,
(cc) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize
(i) a risk of harm to the health or safety of a minor, or
(ii) an imminent danger to the health or safety of any person,
(ee) to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor, or
(ff) to another public body for the purpose of carrying out data matching to create data derived from personal information under section 17(1).
(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.

- PIPEDA s.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 authorized or required by
(i) a statute of Alberta or of Canada,
(ii) a regulation of Alberta or a regulation of Canada,
(iii) a bylaw of a local government body, or
(iv) a legislative instrument of a professional regulatory organization;
(b.1) the disclosure of the information is for a purpose for which the information was collected pursuant to a form that is approved or otherwise provided for under a statute of Alberta or a regulation of Alberta;
(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;
(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;
(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, and the information is disclosed to or by
(i) an organization that is permitted or otherwise empowered or recognized to carry out any of those purposes under
(A) a statute of Alberta or of Canada or of another province of Canada,
(B) a regulation of Alberta, a regulation of Canada or similar subordinate legislation of another province of Canada that, if enacted in Alberta, would constitute a regulation of Alberta, or
(C) an order made by a Minister under a statute or regulation referred to in paragraph (A) or (B),
(ii) Équité Association, or
(iii) the Canadian Bankers Association, Bank Crime Prevention and Investigation Office;

- Privacy Act s. 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.
(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 any of its institutions and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act, the council of a participating First Nation as defined in section 2 of the Anishinabek Nation Education Agreement Act,

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;
(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; 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;
(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.

15. Corrections (Back)

- HIA s.13(1) An individual who believes there is an error or omission in the individual's health information may in writing request the custodian that has the information in its custody or under its control to correct or amend the information.

- PIPA s. 25(1) An individual may, in accordance with section 26, request an organization to correct an error or omission in the personal information about the individual that is under the control of the organization.

- POPA s.7(1) An individual who believes there is an error or omission in the individual's personal information may request the head of the public body that has the information in its custody or under its control to correct the information.
(2) Despite subsection (1), the head of a public body must not correct an opinion, including a professional or expert opinion.

- PIPEDA s. 25(1) An individual may, in accordance with section 26, request an organization to correct an error or omission in the personal information about the individual that is under the control of the organization.

- Privacy Act s. 12 (2) Every individual who is given access under paragraph (1)(a) to personal information that has been used, is being used or is available for use for an administrative purpose is entitled to
(a) request correction of the personal information where the individual believes there is an error or omission therein;
(b) require that a notation be attached to the information reflecting any correction requested but not made; and
(c) require that any person or body to whom that information has been disclosed for use for an administrative purpose within two years prior to the time a correction is requested or a notation is required under this subsection in respect of that information

(i) be notified of the correction or notation, and
(ii) where the disclosure is to a government institution, the institution make the correction or notation on any copy of the information under its control.

16. Right of Access by Individuals (Back)

- ATIA s.6(1) An applicant has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.
  (2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.

- HIA s. 7(1) An individual has a right of access to any record containing health information about the individual that is in the custody or under the control of a custodian.
  (2) The right of access to a record does not extend to information in respect of which a custodian is authorized or required to refuse access under section 11, but if that information can reasonably be severed from a record, an individual has a right of access to the remainder of the record.
  (3) The right of access to a record is subject to the payment of any fee required by the regulations.

- PIPA s. 24(1) An individual may, in accordance with section 26, request an organization
  (a) to provide the individual with access to personal information about the individual, or
  (b) to provide the individual with information about the use or disclosure of personal information about the individual.

- PIPEDA s. 24(1) An individual may, in accordance with section 26, request an organization
  (a) to provide the individual with access to personal information about the individual, or
  (b) to provide the individual with information about the use or disclosure of personal information about the individual.

- Privacy Act s. 12 (1) Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to
  (a) any personal information about the individual contained in a personal information bank; and
  (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

17. Retention (Back)

- PIPA s. 35(1) An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.

- POPA s. 6 If an individual's personal information will be used by a public body to make a decision that directly affects the individual, including a decision made using an automated system, the public body must

(a) make every reasonable effort to ensure that the information is accurate and complete, and
(b) retain the information for at least one year after using it so the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by
(i) the individual,
(ii) the public body, and
(iii) if the body that approves the records retention and disposition schedule for the public body is different from the public body, that body.

- PIPEDA s. 35(1) An organization may retain personal information only for as long as the organization reasonably requires the personal information for legal or business purposes.
(2) Within a reasonable period of time after an organization no longer reasonably requires personal information for legal or business purposes, the organization must
(a) destroy the records containing the personal information, or
(b) render the personal information non-identifying so that it can no longer be used to identify an individual.

- Privacy Act s. 6 (1) Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

18. Records (Back)

- HIA s.1(1) In this Act,
(t) "record" means a record of health information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records;

- PIPA s.1(1) (m) "record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or any other form, but does not include a computer program or other mechanism that can produce a record;

- POPA s.1 In this Act,
(v) "record" means a record as defined in the Access to Information Act;
- ATIA s.1(u) "record" means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio or other medium, but does not include any software or other mechanism used to store or produce the record;

- PIPEDA s. 1(1) In this Act,
(m) "record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or any other form, but does not include a computer program or other mechanism that can produce a record;

- Privacy Act s.3 In this Act, personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

19. Consent Requirements (Back)

- HIA s.34(2) A consent referred to in subsection (1) must be provided in writing or electronically and must include
  (a) an authorization for the custodian to disclose the health information specified in the consent,
  (b) the purpose for which the health information may be disclosed,
  (c) the identity of the person to whom the health information may be disclosed,
  (d) 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,
  (e) the date the consent is effective and the date, if any, on which the consent expires, and
  (f) 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.

- PIPA s. 7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,
  (a) collect that information unless the individual consents to the collection of that information,
  (b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,
- PIPA s. 8(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual.
  (2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if
  (a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose, and
  (b) it is reasonable that a person would voluntarily provide that information.
- See also Note 9 – Notice.

- POPA Regulation s.2(2) An individual's consent to a public body using or disclosing any of the individual's personal information under section 12(1)(b) or 13(1)(c) of the Act
  (a) must meet the requirements of subsection (3), (4) or (5),
  (b) must specify the personal information to which the consent relates,
  (c) must specify to whom the personal information may be disclosed and how the personal information may be used, and
  (d) must specify the date on which the consent is effective and, if applicable, the date on which the consent expires.
  (3) For the purposes of this section, a consent in writing is valid if it is signed by the individual who is giving the consent.
  (4) For the purposes of this section, an electronic consent is valid if
  (a) the head of the public body has established rules respecting the purposes for which electronic consent is acceptable,
  (b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),
  (c) the public body has explicitly communicated that it will accept electronic consent,
  (d) the electronic consent

(i) is accessible by the public body so as to be usable for subsequent reference,
(ii) is capable of being retained by the public body,
(iii) can be authenticated in a manner that allows the individual giving the consent to be identified, and
(iv) meets the information technology standards, if any, established by the public body,
(e) the electronic consent includes the electronic signature of the individual giving the consent,
(f) the electronic consent is provided in a manner consistent with the electronic signature requirements in section 16(2) of the Electronic Transactions Act, and
(g) the association of the electronic signature with the consent is reliable for the purpose for which consent is given.
(5) For the purposes of this section, a consent that is given orally is valid if
(a) the head of the public body has established rules respecting the purposes for which consent that is given orally is acceptable,
(b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),
(c) the public body has explicitly communicated that it will accept consent that is given orally,
(d) the record of the consent
(i) is accessible by the public body so as to be usable for subsequent reference, and
(ii) is capable of being retained by the public body,
(e) the public body has authenticated the identity of the individual giving consent, and
(f) the method of authentication is reliable for verifying the identity of the individual and for associating the consent with the individual.
(6) For the purposes of subsection (5)(d), the record of the consent must be
(a) an audio recording of the consent created by or on behalf of the public body,
(b) in the form of documentation of the consent created by an independent third party, or
(c) in the form of documentation of the consent created by the public body in accordance with the rules established by the head of the public body.
(7) Notwithstanding subsections (3) to (5), the consent of a minor is not valid unless the public body has determined, on reasonable grounds, that the minor has the capacity to understand the information relevant to providing consent and appreciates the consequences of providing consent.
(8) Despite anything to the contrary in this section, a consent under section 12(1)(b) *(See Note 11 – Use)* or 13(1)(c) *(See Note 13 – Disclosure)*of the Act is no longer valid if an individual provides notice to a public body that the individual withdraws the individual's consent.
(9) Nothing in this section requires an individual to give consent in an electronic form or orally.

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

- Privacy Act s. 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).
- s.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).
- s.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.
- s.19 (2) The head of a government institution may disclose any personal information requested under subsection 12(1) that was obtained from any government, organization or institution described in subsection (1) if the government, organization or institution from which the information was obtained
  (a) consents to the disclosure;

20. Professional College (Back)

- *Health Professions Act* s.1(1) In this Act,
  (e) "college" means the college of a regulated profession;
  "health profession" means a health profession set out in Schedule 1;

- s.3(1) A college
  (c) must establish, maintain and enforce standards for registration and of continuing competence and standards of practice of the regulated profession,

SCHEDULES

Green highlights indicates designation as custodians under the HIA.

SCHEDULE 1 – PROFESSION OF ACUPUNCTURISTS
SCHEDULE 2 – PROFESSION OF CHIROPRACTORS
SCHEDULE 3 – PROFESSION OF COMBINED LABORATORY AND X-RAY TECHNOLOGISTS
SCHEDULE 4 – PROFESSION OF DENTAL ASSISTANTS
SCHEDULE 5 – PROFESSION OF DENTAL HYGIENISTS
SCHEDULE 6 – PROFESSION OF DENTAL TECHNOLOGISTS
SCHEDULE 7 – PROFESSION OF DENTISTS
SCHEDULE 8 – PROFESSION OF DENTURISTS
SCHEDULE 9 – PROFESSION OF HEARING AID PRACTITIONERS
SCHEDULE 10 – PROFESSION OF LICENSED PRACTICAL NURSES
SCHEDULE 11 – PROFESSION OF MEDICAL LABORATORY TECHNOLOGISTS
SCHEDULE 12 – PROFESSION OF MEDICAL DIAGNOSTIC AND THERAPEUTIC TECHNOLOGISTS
SCHEDULE 13 – PROFESSION OF MIDWIVES
SCHEDULE 14 – PROFESSION OF NATUROPATHS
SCHEDULE 15 – PROFESSION OF OCCUPATIONAL THERAPISTS
SCHEDULE 16 – PROFESSION OF OPTICIANS
SCHEDULE 17 – PROFESSION OF OPTOMETRISTS
SCHEDULE 18 – PROFESSION OF PARAMEDICS
SCHEDULE 19 – PROFESSION OF PHARMACISTS AND PHARMACY TECHNICIANS
SCHEDULE 20 – PROFESSION OF PHYSIOTHERAPISTS
SCHEDULE 21 – PROFESSION OF PHYSICIANS, SURGEONS, OSTEOPATHS AND PHYSICIAN ASSISTANTS
SCHEDULE 21.1 – PROFESSION OF PODIATRISTS
SCHEDULE 22 – PROFESSION OF PSYCHOLOGISTS
SCHEDULE 23 – PROFESSION OF REGISTERED DIETITIANS AND REGISTERED NUTRITIONISTS
SCHEDULE 24 – PROFESSION OF REGISTERED NURSES
SCHEDULE 25 – PROFESSION OF REGISTERED PSYCHIATRIC NURSES
SCHEDULE 26 – PROFESSION OF RESPIRATORY THERAPISTS
SCHEDULE 27 – PROFESSION OF SOCIAL WORKERS
SCHEDULE 28 – PROFESSION OF SPEECH-LANGUAGE PATHOLOGISTS AND AUDIOLOGISTS

21. Security of Information (Back)

- HIA s.60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
  (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,
  (b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information,
  (c) protect against any reasonably anticipated
  (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or

(ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
and
(d) otherwise ensure compliance with this Act by the custodian and its affiliates.
(2) The safeguards to be maintained under subsection (1) must include appropriate measures
(a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, and
(b) for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.
(3) In subsection (2)(a), "electronic health records" means records of health information in electronic form.

- PIPA s. 34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

- POPA s.10(1) The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction

- PIPEDA s. 34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

22. Breaches (Back)

- HIA s.60.1(1) Subject to the regulations, an affiliate of a custodian must as soon as practicable notify the custodian in accordance with the regulations of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian.
(2) Subject to the regulations, subsections (4) and (5) and section 85.1, a custodian must as soon as practicable give notice in accordance with the regulations and subsection (3) of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.
(3) The notice required by subsection (2) must be given to
(a) the Commissioner,
(b) the Minister, and
(c) the individual who is the subject of the individually identifying health information.
(4) A custodian must consider all relevant factors, including the factors prescribed by the regulations, in assessing for the purposes of subsection (2) whether there is a risk of harm to an individual.
(5 If a custodian considers that giving notice under subsection (2) to an individual who is the subject of individually identifying health information could reasonably be expected to result in a risk of harm to the individual's mental or physical health, the custodian may

decide not to give notice to the individual, in which case the custodian must immediately give notice to the Commissioner of the decision not to give notice to the individual, and the reasons for the decision, in accordance with the regulations.

- PIPA s. 34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

- POPA s.10(2) If an incident occurs involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody or under the control of a public body where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, unauthorized access or unauthorized disclosure, the public body must give notice, without unreasonable delay, of the incident to the following:
  (a) the individual to whom there exists a real risk of significant harm;
  (b) the Commissioner;
  (c) the Minister.
  (3) A notice given under subsection (2) must comply with the prescribed requirements.

- PIPEDA s. **34.1(1)** An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.
  (2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

23. Evaluation (Back)

It should be noted that evaluating the effectiveness of a service or program should be deemed a use that is consistent with the initial purpose for which the personal information is collected and used. However, the ability to disclose personal and health information for that purpose may be restricted by legislation.

- HIA s.27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:
  (g) for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

- POPA Part 3, Division 1 addresses the ability of a public body to carry out data matching for a number of purposes including research and analysis. Additional sections authorize the collection [s.5], and disclosure [s.13] of personal information to evaluate a common or integrated program or service.

24. Research

- An organization must have the consent of the individual to collect, use, or disclose the individual's personal information for research purposes unless one of the following apply.

- PIPA s. 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:
  (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;
- Similar provisions exist for use [s.17(k),(l)] and disclosure [20(p),(q)] without consent.

- HIA allows for the use of health information for research purposes, and requires a process to be followed. See the HIA Part 5, Division 3.

- POPA Part 3, Division 1 addresses the ability of a public body to carry out data matching for a number of purposes including research and analysis. Additional sections authorize the collection [s.5], and disclosure [s.13] of personal information to evaluate a common or integrated program or service.

- PIPEDA s.7(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
  (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 information is used;
  (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
  (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;

- Privacy Act see Note 14, section 8

Appendix B: Alberta Privacy Legislation Disclosure Matrix

Back

The following legislative provisions are extracts from the various privacy legislations that apply in Alberta. The listed extracts are ones that may be appropriate to the sharing (collection, use, and disclosure) of personal and health information by organizations working in a collaborative manner in the areas of social and health supports. Depending on the circumstances, it is quite possible that more than one provision can be relied on. Disclosure should be viewed as a two-sided process. There must be authority by a receiving organization to collect personal and health information, and there must be authority by the disclosing organization to disclose the information. The matrices outline the authority under the various legislation to collect, followed by the authority to disclose. Unless otherwise stated, these provisions outline circumstances where it may be permissible to disclose information, and there is no requirement to disclose. For this reason, it is important for collaborating organizations to determine what information is required in the course of the collaboration, by whom, and under what authority. With that clearly outlined and understood, they are then in a position to agree that they will disclose the information identified for the circumstances that fall under their collaborative approach.

Note: Organizations working collaboratively that intend to share information need to determine what specific provisions would apply to the circumstances they provide supports or services in. Being clear about the purpose and objectives for the collaboration will assist them to determine what information is required, and the specific authorities that support it being shared.

Listed Legislation:

APPLICABLE PROVINCIAL LEGISLATION

Protection of Privacy Act (POPA)		Back

Collection:

Who (Organization)	Can Collect What Information	Comments
Public Bodies under POPA, (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	No personal information can be collected by a public body unless: • the collection of that information is expressly authorized by an enactment of Alberta or Canada [4(a)],	• This section recognizes the legitimacy of other legislation where that legislation authorizes the collection.
	• that information is collected for the purposes of law enforcement [4(b)], or	• This section recognizes the need for collection of information for law enforcement purposes. Note that law enforcement is defined to include policing, including criminal intelligence operations; a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred; or proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred.
	• that information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program or service. [4(c)].	• This section authorizes the collection of personal information where it is required by an operating program or activity that is put in place by the public body. The head (or delegate) of the public body is generally seen to be the one who would

Who (Organization)	Can Collect What Information	Comments
		authorize such a program or activity. This will include information required to plan, administer, and deliver services under common or integrated programs or services that may include other organizations.

Use:

Who (Organization)	Can Use What Information	Comments
Public Bodies under POPA, (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	A public body may use personal information only • for the purpose for which the information was collected or compiled or for a use consistent with that purpose, 12(1)(a)	• This section recognizes the legitimate use of information, and ties the use to the stated purpose(s). For this reason, the purpose should be well articulated and cover the intentions. Consistent use must be demonstrable. (E.g. evaluating the effectiveness of a service is consistent with the delivery of that service.)
	• if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, 12(1)(b) or	• Individuals can provide consent for a specific use of their information. Use of their information is restricted to the stated purpose(s). Consent may be written. Electronic, or verbal consent is also allowed, subject to certain conditions, and should be recorded.
	• for a purpose for which that information may be disclosed under section 13, 15 or 16. 12(1)(c)	• The listed sections outline when information may be disclosed to a public body. If the disclosure is for an authorized purpose under those sections, the public body is authorized to use that information.
	• A public body may use personal information only to the extent necessary to enable the public	• This section limits the public body to only use the information to the degree required.

Who (Organization)	Can Use What Information	Comments
	body to carry out its purpose in a reasonable manner. 12(4)	

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA, (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	Public body may disclose Personal information only:		Note: "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. 13(4) Note: This section is permissive, not required (unless otherwise noted). The word 'only' means that one or more of the provisions listed must apply before disclosure can occur.
	• for the purpose for which the information was collected or compiled or for a use consistent with that purpose, [13(1)(b)]	• to any person responsible for fulfilling the stated purpose.	• Recognizes the legitimate use of information, and ties the use to the stated purpose(s). Consistent use must be demonstrable. (e.g. evaluating effectiveness of a service is consistent with the delivery of that service.)
	• if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure [13(1)(c)]	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Supports the individual having some control over who can access their information. Generally, the consent form should name an organization rather than an employee within it.
	• for the purpose of complying with an enactment of Alberta or		• References the need to comply, i.e. "must do" with the obligations laid out

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada, [13(1)(d)]	• to any person responsible for or identified within the enactment.	in the enactment, or in accordance with a legislative instrument.
	• for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure, [13(1)(e)]	• to any person responsible for or identified within the enactment.	• Includes both a 'can respond' and 'must respond', depending on the enactment's wording.
	• 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, [13(1)(f)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
	• 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, [13(1)(g)]	• to any employee of the public body as required by their position and duties.	• May apply to staff beyond those delivering the specific program. (e.g. may include staff responsible for administrative support, data analysis, etc.)
	• to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for planning, administering, delivering, managing, monitoring	• to any employee of another public body who is involved in the delivery of a common program or integrated service as required by their position and duties.	• Limited to disclosure between public bodies involved in the administration and other activities related to common or integrated programs or services; it does not limit participation by other organizations under other provisions,

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	or evaluating a common or integrated program or service and for the performance of the duties of the officer, employee or member to whom the information is disclosed, [13(1)(h)]		but would not support disclosure to them unless they are acting on behalf of a public body as 'employees'[1].
	• for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit, [13(1)(k)]	• to any person who requires the information to determine suitability and eligibility.	• Not limited to programs run by public bodies, e.g., when an individual applies for supports by an agency.
	• 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, [13(1)(p)]	• to any public body, or an agency that meets the definition of law enforcement, and related to a law enforcement proceeding underway or likely to take place.	• Authorizes disclosure to a public body that may require it for an investigation and proceeding under an act, as well as to a law enforcement agency. Evidence of a proceeding, including an investigation may be requested.
	• 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, [13(1)(q)]	• to any law enforcement agency in Canada and outside of Canada	• Authorizes disclosure of information between a public body that is deemed law enforcement to other law enforcement agencies.

[1] "employee", in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body; POPA s.1(h).

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	• if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize a risk of harm to the health or safety of a minor, [13(1)(cc)(i)]	• to any person who may be involved in addressing risk of harm to a minor (under the age of 18)	• Organizations using this should be prepared to provide rationale/argument of the potential for harm. There may be a need to provide the public body with information to assist in their decision making.
	• 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, [13(1)(cc)(ii)] Note: POPA Regulation states: For the purposes of the Act, "imminent danger" includes a situation in which the head of a public body believes, on reasonable grounds, that (i) there is a significant risk of harm to the health or safety of a person, and (ii) disclosure of personal information is necessary to protect the health or safety of the person; [1(1)(b)]	• to any person who may be involved in addressing the risk of an imminent danger to any person	• While the bar is somewhat higher, the definition of Imminent harm found in the regulations mirror the definition in the Health Information Act. Where there is imminent danger, action should be enabled early enough to prevent it. The use of a risk assessment tool may be of value. There may also be a need to provide the public body with information you have to assist in their decision making.
	• to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a	• to any organization meeting the criteria that is involved in services to minors, or has implications for the minor, if in the best interests of the minor.	• This somewhat mirrors the *Children First Act*, and authorizes disclosure of information about the minor or their parent or guardian if in the best interests of the minor. There may be a need to provide the public body with

Who (Organization)	Can Disclose What Information	To Whom	Comments
	minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor. [13(1)(dd)]		information to assist in their decision making. Note that there is no prescribed person or body.

Access to Information Act (ATIA) Back

Disclosure

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under ATIA (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	• Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people, to any person or to an applicant (a) information about a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person or of the applicant, or (b) information the disclosure of which is, for any other reason, clearly in the public interest. [37(1)]	To the appropriate member or members of the public, dependent on the circumstances and focus of the risk.	Requires the disclosure of information, (including personal information if appropriate), where there is a risk of significant harm or where the disclosure is in the public interest. It also requires notice be provided in situations where personal information will be disclosed, to the person the information is about, and to the Information and Privacy Commissioner, in advance if practicable.

Health Information Act (HIA)	Back

Collection:

Who (Organization)	Can Collect What Information	Comments
Custodians as identified in the Act and Regulations (Includes those working on their behalf, defined as 'affiliates'.)	Non-identifying health information for any purpose [19]. Individually identifying health information: • if the collection of that information is expressly authorized by an enactment of Alberta or Canada [20(a)], or • if that information relates directly to and is necessary to enable the custodian to carry out a purpose that is authorized under section 27. [20(b)] The individual's personal health number (PHN) may only be required to be provided by: • custodians [21(1)(a)]; • persons authorized by the regulations to do so [21(1)(b)].	• This section outlines there not being any restrictions on the collection of non-identifying health information. • This section recognizes the legitimacy of other legislation where that legislation authorizes the collection. • Section 27 outlines the various purposes for which a custodian may use health information, including the provision of health services. • This section acknowledges that the PHN may be required by custodians and their affiliates. • The HIA Regulations set out which entities have authority to collect the PHN.

Use:

Who (Organization)	Can Use What Information	Comments
Custodians as identified in the Act and Regulations (Includes those working on their behalf, defined as 'affiliates'.)	A custodian may use non-identifying health information for any purpose. [26]	This outlines that a custodian is not bound by any restrictions in how they use information that is not personally identifying. The listed subsections are allowable uses by the custodian that could generally be relied on within the

Who (Organization)	Can Use What Information	Comments
Custodians as identified in the HIA and Regulations	A custodian may use individually identifying health information in its custody or under its control for the following purposes:	context of collaborative/integrated services. Others may also apply in specific situations.
	• providing health services; 27(1)(a)	• Health services as defined in the Act.
	• determining or verifying the eligibility of an individual to receive a health service; 27(1)(b)	• Information that may be required in the assessment of what health services are required.
	• conducting research or performing data matching or other services to facilitate another person's research *(under a set of conditions that must be met)* 27(1)(d)	• Information that may be used for research or data-matching by the custodian, where the outputs are required by another person (not necessarily a custodian) in research they are managing.
	• carrying out any purpose authorized by an enactment of Alberta or Canada; 27(1)(f)	• Where the purpose is authorized by other legislation, provincial or federal.
	• for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management. 27(1)(g)	• Where necessary for administrative purposes as outlined.
	An affiliate of a custodian must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian. 28	This section restricts the affiliate to only use information to carry out their responsibilities outlined by the custodian.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the Act and Regulations (Includes those working on their behalf, defined as 'affiliates'.)	Health information may be disclosed in the following circumstances:		The HIA requires that any collection, use and disclosure "be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances". 2(c)
	• 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. [34(1)]	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Consent must be in writing and meet HIA requirements.
	Disclosure without consent:	• 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 (with some exceptions). [42(1)]	• Exceptions include disclosures to another custodian (s.35(1)(a),s.47), to a police service or Justice Minister (s.37.1,37.2, or 37.3).
	• to another custodian for any or all of the purposes listed in section 27(1) or (2), as the case may be, [35(1)(a)]	• to another custodian	• For the purposes outlined in s.27, which focus primarily (but not exclusively) on providing health care
	• to a person who is responsible for providing continuing treatment	• to any person responsible for providing continuing treatment and care.	• Not limited to health care providers, so applies to entities outside of the formal health system. E.g., schools,

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the HIA and Regulations	and care to the individual, [35(1)(b)]		social workers, support agencies. Providing the custodian with information to assist in their decision may be necessary.
	• 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, [35(1)(i)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
	• to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize a risk of harm to the health or safety of a minor, [35(1)(m)(i)]	• to any person who may be involved in addressing risk of harm to a minor (under the age of 18)	• Organizations using this should be prepared to provide rationale/ argument of the potential for harm. Providing the custodian with information to assist in their decision may be necessary.
	• to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize a significant risk of harm to the health or safety of any person, [35(1)(m)(ii)]	• to any person who may be involved in addressing the risk of significant harm to any person	• While the bar is somewhat higher, where there is a significant risk, action should be enabled. The use of a risk assessment tool may be of value. Providing the custodian with information to assist in their decision may be necessary.
	• if that individual lacks the mental capacity to provide a consent and, in the opinion of the custodian, disclosure is in the best	• to any person who can address the issue who requires the information	• Requires the custodian to determine the lack of mental capacity, and that the disclosure is in the best interests, which while not defined, allows for the

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the HIA and Regulations	interests of the individual, [35(1)(n)]	and acts in the best interests of the individual	custodian to make determination based on the individual and the circumstances. Providing the custodian with information to assist in their decision may be necessary.
	• if the disclosure is authorized or required by an enactment of Alberta or Canada, [35(1)(p)]	• to any person responsible for or identified within the enactment.	• Includes both a 'can respond' and 'must respond', depending on the enactment's wording.
	• 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 Solicitor 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. [37.3(1)]	• To a police service or the Minister of Justice and Solicitor General	• Authorizes disclosure of demographic and other to police services where there is potential for risk to the health and safety of an individual or group of Albertans, through the possible commission of an offence. There may be situations where the potential offence needs to be identified to assist in the decision making.

Personal Information Protection Act (PIPA)	Back

Collection:

Who (Organization)	Can Collect What Information	Comments
Private and non-profit organizations *(The act does not apply to non-profit organizations (as stated) but does apply to personal information they manage in connection to commercial activities.)*	• An organization may collect personal information only for purposes that are reasonable [11(1)]. • 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 [11(2)].	• This section applies the standard for reasonableness as defined in section 2, that is, what a reasonable person would consider appropriate in the circumstances. • This section outlines that there must be a reasonable connection between the information collected, and the purpose for which it is collected.

Use:

Who (Organization)	Can Use What Information	Comments
Private and non-profit organizations *(The act does not apply to non-profit organizations [as defined] but does apply to personal information they manage in connection to commercial activities.)*	An organization may use personal information only for purposes that are reasonable. 16(1) 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. [16(2)] 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 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	The test for 'reasonable' is what a reasonable person would consider appropriate in the circumstances. There must be other conditions present, including notice, etc.. The following listed subsections are allowable uses by the organization that could generally be relied on within the context of collaborative/integrated services. Others may also apply in specific situations. • This addresses situations where consent cannot be obtained but would not likely have been withheld, and will be used in the interests of the individual.

Who (Organization)	Can Use What Information	Comments
Private and non-profit organizations	individual would not reasonably be expected to withhold consent; [17 (a)]	
	• the use of the information is authorized or required by (i) a statute of Alberta or of Canada, (ii) a regulation of Alberta or a regulation of Canada, (iii) a bylaw of a local government body, or (iv) a legislative instrument of a professional regulatory organization; [17 (b)]	• These sections outline the authority for the organization to use information in accordance with one of the listed legal requirements.
	• 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; [17 (c)]	• This section outlines the authority for the organization to use information in accordance with one of the listed legal requirements.
	• the use of the information is reasonable for the purposes of an investigation or a legal proceeding; [17 (d)]	• This section outlines the authority for the organization to use information as stated.
	• the information may be disclosed by an organization without the consent of the individual under section 20; [17 (h)]	• This section outlines the authority for the organization to use information that is disclosed to it under section 20. (see Disclosure, below)
	• 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; [17 (i)]	• This section outlines the authority for the organization to use information where necessary to address situations that may pose a risk to another person or persons.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Private and non-profit organizations *(The act does not apply to non-profit organizations [as defined] but does apply to personal information they manage in connection to commercial activities.)*	Personal information of an individual • can be collected, used and disclosed with the consent of the individual, [7(1)] or	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Consent may be provided in writing or orally (and documented), and should be informed.
	• by giving an appropriate notice and a reasonable amount of time for the individual to respond [8(3)].	• to any person or staff of an organization identified in the notice responsible for the purposes stated therein.	• Requires determination that the disclosure be reasonable, also taking into consideration the sensitivity of the information.
	Personal information about an individual may be disclosed without consent when: • 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; [20(a)]	• to any person who can address the issue who requires the information and acts in the best interests of the individual	• Requires the organization holding the information to determine the disclosure to be in the person's best interests. While not defined, it allows the organization to make determination based on the individual and the circumstances. There may be a need to provide the organization with information to assist in their decision making.
	• the disclosure of the information is authorized or required by (i) a statute of Alberta or of Canada,	• to any person responsible for or identified within the enactment, or legislative instrument.	• Includes both a 'can respond' and 'must respond', depending on the enactment's wording.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Private and non-profit organizations	(ii) a regulation of Alberta or a regulation of Canada, (iii) a bylaw of a local government body, or (iv) a legislative instrument of a professional regulatory organization; [20(b)]		
	• 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; [20(c)]	• to any staff or official in the public body with responsibility under the enactment.	• Authorizes a public body to collect the information they may require to deliver its programs and services.
	• 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; [20(e)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
	• 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; [20(f)]	• to any public body, or an agency that meets the definition of law enforcement, and related to a law enforcement proceeding underway or likely to take place.	• Authorizes disclosure to a public body that may require it for an investigation and proceeding under an act, as well as to a law enforcement agency. Evidence of a proceeding, including an investigation may be requested.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Private and non-profit organizations	• 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; [20(g)]	• to any person who may be involved in responding to the emergency	• Organizations or persons requesting or undertaking disclosure should be prepared to provide rationale/evidence of the potential emergency. There may be a need to provide the organization deciding on disclosure additional information to assist in their decision making.
Non-profit organizations who are not subject to legislation can be 'pulled' under legislation. For example, if they are acting on behalf of a Public Body or a Custodian they are then deemed to be an employee or affiliate for the purposes of fulfilling their duties. They can also demonstrate accountability by means of agreements entered into with their partner organizations.			

Children First Act Back

Collection and Use:

Who (Organization)	Can Collect and Use What Information	Comments
Defined Service Providers (Government Departments, educational bodies (schools and charter schools – as defined in POPA), Police Service (as defined in *Police Act*), agencies providing services to a child under an agreement with a public body)	For the purposes of enabling or planning for the provision of services or benefits to a child, a service provider may collect and use either or both of the following:	
	• personal information about the child or a parent or guardian of the child from another service provider [4(1)(a)];	• This section authorizes the collection and use of personal information about a child or a parent or a guardian of the child if it is required for enabling or planning for the provision of services to the child.
	• health information about the child from a custodian [4(1)(b)].	• This section authorizes the collection and use of health information about a child if it is required for enabling or planning for the provision of services to the child.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Defined Service Providers (Government Departments, educational bodies (schools and charter schools – as defined in POPA), Police Service (as defined in *Police Act*), agencies providing services to a child under an agreement with a public body)	**Personal information of a child or of their parent/guardian** that: • is necessary for enabling or planning services or benefits to a child, if the disclosing service provider determines it is in the best interests of the child [4(2)(a)]	• another service provider	This act only applies to children under 18. • Authorizes the disclosure of personal information if the service provider holding the information determines that it is in the best interests of the child to do so, and only to another service provider. It may be necessary to provide the service provider deciding on disclosure additional information, to assist in their decision making.
Defined Service Providers	**Personal information of a child** that: • in the opinion of the service provider is in best interests of the child, and not contrary to the express request of the child [4(3)(a, b)]	• to the parent or guardian	• Authorizes disclosure to the child's parent or guardian only if it is not contrary to the request of the child.
Custodians as defined under the HIA	**Health information of a child** that: • is necessary for enabling or planning services or benefits to a child, if the disclosing custodian determines it is in the best interests of the child. [4(3)(a,b)]	• a service provider or another custodian	• Only authorizes disclosure of the child's health information, and if the custodian holding the information deems it in the best interests of the child to disclose it. It may be necessary to provide the custodian deciding on disclosure additional information, to assist in their decision making.

Canadian Centre Of Recovery Excellence Act	Back

Outlines the authority for the Centre of Recovery Excellence (CORE), a crown corporation in the Government of Alberta for the collection, use, and disclosure of personal and health information (PHI) for the purposes outlined. The collection, use, and disclosure, (as outlined in section 13 of the Act) may be in aggregate form, non-identifying if aggregate is not adequate, and identifying only if necessary for its stated mandate. Both the mandate and activities are outlined in section 3.
The mandate is to support an improved approach to mental health and addiction issues by:
• conducting and supporting research, evaluations and innovations related to mental health and addiction issues,
• providing advice, information, reports and the results of research and evaluations to the Minister …, and
• supporting the provision of services to individuals in Alberta with mental health and addiction issues, and providing provincial, national and international leadership on
  ○ addressing mental health and addiction issues, and
  ○ recovery-oriented systems for providing services to individuals with mental health and addiction issues. [3(1)]
	This Act has provided the Centre with significant authority to collect, use, and disclose personal and health information in order to achieve its mandate.

The Centre shall collect, use or disclose • aggregate information if it is adequate for the intended purpose, and • non-identifying health information and non-identifying personal information if it is adequate for the intended purpose and the collection, use or disclosure of aggregate information is inadequate for the intended purpose, • and may only collect, use or disclose personal information and individually identifying health information when necessary for purposes that the Centre is authorized, under this or any other enactment, to collect, use or disclose that information for. [13(3)]	This requires the Centre to collect information in an aggregate form, or in a non-identifying manner if aggregate is not sufficient for the purposes, or in an identifying form if neither aggregate or non-identifying is not sufficient.
The Centre may collect, directly or indirectly, use and disclose information, including personal information and individually identifying health information, for the purposes of fulfilling the Centre's mandate, undertaking the Centre's activities, exercising the Centre's powers and performing the Centre's duties and functions under this Act, and for any other purposes prescribed in the regulations. [13(4)]	This section broadly outlines the authority of the Centre.
Personal and health information may be collected from any of the following: • custodian as defined in the Health Information Act,	Note that at this time Regulations have not been enacted, which limits the Centre

• Minister or department, • public body prescribed in the regulations, • public agency prescribed in the regulations, • organization prescribed in the regulations, • mental health and addiction service provider prescribed in the regulations, or • other persons or entities prescribed in the regulations [13(5)] Personal information and individually identifying health information may be disclosed under this section without the consent of the individual who is the subject of the information. [13(7)]	to the information held by the first two types of entities. This outlines the authority of the Centre to collect the information they require without the consent of the individuals to whom it pertains.

Emergency Health Services Act Back

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Ambulance attendants (as defined in the Ground Ambulance Regulations)	• Notwithstanding the Health Information Act, for the purposes of an investigation by a peace officer, an ambulance attendant may disclose the information described in subsection (2) that the ambulance attendant observed or collected when dispatched to and attending the scene of an incident to the peace officer without the consent of the patient or other individual who is the subject of that information. [40.1(1)]	• to a peace officer conducting an investigation	• Authorizes the disclosure of some demographic information of a patient or other individual, and including information and observations regarding the scene of the accident, as outlined.

APPLICABLE FEDERAL LEGISLATION

Privacy Act	Back

Collection:

Who (Organization)	Can Collect What Information	Comments
Federal institutions (E.g. RCMP and Health Canada)	No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution. [4]	• This section authorizes the collection of personal information only if it required for the purposes of an operating program or activity of the institution collecting it.

Use under the federal Privacy Act:

Who (Organization)	Can Use What Information	Comments
Federal institutions (E.g. RCMP and Health Canada)	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 • for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; [7(a)] or • for a purpose for which the information may be disclosed to the institution under subsection 8(2) [7(b)].	• This provision outlines that the consent of the individual to whom the information pertains is required for any use of their information with the following exceptions: • This allows the institution to use the information they have collected for the purpose(s) for which it was collected, • This allows the institution to use the information they have collected for the purpose(s) for which it was disclosed to them.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federal institutions (E.g. RCMP and Health Canada)	**Personal information** of the individual: • with the consent of the individual [8(1)]	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Supports the individual having some control over who can access their information. Generally, a consent form used by an organization should name an organization rather than an employee within it.
	• for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose [8(2)(a)]	• to any person responsible for fulfilling the stated purpose.	• Recognizes the legitimate use of information, and ties the use to the stated purpose(s). Consistent use must be demonstrable. (e.g. evaluating effectiveness of a service is consistent with the delivery of that service.)
	• for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure; [8(2)(b)]	• to any person responsible for fulfilling the purpose identified within the enactment	• Authorizes the disclosure of information as authorized under another act or regulation of Canada.
	• 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 [8(2)(c)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federal institutions	• 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 [8(2)(e)]	• to the investigative bodies specified in the regulations (includes the RCMP)	• Supports a request made by law enforcement bodies such as the RCMP
	• for any purpose where in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure [8(2)(m)(i)]	• anyone who requires it to address the matter that is in the public interest	• Authorizes the disclosure of personal information where the disclosure is in the public interest. Public interest is not defined, allowing the institution to make a determination based on the circumstances, and may include health and safety reasons. There may be a need to provide the organization with information to assist in their decision making.
	• for any purpose where in the opinion of the head of the institution, would clearly benefit the individual to whom the information relates [8(2)(m)(ii)]	• anyone who requires it to address the matter that would benefit the individual	• Authorizes the disclosure of personal information where the disclosure is to the person's benefit. The 'person's benefit' is not defined, allowing the institution to make a determination based on the individual and their circumstances. There may be a need to provide the organization with information to assist in their decision making.

Personal Information Protection and Electronic Documents Act (PIPEDA)	Back

Collection:

Who (Organization)	Can Collect What Information	Comments
Federally Regulated Organizations and Private Sector Organizations that collect, use, or disclose personal information in the course of a commercial activity.	An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.	• This section applies the test for reasonableness as defined in section 3, that is, what a reasonable person would consider appropriate in the circumstances.

Use under the Personal Information and Protection of Privacy Act:

Who (Organization)	Can Use What Information	Comments
Federally Regulated Organizations and Private Sector Organizations that collect, use, or disclose personal information in the course of a commercial activity.	Personal Information of the individual may be used • with the consent of the individual, [Principle 3, clause 4.3 of Schedule 1] Personal Information of the individual may be used by an organization without the knowledge or consent of the individual, use personal information only if • 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	Note that section 6.1 states: "For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." The provisions listed here allow for the organization to use personal information without the consent of the individual to whom it pertains. • Allows the organization to use information for the purpose(s) of investigating any contravention of laws. This would likely be deemed to be limited to the use by that organization if it fits within their mandate or role.

Who (Organization)	Can Use What Information	Comments
Federally Regulated Organizations and Private Sector Organizations	committed, and the information is used for the purpose of investigating that contravention; [7(2)(a)] • it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual; [7(2)(b)] • it was collected under paragraph (1)(a), (b) or (e). [7(2)(d)]	• Allows the organization to use information to address any situations where there is a potential or active risk to the health or safety. • Allows the organization to use the information where: ○ it is in the best interests of the individual, ○ it is necessary for purposes of investigating a breach of an agreement, or a contravention of the laws of Canada or a province, or ○ it is required by law.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations that collect, use, or disclose personal information in the course of a commercial activity. Note that private sector organizations in Alberta are subject to PIPA, unless the information crosses borders in the	**Personal Information** of the individual • With the consent of the individual, [Principle 3, clause 4.3 of Schedule 1] **Personal Information** of the individual without the consent of the individual when:	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Note that section 6.1 states: "For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

Who (Organization)	Can Disclose What Information	To Whom	Comments
course of commercial activities. (E.g., personal information collected by a private sector organization in Alberta is processed in another jurisdiction such as credit card payments.)	• 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; [7(3)(c)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
	• 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 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, [7(3)(c.1)(ii)]	• to any government institution or part thereof and related to law enforcement, or carrying out an investigation related to law enforcement, of Canada or a province.	• "Government Institution" is not defined in PIPEDA, but given that this section applies to provincial legislation as well, an argument can be made that provincial government departments could make the request.
	• 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 the disclosure is requested for the purpose of	• to any government institution or part thereof and related to administering a legislation of Canada or a province.	• "Government Institution" is not defined in PIPEDA, but given that this section applies to provincial legislation as well, an argument can be made that provincial government departments could make the request. This would not be tied in with law enforcement per se, but rather where

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	administering any law of Canada or a province, [7(3)(c.1)(iii)]		legislation authorizes the collection of information for various purposes.
	• 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 the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual; [7(3)(c.1)(iv)]	• to any government institution or part thereof and related to administering a legislation of Canada or a province.	• "Government Institution" is not defined in PIPEDA, but given that this section applies to provincial legislation as well, an argument can be made that provincial government departments could make the request. The legislation cited should include the authority to disclose information to a next of kin or authorized representative for the outlined purposes. (E.g., HIA s. 35(1)(d)).
	• made on the initiative of the organization to a government institution or a part of a government institution and the organization has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed [7(3)(d)(i)]	• to any government institution or part thereof and related to a potential or current contravention of a law (legislation).	• The institution would presumably need the authority to collect such information, including having the legislative responsibility to deal with the contravention.
	• made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province	• to any organization that has the capacity and mandate to investigate a breach of an agreement or contravention	• Opens disclosure to a broader group of organizations beyond government institutions. They should still be required to demonstrate their

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation; [7(3)(d.1)]	of the laws of Canada or a province.	authority to collect and use such information.
	• made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud; [7(3)(d.2)]	• to any organization that has the capacity and mandate to investigate or prevent fraud.	• Opens disclosure to a broader group of organizations beyond government institutions. They should still be required to demonstrate their authority to collect and use such information for the specific purposes outlined.
	• made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse, the disclosure is made solely for purposes related to preventing or investigating the abuse, and it is reasonable to expect that	• to any government institution or to the individual's next of kin, or the individual's authorized representative, where they have the capacity and mandate to investigate or deal with financial abuse.	• Opens disclosure to a broader group of organizations beyond government institutions. They should still be required to demonstrate their authority to collect and use such information for the specific purposes outlined.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse; [7(3)(d.3)]		
	• necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure; [7(3)(d.4)]	• to any government institution or to the individual's next of kin, or the individual's authorized representative, where they have the capacity to identify the individual.	• Organizations or persons should be prepared to provide evidence of their authority. The individual whose information is being disclosed should be notified about the disclosure, if they are alive.
	• 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; [7(3)(e)]	• to any person who may be involved in responding to the emergency	• Organizations or persons requesting or undertaking disclosure should be prepared to provide rationale/evidence of the potential emergency. There may be a need to provide the organization deciding on disclosure additional information to assist in their decision making. The individual whose information is being disclosed should be notified in writing about the disclosure, though dependent on the circumstances that could occur simultaneously or as soon after the disclosure occurs as is practicable.

Beyond the above, information may need to be collected from other sources, including parents, friends, classmates, etc. While they may not be subject to any legislation that prescribes their authority to disclose information, there should be authority for it to be collected, and they should be advised as to that authority.

The interpretations listed in this document are not to be construed as legal advice. While they are based on information gained from a variety of Government and Privacy Commissioner sources, it is up to the organizations applying the legislation to determine if they require legal advice in their application.

Prepared by: George Alvarez
on behalf of Converge Mental Health Coalition

Appendix C: Disclosure Tool (Alberta)

Back

The following tool is meant to broadly identify what type of organization (based on applicable privacy legislation) can disclose what type of information to whom, under what types of circumstances. It is meant to be broad, to provide a sense of how organizations working in a collaborative manner across sectors can share (collect, use, and disclose) the information necessary in that work.

Use of the Tool:

1. If disclosure is authorized through informed consent of the individual, ensure that the information being disclosed is as stated for the purpose(s) as stated in the consent, and disclosure is to an organization identified in the consent.
2. If the disclosure is not authorized through consent, apply the tool as follows.
3. In the "Authority to Disclose" table, find the legislation that applies to your organization.
4. Determine if any of the legislative provisions (sections) listed apply to the situation you are working in. The provisions are abbreviated so if not familiar with the actual provision, you should review the actual wording to ensure it fits with the situation outlined.
5. In the "To Whom Can I Disclose" table, under the column on the left-hand side titled *"Why Am I Disclosing*, identify the circumstances that apply to your situation.
6. Move across from that circumstance and determine if one of the provisions listed under the heading *"Authority to Disclose"* apply, and identify whether the type of organization to whom you are disclosing is listed under that provision. Note that the provisions are listed across the top and bottom halves of the table.
7. In the "What Information Can I Disclose for What Purpose" table, identify the type of service is being provided by the organization or area you are determining disclosing to, and the type of collaboration occurring (as per the roles and responsibilities of the member organizations involved in the collaborative approach).
8. Move across from the type of service/collaboration and identify the type of information that can be disclosed. Note that the information types are generally relevant to the type of service, but the actual details of the service and the needs of the provider in order to deliver that service should be guiding the details of the disclosure. **Disclosure is to be limited to what is required to provide that service.**

Questions on the applicability of any of the above should be reviewed with your privacy or legal supports.

Authority to Disclose									
Identify what legislation applies to you.									
(A)	I am subject to privacy legislation: PO - POPA / H - HIA / P - PIPA / PE - PIPEDA / PA - Privacy Act / C - CFA / N - None								
Identify if one of the listed authorities to disclose applies.									
(B)	Authority to Disclose Under								
POPA/ATIA		**HIA**		**PIPA**		**Privacy Act**		**PIPEDA**	
13(1)(c)	With consent	34(1)	With consent	7(1)/ 8(3)	With consent	8(1)	With consent	Sched.1; 4.3	With consent
13(1)(b)	For Stated or consistent purpose	35(1)(a)	For purposes listed in s.27	20(b)	To comply with legislation	8(2)(a)	For Stated or consistent purpose		
13(1)(d)	Comply with enactment							7(3)(c.1)(ii)	For purpose of enforcing any law of Canada or a province
13(1)(e)	In accordance with enactment	35(1)(p)	In accordance with enactment	20(b)	In accordance with statute, …	8(2)(b)	In accordance with Act of Parliament	7(3)(c.1)(ii)	For purpose of administering any law of Canada or a province
13(1)(f)	Comply with subpoena	35(1)(i)	Comply with subpoena …	20(e)	Comply with subpoena	8(2)(c)	To comply with subpoena	7(3)(c)	To comply with subpoena
13(1)(g)	To public body staff who require it			20(c)	To authorized public body				
13(1)(h)	Common/ integrated program/service								
13(1)(k)	Suitability/eligibility for program/benefit								
		35(1)(a)	Determine eligibility for a health service						
POPA/ATIA		**HIA**		**PIPA**		**Privacy Act**		**PIPEDA**	
13(1)(p)	To Law Enforcement for investigation			20(f)	To Law Enforcement for investigation	8(2)(e)	To investigative body to enforce a law or investigate	7(3)(d.1,2)	Where reasonable to investigate an offence and consent might compromise
13(1)(q)	From law Enforcement to law Enforcement								
13(1)(cc)(i	Avert risk of harm to a minor	35(1)(m)(i)	Avert risk of harm to a minor	20(g)	Respond to an emergency that threatens life, health & security	8(2)(m(i)	For any purpose where the public interest in disclosure clearly outweighs any invasion of privacy	7(3)(e)	Where needed due to threat to health & safety of individual, who will be informed in writing w/out delay
13(1)(cc)(ii)	Avert imminent harm to anyone	35(1)(m)(ii)	Avert significant risk of harm						
ATIA 37(1	Avert risk to public health & safety								
13(1)(ee)	Best interest of a minor	35(1)(p)	Best interest of a minor (in conjunction with CFA)	20(b)	Best interest of a minor (if agency identified in CFA)	8(2)(m)(ii)	For any purpose where it would clearly benefit the individual		
		35(1)(b)	Person responsible for continuing treatment and care						
		35(1)(n)	Best interest of person lacking capacity to consent						
		37.3(1)	If related to an offence and will protect health and safety					7(3)(d)(i)	Where the information relates to the possible commission or intent to commit an offence
				20(a)	Best interest of person who cannot consent in timely way				
POPA/ATIA		**HIA**		**PIPA**		**Privacy Act**		**PIPEDA**	

NOTE: In addition to the above legislation, the Children First Act authorizes the disclosure of personal information of a minor or of their parents by Government of Alberta departments, School Authorities, Police Services, and agencies providing ervices on behalf of public bodies; and health information of a minor by HIA Custodians for enaling/planning services in the best interest of the minor child.

	To Whom Can I Disclose								
	I am subject to privacy legislation: PO-POPA / H-HIA / P-PIPA / PE-PIPEDA / PA-Privacy Act / C-CFA / N-None								
	Authority to Disclose								
	PO,H,PA	PO,P,PA,N	PO,H,P	PO,H,P,PA,N	PO	PO	PO	H,C	PO,PA
	For Stated Purpose	**Complying with legislation**	**Accordance with legislation**	**Complying with subpoena…**	**To public body**	**Common/ integrated program or service**	**Suitability/eligibility for program**	**Determine eligibility for health service**	**To Law Enforcement for investigation**
Why am I disclosing?	I may disclose to: **P-Public Body** / **C-Custodian** / **PS-Private Sector** / **I-Federal Institution** / **NP-Non Profit**								
Support to person in need in community	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Supports for youth homelessness	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Supports for adult homelessness	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Service to a youth in crisis	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Service to an adult in crisis	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Assist domestic abuse victim	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Suicide Prevention	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Risk of harm to self	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Risk of harm to minor	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I
Risk of harm to adult	P,C,I	P,C,I	P,C,I	P,I	P,PS	P	P,C,PS,I,NP	C	P,I

	I am subject to privacy legislation: PO-POPA / H-HIA / P-PIPA / PE-PIPEDA / PA-Privacy Act / C-CFA / N-None								
	Authority to Disclose								
	PO	ALL	PO,H,P,PA,N	ALL	PO,PA	H	H,PA	H,P	P,PA
	From law Enfrcmt to law Enfrcmt	**Avert risk of harm to a minor**	**Avert imminent harm to anyone**	**Best interest of a minor****	**Avert risk to public health & safety**	**To person responsible for treatment and care**	**Best interest of person lacking capacity**	**Assist investigation related to an offence**	**Best interest of person who cannot timely consent**
Why am I disclosing?	I may disclose to: **P-Public Body** / **C-Custodian** / **PS-Private Sector** / **I-Federal Institution** / **NP-Non Profit**								
Support to person in need in community	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Supports for youth homelessness	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Supports for adult homelessness	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Service to a youth in crisis	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Service to an adult in crisis	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Assist domestic abuse victim	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Suicide Prevention	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Risk of harm to self	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Risk of harm to minor	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP
Risk of harm to adult	P,I	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,C,PS,I,NP	P,I	P,C,PS,I,NP

Note: In addition to the above authorities, all legislation listed includes authority to disclose with consent to any person or organization, which can apply in all the situations listed.

What Information Can I Disclose for What Purpose?										
	What am I disclosing:	Name	Contact Info	Identify Needs	Needs Assmnt	In Depth Assmnt	Health Info	Financial Info	Safety Info	Case Mgmt
For What Purpose Am I Disclosing										
Type of Service	Type of Collaboration	Type of Information								
All Services	Referral	?								
Support to person in need in community	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x				x	
	Collaborative support	x	x	x	x	x			x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Supports for youth homelessness	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x		x	x	x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Supports for adult homelessness	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x		x	x	x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Service to a youth in crisis	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x				x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Service to an adult in crisis	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x				x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Service to assist domestic abuse victim	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x				x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Suicide Prevention	Warm handoff	x	x	x						
	Coordinated support	x	x	x	x		x		x	1
	Collaborative support	x	x	x	x	x	x		x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Risk of harm to self	Warm handoff	x	x	x	x				x	
	Coordinated support	x	x	x	x	x	x		x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Risk of harm to minor	Warm handoff	x	x	x	x				x	
	Coordinated support	x	x	x	x		x		x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
Risk of harm to adult	Warm handoff	x	x	x	x				x	
	Coordinated support	x	x	x	x		x		x	1
	Collaborative support	x	x	x	x	x	x	x	x	2
	Integrated support	x	x	x	x	x	x	x	x	3
		Name	Contact Info	Identify Needs	Needs Assmnt	In Depth Assmnt	Health Info	Financial Info	Safety Info	Case Mgmt
Case Management Plan Levels										

1 Basic: no true dependencies but relationship of needs may exist

2 Collaborative: some dependencies may exist, requires some increased level of information sharing

3 Comprehensive/integrated: relationships and dependencies exist, requiring organizations to regularly update each

Appendix D: Sample Collaborative Approach Training Resource

Back

Using this Resource: *Staff should be orientated to and understand the material contained in this resource. The member organizations should ensure that the material fits the manner in which they will be working, and where necessary made the necessary adjustments or enhancements. The following sections require additional information to be provided by the member organizations. (Sections 1.1, 1.2, 1.4, 1.5, 1.6, 3.1, 4.1, 5.1, 5.3, 6.3, 8.4, 8.5, 8.8, 8.10)*

Purpose

Staff must understand the Purpose, Outcomes, and Objectives of the collaborative or integrated service delivery approach, and be able to explain it to the individuals they work with in a manner they would understand. There may be a benefit to having documents that outline the purpose and the partner organizations involved, to provide to staff and the individuals they support.

Policy

The policies and practices outlined here and in accompanying documents have been developed and accepted to support a consistent approach to managing the information of the individuals being served under the *<Identify the name of the Collaborative Approach>*. All staff users of the collaborative approach should ensure they have familiarized themselves with all policies and practices. For additional information, see the Information Sharing Framework.

Legislation

Do staff know what, if any, legislation they are subject to?

In order for the collaborative approach members to work effectively together in support of individuals and families experiencing mental health issues or concerns, they need to share (collect, use, and disclose) the personal and health information of their clients. Member organizations therefore need to understand what privacy or other legislation they may be subject to, and what authority exists for them to collect, use, and disclose, the personal and health information of the individuals they support and provide services to. While privacy legislation in Alberta is not harmonized, there are sufficient provisions that when considered collectively, do enable the partnering organizations to work together and share the information they need.

Privacy legislation is intended to ensure the access to, and use of, personal and health information is appropriate and authorized. Such information is by definition sensitive, regardless of whether the individual to whom it pertains thinks of it in that way, and the legislation sets out minimum expectations on how it must be managed. The legislation is also intended to, as much as is possible, put the control of the information in the hands of the individual to whom it pertains. Privacy legislation addresses a number of areas relative to the management of this information, including:

- What information it pertains to (e.g., personal information, health information)
- Who is subject to the legislation (e.g., government organizations, health service providers, non-government organizations)
- What authority exists to collect, use, and disclose the information (e.g., legislated, with consent, for specific purposes)
- How the information should be managed (i.e., in a secure manner, conducting Privacy Impact Assessments)

- What oversight exists (e.g., Office of the Information and Privacy Commissioner, Privacy Breach Reporting)

Staff involved in the collaborative approach should also be somewhat familiar with the legislation that applies to their partner organizations, and recognize that there may be different provisions, expectations, and restrictions, on the collection, use, and disclosure, of personal and health information.

For more information see "*Appendix B: Privacy Legislation Disclosure Matrix"*, and the specified legislation.

Non-Profit Organizations

It must also be recognized that while non-profit agencies, who often make up a significant percentage of the partners providing collaborative social and health supports, may not be subject to privacy legislation, they can nevertheless participate in these partnerships. In order to do so, the participating non-profits commit to following the minimum level of requirements as supported through legislation. By entering into this partnership, all member organizations agree that by working collectively, they are working on behalf of each other, in order to achieve the identified purposes and outcomes.

Contracted and Other Service Relationships

When an individual or agency works on behalf of another organization, they are deemed to be an extension of that organization. Privacy legislation defines or identifies that a person or entity who acts on behalf of an organization (public body, institution, custodian) as also being subject to the legislation (as an employee, agent, affiliate). In those situations, the rules around the collection, use, and disclosure, that apply to the organization would also apply to the entity acting on their behalf. However, the contracts or agreements they enter into often narrow the uses of information to that which is required for the agency to conduct the work they are contracted to perform, and other uses may be restricted or require permission.

This is important from a couple of perspectives:

First, the authority provided by the legislation, along with the inherent responsibilities, is extended to the agency, thereby providing a (potentially different) legislative umbrella to protect the information.

Second, if the contracted entity becomes part of a collaborative, they may find that they require the permission of the contract holder to use the information they are managing under the contract or agreement for the purpose of the collaborative.

The relationships are recognized by legislation as follows:

Legislation	Provision
POPA	"Employee", in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body.
HIA	"Affiliate", in relation to a custodian, means (i) an individual employed by the custodian,

	(ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian, amongst others (see HIA section 1(1)(a)).
PIPA	"Employee" means an individual employed by an organization and includes an individual who performs a service for or in relation to or in connection with an organization (i) as a partner or a director, officer or other office holder of the organization, (i.1) as an apprentice, volunteer, participant or student, or (ii) under a contract or an agency relationship with the organization.

Privacy Training

There are different training courses or modules available for organizations. If necessary, consideration should be given to the development and provision of custom sessions.

Health and Safety

Working with individuals who present with potential health and safety issues should be recognized, and staff should be oriented to a number of areas, if applicable, including:

- Messaging: Ensuring that part of the messaging to individuals being supported is that the collaborative approach member organizations are working together in part to ensure that the services are being provided within a healthy, safe environment, and should there be risks to health and safety that emerge they will be addressed, which may require the sharing of personal and health information as deemed necessary (notwithstanding consent);
- Risk Identification: Individuals being supported may themselves identify safety issues, or staff working with them may be able to determine at-risk situations or risky behaviours. Member organizations should ensure their staff are trained on what to look for, or where to find resources and supports.
- Response: Staff should be trained on how to respond to at-risk situations, whether they are expected to deal with such situations, or that they know what resources might exist both internal and external to the collaborative;

Roles

Staff working as part of the collaborative approach may find that their roles have shifted somewhat from the role they normally fulfill within their own organization. Defined roles should be clearly laid out, and staff should be trained on their individual areas of responsibility.

In addition, as organizations start to work more effectively together through the implementation of collaborative and integrated service delivery approaches, their staff become part of a larger 'team', and may find that they have to rely on or be relied upon in somewhat different ways. In a sense, they may find that they act as the 'eyes and ears' for one of their partners or colleagues, or vice versa.

Policy/Practice

Policy development and implementation are only useful if staff are trained and have them available for reference. Partners being onboarded should commit to completion of training, and to ensure they familiarize themselves with related implications.

The following table sets out areas that staff should be knowledgeable of and which they put into practice.

What Staff Need to Know

Area	Item	Notes
1. Collaborative/Integrated Service Delivery		
1.1 Purpose	The purpose for or reason the member organizations to be working together.	No single organization can typically meet all the needs a homeless individual has to deal with. Member Organizations are working in a collaborative or integrated manner to *<state the specific purpose here>*. Staff need to both understand the reasons why the member organizations are working together, and be able to explain it to the individuals they work with in a manner they understand.
1.2 Objectives/Goals / Outcomes *<List the anticipated or desired objectives etc.>*	Objectives: Goals: Outcomes:	E.g., Individuals are able to receive the necessary services without having to repeat themselves. Agencies are more effective in their resource utilization, Agencies refer individuals more accurately and efficiently. Waiting times are reduced for individuals accessing the service, Individuals access services and move forward more efficiently, Escalation of risk situations has been reduced.
1.3 Members	Core Members Extended Members Ad Hoc/Other Organizations	Core members are those who are part of the main team, and have access to the shared information if they are involved with the individual, including assessment, determining eligibility, and providing the service. Extended members are ones we may refer the individual to that are somewhat outside of the collaborative approach. They would only have access to information with consent. Ad hoc or other members may be brought in for example, if they have a particular area of expertise, and would have access to the information they need to provide that service. An example may include specialized counselling.

Area	Item	Notes
1.4 Roles	Staff	Specific role the staff plays. E.g., Initial contact, scheduling/referring/ streaming, initial identification of needs, in-depth assessment, counselling, assistance with < >,
	Other members	The roles that other staff the individual may come into contact with (E.g., could be the other roles listed above).
	Other Areas	Staff need to know who to go to with issues regarding individuals, information, authority levels on decisions they cannot make, security, risk situations, …
1.5 Governance	Oversight	*Identify the organizations or structures responsible for decisions regarding the overall collaborative service delivery and members.*
	Leadership Team	*Identify any leadership committees or groups and what their roles are in oversight and decision making.*
	Liaisons	*Identify any liaisons or areas of responsibility the staff should be aware of. This would include who to bring issues to or questions regarding individuals requesting services or being supported, policies and practices, or breaches or potential breaches to privacy and security.*
1.6 Safe Environment (optional)	The staff and individuals may have an expectation, or the collaborative approach may have identified that the services will be delivered within a safe and healthy environment.	One of the goals may be to ensure the supports and services are provided in a manner that creates a safe place for individuals and staff. That means if any risks to someone's health or safety emerge, steps will be taken to minimize that risk, working with others if necessary. That might require the sharing of some information about the individuals involved or impacted by the risk, to deal with the situation. Such a disclosure or sharing will take place notwithstanding consent, as the best interests of all individuals must be top of mind. Staff who interact directly with individuals need to explain this to the individuals being served in a manner they can understand.
2. Legislation		
2.1 Privacy Legislation in Alberta	*Protection of Privacy Act* (POPA)	POPA applies to public bodies (government entities in Alberta), including provincial municipal and others. The act sets out the rights of access and of privacy, and the expectations on how the public bodies are

Area	Item	Notes
		to manage their obligations regarding the information that is in their custody or under their control.
	Health Information Act (HIA)	The HIA applies to custodians as defined in the Act and Regulations. The regulations identify which professions under the *Health Professions Act* are subject to the Act, if they are providing a health service. The act sets out the requirements and obligations custodians must follow in their management of health information, including providing access.
	Personal Information Protection Act (PIPA)	PIPA applies to private sector organizations in Alberta but does not include nonprofit agencies unless they manage personal information in the performance of a commercial activity, in which case the information is to be managed in accordance with the Act. The Act sets out the requirements and obligations covered organizations must follow in managing personal information, including providing access.
	Privacy Act	The federal *Privacy Act* applies to federal government institutions. The Act sets out the requirements and obligations institutions must follow in managing personal information.
	Personal Information Protection and Electronic Documents Act (PIPEDA)	PIPEDA applies to private sector organizations who are responsible for federal work, undertaking, or business (e.g., banks and financial institutions) and other organizations who do business in a province that does not have substantially similar legislation. Alberta's PIPA has been deemed substantially similar, placing organizations doing business in Alberta under PIPA, but they may be subject to PIPEDA if they transport personal information across provincial boundaries, or perform federal work.
2.2 Privacy Legislation	Applicable to the organization	Staff need to know which legislation applies to their own organization.
	Applicable to the other members	Staff should know which legislation applies to their partner organizations.
	If no legislation applies	Staff need to know how their organization, or how their partner organizations will demonstrate accountability for the information it manages in a

Area	Item	Notes
		manner consistent with the intent of privacy legislation if no legislation applies (e.g., nonprofits).
2.3 Some Areas of Similarity across Legislation	Purpose	All privacy legislation includes a Purpose for the legislation, that sets out the intentions for the legislation, which are primarily to govern how the organizations subject to the Act manage the information in their control or custody in a privacy protected manner, and to authorize the use, collection, and disclosure where appropriate and necessary. This is seen as the authority under an act for an organization to do something with the information.
	Access	Access to information is addressed by the legislation (note that there is as well the *Access to Information and Privacy Act*), dealing primarily with the right of access by individuals to their own information.
	Enables disclosure to others working on their behalf	Legislation identifies the circumstances under which the Act is extended to entities that are working on behalf of the organization, for example, under an agreement, by contract, or as a volunteer. POPA defines them as an employee, HIA as an affiliate. Identifying them in this manner sets out the authority for the organization to provide that entity with the information hey require to conduct the services that they are expected to provide.
	Collection Use and Disclosure	Legislation provides the authority for the collection, use and disclosure, outlining in what circumstances the organization is allowed to conduct those activities. (Note that in terms of the collaborative approach, 'sharing' refers to the collection, use, and disclosure.)
	Consent	Consent refers to the use of informed consent or permission for the collection and disclosure of an individual's own information. Consent is not authority under POPA for the collection of information, but is a means by which an authorized collection can occur.
	Notice	Notice or notification refers to the requirement for an organization that when collecting information directly from the individual it pertains to, to advise them of the reason for and authority by which their information is being collected, how it will be used, to whom it may be disclosed, and the name/title/position, business number and address of

Area	Item	Notes
		someone in the organization who can answer their questions about the collection.
	Safety Clause	Legislation includes a provision that authorizes the disclosure of personal and health information in circumstances where there is a risk to the health and safety (and well-being) of an individual, including the person or others. The provisions all differ, but the intent behind them is ostensibly to allow an organization to take the steps necessary to avert or minimize the risk situation from occurring.
	Security	Legislation places a requirement on organizations to ensure they protect the information they manage by implementing safeguards and processes that manage and respond to risk situations. The language varies across the legislation, but the intent is clear, that organizations must do what they can to protect the information in their custody and under their control against risks of unauthorized collection, use, disclosure, modification, and integrity do so. Staff should be trained on and aware of their roles in managing information in a secure and confidential manner.
	Retention	Legislation requires that information be retained for a period of time. While the amount of time varies, either under the legislation or in accordance with other requirements, it allows the individual the opportunity to request access to their information, as well as to who may have had access to it. Staff should be aware of what the retention period is for the information managed collectively under the collaborative approach.
	Oversight	Provincial privacy legislation establishes the oversight role of the Information and Privacy Commissioner. The Commissioner has specific authorities that allow it to conduct or review complaints, policies, and practices, of the organizations subject to the legislation to ensure they comply with the provisions of the legislation. The Office of the Information and Privacy Commissioner (OIPC) generally conducts reviews and investigations of complaints, in a manner that is meant to guide the organizations towards compliance, rather than being punitive, as a manner of practice. The Commissioner can also order compliance.

Area	Item	Notes
2.4 Some Differences between Legislation	Purpose	The HIA outlines in its Purpose that it is meant to prescribe rules for the collection, use, and disclosure of health information, which are to be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances. This is seen to apply more rigour to the way in which information is managed by a custodian.
	Type of information	Privacy legislation deals with personally identifying information of individuals, but the scope differs. Health information under the HIA is defined to include diagnostic, treatment and care information, along with registration information, that is managed by a custodian. Personal information under POPA is defined as recorded information about an identifiable individual, including information about the health and health care history, (among other areas), while PIPA defines personal information as information about an identifiable individual. The critical element is which organization holds the information. Information about the health of an individual is health information under the HIA, if it is in the control or custody of a custodian under that Act. The same information is considered personal information if held by a public body under POPA, or by an organization under PIPA.
	Least amount of information	Legislation requires that when dealing with collection, use, and disclosure, organizations limit themselves to the least amount or that which is deemed to be reasonable, in the circumstances. While similar to the HIA provisions the impact is not as broad as the requirements are not built into the purpose.
	Anonymous as possible	The HIA also states in its Purpose that the Act prescribes rules requiring the information be managed with the highest degree of anonymity as possible in the circumstances. This requirement is not explicitly stated in POPA or PIPA, and is very situational. For example, organizations involved in coordinated or integrated case management or service delivery would need to know they are working with the same individual. However, staff from an organization attending interagency meetings who wants to know what might be a good

Area	Item	Notes
		resource or referral for an individual they are dealing with, may not have to disclose the identity of that individual.
	Privacy Impact Assessment (PIA)	PIAs are a requirement under the HIA. However, as a due diligence exercise that assesses the risks when new or enhanced changes to the manner in which personal information is managed, including collection, they are strongly encouraged regardless of what legislation applies.
	Breach Notification	Breaches of privacy occur when there is unauthorized access, or a situation occurs where there is a potential risk of unauthorized access. Managing the breaches includes reporting the breach to the Office of the Information and Privacy Commissioner. The requirement to do so only exists under the HIA and PIPA, but reporting significant breaches is strongly encouraged regardless of what legislation applies.
	Common or integrated program or service	Organizations working together in a collaborative or integrated manner, is supported under the POPA Act, but the provision only applies to public bodies. That does not necessarily preclude the relationships with other organizations, but other provisions would need to be used to provide the authority.
2.5 Examples of other legislation that may come into play	*Children First Act*	The *Children First Act* applies to service providers as identified in the Act (provincial government departments, educational bodies as defined in POPA (which does not include private schools) police services as defined in the *Police Act* (which does include the RCMP), and agencies that provide services to children under a contract or agreement to a public body). It also applies to custodians under the HIA, and authorizes the disclosure of personal information about a child or the parent of a child to another service provider for the purposes of enabling or delivering services when it is in the best interest of the child. This provision is mirrored in POPA. The Act also authorizes the disclosure of health information about the child by a custodian to a service provider when necessary for the purposes of enabling or delivering services when it is in the best interest of the child.

Area	Item	Notes
	Child Youth and Family Enhancement Act	The *Child Youth and Family Enhancement Act* provides authority for the department of Children's Services to assess and determine if there is a need to provide services to a child that is in need of intervention. The act also places a requirement on any person who has reasonable and probable grounds to believe that a child is in need of intervention, to report that to a director (under the Act) or a police officer. The Act also contains a number of provisions providing authority for the collection and disclosure of personal and health information when conducting an assessment or investigation or providing services under the Act.
	Health Professions Act	The *Health Professions Act* sets out the authorities for the establishment of professional Colleges under the Act, and to manage information relative to the regulated members. Colleges are authorized to set Standards of Practice and Cdes of Conduct for its members. These standards may impose additional requirements on its members regarding the management of personal and health information.
2.6 Contracts and Agreements	Employees and Affiliates	As noted above, privacy legislation defines employees (POPA, PIPA) and affiliates (HIA) as individuals (and others) working on behalf of the organization, and may include volunteers, and those working under a contract or agreement. The legislation authorizes the disclosure to and use of information by these entities where it is required for the purposes of providing the services that is expected of them. Contracts or agreements should ensure the entity manages the information in such a manner that the host organization remains accountable for the information in compliance with the legislation. This may have implications on the entity in how they can use or disclose the information, which should be a consideration when they are involved in collaborative or integrated service delivery approaches.
3. Working with Individuals		
3.1 Authentication / Verification *(If applicable)*	Need to authenticate or verify identity	When determining the eligibility of individuals for services, there may be a need to know who the individual is. The member organizations will have determined if such a need exists, and the methods for doing so.

Area	Item	Notes
	Verification	Verification is the process of establishing the individual's identity through the review of documents such as an identification card, driver's license, birth certificate or other. When reviewing such documents, it may be sufficient to record that they were reviewed without any copies being made.
	Authentication	Authentication is the process of establishing that someone is who they claim to be, often in the context of a virtual connection, such as when online or phone. Examples of authentication include the use of two-factor authentication relying on the use of credentials to access an electronic information management system. When working with individuals it may be sufficient to authenticate them by asking for a piece of information that they are likely the only ones who would know.
3.2 Transparency	Trust	Individuals who are seeking support may not always feel comfortable doing so, nor have a high degree of trust in formal organizations, whether government or other. Building that trust with individuals and families is important when assessing their needs and providing services, and assisting them in working through the issues they are dealing with. One way to support this is to be open with them about the need for their information, and how it will be used.
	Notice	Notice or notification is a requirement under privacy legislation whenever personal and health information is being collected directly from the individual, which is also the default (but not the only) manner of collection. providing notice means advising the individual what information is required to be collected, under what authority, and used for what purpose. It should also indicate to whom the information may be disclosed, and the name or title of someone who can answer their questions about the collection must be provided, along with their business phone number and address. Beyond the formal requirements, it is important for staff working with the individual to explain what 'Notice' means in a way the individual can understand. (See also Deemed Consent, 7.1 below)
	Revisiting Notice	Recognizing that individuals in crisis may not always absorb everything they are being told, it may be important to revisit that notice at a later point in time, once the crisis has passed or been tempered.

Area	Item	Notes
4. **Collection**		
4.1 Purpose for Collection	Purpose Required Information	*Authority to collect information is driven by the purpose. Legislation authorizes the collection of personal and health information for specific purposes, which generally have as their foundation the reason why services are being assessed for and delivered. Staff need to be clear about the purpose for working together, and how the collection of information relates to that purpose.* *When the member organizations worked through their intentions for working collaboratively, and what they hope to achieve, they should have also put their minds to identifying how the services would be delivered, by whom and in what manner, and from that generally identify the type of information that would be required for the various roles, programs and services. In compliance with legislation, organizations should only collect the information necessary to provide whatever services or programs are being assessed for or delivered, or for purposes consistent with that.*
4.2 Authority to Collect	Where authority comes from POPA HIA PIPA	The authority to collect personal and health information is stipulated in the privacy legislation. POPA defines allowable purpose for the collection of personal information to be limited to • Where authorized by an enactment of Alberta or Canada, • Where required for law enforcement purposes, • Where directly related to and necessary for an operating program or activity of the public body. (see POPA s.4) Many programs and services delivered by government are based on legislation or some form of legislative instrument. However, there are also many programs and services that have been implemented under the authority/approval of the 'Head' of the public body. HIA outlines that health information can be collected for specific purposes primarily focused on the determination of need for and delivery of health services. (See HIA s.20, 27) or where authorized under legislation. PIPA limits the collection of personal information to purposes that are 'reasonable', which is further

Area	Item	Notes
		determined to mean 'what a reasonable person would consider appropriate in the circumstances'.
	Consent	Consent in and of itself should not be seen as the authority to collect information, but rather the means by which permission is granted by the individual for the collection of their information for the stated purpose. In other words, once an organization has determined they have authority to collect information, that it will be collected from the individual, and have provided notice to that individual, consent 'opens the door'. If consent is not provided, the organization has to rely on some other provision to collect the information, if available. (See also Deemed Consent, 7.1 below).
4.3 Limiting Collection	Limiting collection when working on behalf of an integrated service	It's important to have a good understanding of what information is likely to be required, including for when the information is collected on behalf of the member agencies participating in a collaborative or integrated service delivery approach. This may have been identified by listing questions that need to be answered, or completion of forms as part of screening and assessment tools, or by some other means. At the same time, it is not possible to always know what is needed by whom, and there may be information that is pertinent to more than one organization or that has implications for more than one service. For example, an individual with some mental health or addictions issues may be seeking housing. While they may not always seem related, if the issues relate to not being able to manage on their own, they may identify a need for supported housing rather than independent living. There may be occasions where an individual wants to tell their life story. While it may take some practice, it's important to be able to determine and capture or collect only the information pertinent to their situation that is required in order to assess, determine and provide services.
4.4 Insufficient information	Not being able to provide services or address needs with the collected information	If there isn't sufficient information provided to move forward with the services, due to there being gaps, there may be a need to return to the source (the individual) to collect that which is missing. It's not always an easy balance to make, to collect only what is required vs. collecting information in case it's

Area	Item	Notes
		required. Time and experience will help develop that skill.
4.5 Other Sources of Information	Other options	If the individual is not able to provide what is missing, and has indicated involvement with other organizations, it may be feasible to see if they have the required information. This may be especially true in urgent or risk situations where there is limited time or capacity to obtain what is required. The authority to approach them and request that information must be in place.
	Obtaining additional information	The first point of reference is always the individual, as they should be an integral part of the planning and delivery wherever possible. The preferred approach is to go back to them and explain what is required, and why. If they cannot provide or obtain it, or do not have the capacity to do so, the situation may be discussed with management. It may also be possible to broaden the scope of the consent in order to explore with other agencies they may have been involved with.
4.6 Direct or Indirect collection	Direct collection on behalf of the member organizations	Legislation requires that information be collected directly from the individual it pertains to as a default, unless authorized exceptions are met. Information that is collected on behalf of the collaborative/integrated service delivery partners is deemed to be a direct collection for use by the members, with the intent (and consent) for it to be shared with the members who require it.
	Authorized representative	Instances may arise where an authorized representative is acting on behalf of the individual, and provided they meet the defined legislative parameters and are authorized to exercise the individual's rights and powers (HIA s.104(1), POPA s.54, PIPA s.61), then the representative is acting as the individual, and the collection is deemed to be a direct collection.
	Indirect Collection	Exceptions to collecting the information directly do exist, and the collaborative partnership may have identified what is permissible, or the circumstances should clearly meet the legislated provisions, being vetted as required. (POPA s.5, HIA s.22(2), PIPA s.7(b)). An example of an exception is collection with the consent of the individual.

Area	Item	Notes
4.7 Contact Information	Collecting information about contact persons	Collecting contact information is an acceptable part of the process as long as the following criteria are met: • There has to be a reason for having contact information. This can include being able to reach the individual to set up appointments if they are not easily reached (e.g. no phone, couch-surfing,…), or in case of emergency situations. • The contact information is limited to the minimum required, and only for the purposes of connecting with the individual. In other words, it is collected for one purpose, and cannot be used for any other purpose. It may be sufficient in some circumstances to only collect a phone number. It is up to the client to advise their contacts that their information has been provided as a contact, and they should be advised to do so.
4.8 Consent	Requiring consent	The consent of the contact(s) is not required to collect their information. However, if contacted and additional information is requested of them, consent likely would be required, unless other provisions authorize the collection.
5. Use		
5.1 Use	Authorized use	The information about the individual is collected to: *(E.g.)* • *Screening / conducting an initial needs assessment,* • *Providing/facilitating accurate, appropriate referrals,* • *Delivering services meant to address their identified needs.*
5.2 Other Uses	Other authorized uses	There will likely be some consistent or related uses of the information, such as for evaluative purposes. That may include a service evaluation on an individual basis, to ensure the individual is receiving services appropriate to their needs; and on a broader organizational basis to assess the success of the initiative or of the impacts on individual member organizations. Other uses may be appropriate, but may need to be determined on a case-by-case basis. Examples could include dealing with urgent or risk situations, or where required by law, such as the need to report a child in need of intervention. Additional or other uses such as these should likely be discussed with

Area	Item	Notes
		your management team if clear direction has not been provided.
5.3 Risks *(If applicable)*	Risk of harm (to health and safety)	Privacy legislation contains a 'safety valve' that authorizes the disclosure of personal and health information where necessary to prevent or minimize harm. (POPA s.13(1)(CC), HIA s.35(1)(m), PIPA s.20(g)) The language differs, but the underlying intent of the provisions is to allow for actions to be taken to minimize that risk. Where there is an immediate risk to life, requiring an urgent response, police services should be contacted. Where there is an emerging risk, the degree of risk and the response required may shift, and there may be a need to discuss the situation with management. Where the members have identified as part of the purpose for the collaboration that the services are to be delivered in a safe and healthy environment, and a risk to the health or safety of an individual being supported, or any others including staff, emerges, there is a potential that some of the individual's information may be used to address the risk, irrespective of consent. If the individual identifies a risk to their health and safety, or to that of someone else, or if a potential risk situation is identified, the details of the risk situation should be discussed with the appropriate levels *(manager?)*. If there is an immediate safety risk it may be necessary to call 911 or take some action to minimize the risk, without putting anyone else in harm's way. Your organization may have in place risk assessment tools and guidance that can also be used.
	Safe and healthy environment	
6. **Disclosure**		
6.1 Authority to Disclose	Is there authority to disclose information	The authority to disclose personal and health information is stipulated in the applicable privacy legislation. These generally are 'may disclose" provisions, which means the entity holding the information will make a decision whether or not to disclose, but is not required to do so, unless otherwise stated. However, where the disclosure is for the purposes and objectives of the initiative, and meets the outlined criteria, the members have agreed that they will disclose the information, in compliance with the applicable provisions.

Area	Item	Notes
	POPA	POPA identifies a number of circumstances where, if met, disclosure is authorized. These may include: • for the purpose for which it was collected, or a consistent purpose, • if the individual has provided an informed consent, • to comply with an enactment of Alberta or Canada, • to comply with a subpoena, warrant or order issued by someone with authority to compel the production, • to an employee of a public body if the information is necessary for a common or integrated program or service, • to determine or verify someone's suitability or eligibility for a program or service, • to a public body or law enforcement agency to assist with an investigation, • to minimize the risk of harm to the health and safety a minor, or an imminent danger to the health and safety of any person. **See** POPA **s.13 for more information, and the exact wording.**
	HIA	HIA identifies the circumstances under which health information can be disclosed. They include: • to another custodian for purposes outlined in s.27, which primarily deal with the provision of health services, • to a person responsible for continuing treatment and care, (this may include non-health care providers) • to any person to avert or minimize the risk of harm to the health and safety of a minor, or a significant risk of harm to the health and safety of any person, • if a person lacks the mental capacity to provide consent and it is in their best interest, • if authorized or required under an enactment of Alberta or Canada, • with the consent of the individual, • where the information relates to the possible commission of an offence, and the disclosure will protect the health and safety of Albertans. (There are limitations on what can be disclosed under this section (HIA s.37.3) **See HIA ss. 27, 34, 35, 37.3 for more information, and the exact wording.**

Area	Item	Notes
	PIPA	PIPA limits the disclosure of personal information, identifying a number of circumstances under which it may occur. These include: • with consent of the individual, • where a reasonable person would think if in the best interests of the individual, and consent cannot be obtained in a timely way, • where authorized or required by a statute of Alberta or Canada, or some other regulation, bylaw, or legislative instrument, • to a public body or law enforcement agency to assist with an investigation, • where necessary to respond to an emergency that threatens the life, health or security of an individual or the public. **See PIPA ss.7, 20 for more information, and the exact wording.**
	Consent	Consent for the disclosure of information should be informed, meaning the individual has been fully advised as to the purpose for the disclosure of what information, and to which parties. See section 7, below.
6.2 To Whom	Information can be disclosed to whom	The various provisions outlined in legislation will identify to whom the information can be disclosed. Certain provisions indicate that it is to specific organizations or bodies, while others indicate it may be to a person or any person. The provisions should be reviewed to determine what the limitation is, to ensure the information is being disclosed in compliance with the legislation. When relying on consent for the disclosure, the entity should be named or referenced in the consent form wherever possible. If consent is to provide information to an agency, that applies to whomever working in the agency requires the information to provide or fulfill the outlined services or purposes.
6.3 How Disclosure Occurs		*The member organizations will have determined if the manner of sharing information is to be through access to a platform/system/database, or by some other electronic or other means.*
	Access through electronic systems	Access to the electronic platform/system is restricted to those organizations and their staff who have been designated as authorized users. The staff are further restricted to only accessing the

Area	Item	Notes
	Email	information they require to provide supports and services to the individuals they are working with. Information may be provided through some other means, if sanctioned by the member organizations, such as by email. However, given that email is inherently not secure, any personal information sent that way should be within an encrypted (preferred) or password-protected attachment. Personal information, including the name or other identifiers of individuals, should not be included in the email body or subject line. Passwords should be provided separately, and securely.
6.4 Copies	Disclosing copies of records/ recorded information	Where information/records are stored within an electronic information system, they can be accessed by authorized users. If no system is in use, copies of records or other documents, such as consent or other forms, can be sent electronically if required under the circumstances, with the appropriate safeguards in place (See Email, in 6.3, above). Care must be taken to ensure only information required and authorized to be disclosed is contained within the copies of records when providing access.
7. **Consent**		
7.1 Deemed consent	Implicit vs. explicit consent	By virtue of applying for various programs and services, individuals may be providing an implied consent to the collection of their information that is required in that application. Providing Notice (See Notice 3.2, above) to the individual about what information is required for the identified purpose is required when the information is collected directly, at which point the individual may choose not to pursue the application.
7.2 Informing consent	Explaining why consent is required to collect and disclose (share) information	An explanation must be provided to individuals in a manner they will understand that includes: - What they are consenting to (collection or disclosure of what information), - To whom the information will be disclosed. - Why the information is needed, and how it will be used (should be related to the purpose and objectives), - Who they can talk to if they have any questions about how the information will be used, or any other related questions. Explaining things properly and fully supports transparency, and helps to establish trust, and to

Area	Item	Notes
		prevent any of the scenarios in 7.8 through 7.11 (below) from taking place. The explanations may have to be given more than once, especially if the individual is anxious or in crisis.
7.3 Understanding	Assist the individual to understand the implications of providing or not providing their consent	Information should be explained in a manner such that the individual understands the implications are regarding consent: - Consenting means their information will be collected, used, and shared with the agreed upon partners to assess and provide them with services needed, - Not consenting to collection means they may still receive the services they need, but not in an efficient or as effective a manner; - Not consenting to sharing means approaching other agencies individually and repeating their story.
7.4 Capacity	The individual providing consent must have the capacity to understand what is required	The individual should be able to understand what they're told. Wording may need to change or be reframed or paraphrased to help them better understand; or there may be a need for interpreter if language is an issue. If the individual is under the influence of drugs or alcohol, consent may not be valid and may have to be revisited/confirmed at a point in the future. If the individual is too young to understand the implications of what consent means, or if they suffer some form of condition that impacts their capacity to understand, there may be a need to determine if someone can legally act on their behalf, or if there is some other provision that authorizes the collection or disclosure of their information.
7.5 Signature	Individuals must sign the consent form	There needs to be some form of verification that the person has actually consented. The normal way is for the consent form to be signed. The *Health Information Act* requires written consent, which includes electronic consent, but the level of authentication must be sufficient to identify the person signing the consent is who they say they are. Both POPA and the *Personal Information Protection Act* allow for oral or verbal consent, negating the need for a signature in those circumstances. Written consent includes electronic consent, but there is a

Area	Item	Notes
		need to authenticate that the person signing the consent is who they say they are, and under POPA the Head of the public body will need to approve a set of rules regarding the use and process for oral or electronic consent. Verbal consent must be properly documented.
7.6 Representative	Representatives providing consent on behalf of the individual must have the appropriate authority	Privacy legislation requires a person representing another to demonstrate their authority to act on behalf of another. The authorities are identified in: - POPA in section 54(1), - HIA in section 104. - PIPA in section 61(1).
7.7 Consent of a Minor	Determining when (age or other) a minor can provide their own consent, or if there is a need to obtain parental/ guardian consent?	When determining whether an individual has the capacity to understand the implications of providing consent, staff may get a sense of their capacity to understand what they are telling them. Staff may also get a feel for what their situation is, and what led to their being in the circumstances they are. Privacy legislation assumes that each individual has the rights and powers under the legislation, unless they do not have the capacity to understand and apply those rights, and if someone else has the authority to exercise those rights. A child/youth who has the capacity to understand can make their own decisions vis-à-vis their information, and a parent does not necessarily take those rights over. There is not a default requirement that the parent/guardian of a minor child would always need to provide consent for the disclosure of information about the minor. There may even be situations where it is not in the best interests of the minor to involve the parent, or worse yet, the parent's actions may have led, at least in part, to the situation evolving as it has. That said, it is often in the best interests of all to ensure the parent is engaged in the discussions, as they may well need to provide ongoing support or deal with the consequences of whatever the situation is. In summary, the child's capacity to provide informed consent is not the only factor to consider.
7.8 Denied collection consent	If the individual does not provide consent for the	If the individual does not provide consent, it's important to ensure they understand they may not

Area	Item	Notes
	collection of all or some of their information	be able to participate in the processes being used by the collaborative initiative, and while they may still be able to receive services, they would need to go to each organization individually and explain their situation. If the individual provides partial consent, it's important to ensure they understand there will be some limitations in what services, if any, can be provided through the collaborative initiative. For example, if they only consent to their information being shared with one of the member agencies, they will not be able to use the collaborative initiative process for the other agencies.
7.9 Denied consent for disclosure	If the individual does not provide consent	If the individual does not consent to any disclosure, then their information cannot be disclosed, unless one of the exceptions apply. (However, it is best to determine in advance if consent is required or not. Asking an individual for their consent, and then telling them the disclosure will take place regardless if they advise they will not provide their consent, is not appropriate, nor will it build trust.) The individual should be advised again of the implications of not consenting (e.g., limited services). They should also be aware that there may be times when their information needs to be disclosed, such as for dealing with risks to health and safety, or where required or authorized by law, but that should be explained in advance, prior to or in conjunction with the request for consent. The potential need to deal with risk situations should have already been explained. (See also 1.6, 5.3)
7.10 Limited consent	How to deal with the individual requesting that information not be disclosed to certain organizations, or only certain information be disclosed	Explore with the individual why they are making that request. They may have had a bad experience with the agency or someone from the agency previously, or heard from someone who did. If there is likely to be benefit in being able to refer the individual to that agency, it may be worthwhile to discuss options to resolving the issue. If their concern is based on second-hand information, it may fall into the urban-myth category, and it may be possible to dispel the myth based on knowledge of that agency or their staff, or advise that they may be better off to form their own opinion, as the agency has some strong capacity to provide some supports.

Area	Item	Notes
7.11 Withdrawn consent	What to do if the individual withdraws their consent	If the individual withdraws their consent explore with them the reasons for doing so, and explain to them what the implications are of doing so. If the rationale has to do with a bad experience, it may need to be followed up on, It is possible that an adverse incident is coloring their perception of all the agencies. The individual should also be advised that the withdrawal of their consent will prevent any further sharing of their information, but that actions already taken, and information already shared, will not be undone. If the individual is adamant in withdrawing their consent, their choice is to be respected, and actioned appropriately. That means pulling their consent, and likely requires advising any member agencies that have relied on the consent to access and disclose the individual's information. Information that has been stored on an electronic information system for access by the members may need to be removed, segregated, or in some manner be made inaccessible going forward.
8. **Information Management**		
8.1 Common records and storing information	Common records	A 'common' record is one that multiple organizations or member agencies rely on to inform their provision of services or supports to an individual they are collectively working with. The common record may take the form of an actual form, a tool that is used to collect information, or the entirety of the information stored within an electronic information system the members can access.
8.2 Consent forms	Filing a consent form and recording relevant notes	The consent form is an important document that verifies the authority for staff in the initiative to collect the individual's information. As a *common record*, it also needs to be accessible to anyone who may require it to disclose information. Along with the consent form, any relevant notes or comments also need to be recorded and made accessible to authorized users (e.g. any limitations posed by the individual, or the recording of verbal consent). Once the consent form is completed, it may be uploaded into the electronic information system, and managed in accordance with the relevant policies and practices.

Area	Item	Notes
8.3 Content	What information should be recorded	The member organizations may have determined what information is to be collected, and what is to be included in the electronic information management system if one is in use. Individuals generally have a right of access to their information, including the notes and observations that others have documented about them, and the information used to make decisions that impact them. It is important to document properly. Using behavioural observations vs. assumptions is a best practice. For example, it is better to indicate that the individual was observed to be staggering and slurring their speech, or having difficulty focusing, rather than stating that they appeared to be drunk. Information may also need to be collected during an agency's own intake process, and once an individual has been accepted by a member agency for services, that agency may collect additional information as per their normal processes. Those collections are not covered by this policy, although the information collected under the initiative as listed above will likely supplement the agency's own collection.
8.4 Location	Recording information in the proper location	*A determination should be made by the member agencies on where the personal and health information collected through the collaborative initiative should be documented. There may be occasions where staff need to take some initial notes, that then may be transcribed into the official record/file. Afterwards the initial notes could be deemed transitory and disposed of.*
8.5 Copies	Keeping copies of information	*A determination should be made by the member agencies on how the information is to be accessed and managed. If it is meant to be stored and used only through an electronic information management system, or if it is meant to be available and potentially copied into other systems should be clear.* The information collected through the collaborative initiative is collected for the purposes of facilitating a more comprehensive and collective response and support to the individuals it pertains to. All information collected under the Initiative must be maintained in a secure manner, including copies of that information.

Area	Item	Notes
		Agencies that access and pull information out of the system (i.e. make copies) should be readily identifiable, as the individual has a right to know who has accessed their information, and where they can access their information themselves.
8.6 Additional Information	Managing unnecessary information	Information that is not required and deemed superfluous is not authorized to be collected, and should not be documented or otherwise recorded. If provided by an individual, it should be returned or disposed of, with an explanation provided, as appropriate.
8.7 Transitory Information	Defined	Transitory information refers to information that has no value to the individual or the services being provided. Examples can include the initial notes taken by a staff person that are subsequently uploaded to an electronic information system; or the notes someone takes at a case conference or meeting, which are only meant to be used until such time the official record is available. Once they are uploaded or created, the notes should be disposed of in keeping with any retention and disposition requirements, generally immediately.
8.8 Retention	Information to be retained	Privacy legislation generally requires information to be retained for a minimal period of time if it has been used to make a decision that impacts the individual it pertains to. (Note that even a decision not to provide services impacts the individual.) *A determination should be made by the member agencies on what the period of time the information is to be retained for.*
8.9 Disposal	How information is to be disposed of when not required	Information must be managed appropriately throughout its lifecycle. That includes information that has been deemed not relevant or no longer required. Whether information has been recorded on an electronic information system, or in hard copy, or both, it must be disposed of in a secure manner at the end of its required retention period.
8.10 Documents	Documents provided by the individual	*A determination should be made by the member agencies on what if any records may be required from or about an individual, and how they are to be managed.* If documents are required from an individual, hard copy (e.g. paper) records can be copied and stored,

Area	Item	Notes
		whether in hard copy or electronically, then returned. If they are electronic (soft copy), they can be uploaded Note: Care should always be taken to ensure that the source of any electronic documents, especially in the form of attachments are safe, before opening them.
8.11 Corrections	Dealing with correction requests	Privacy legislation requires organizations to keep information as accurate and complete as is reasonable, given the purposes for which it is collected and used. If an individual indicates that the information that has been collected is not accurate, there is an obligation to correct it. Note that this applies to factual information only, not to opinions about an individual. If the individual requests a correction while their information is being collected and recorded, and they have presented the accurate information, the necessary adjustments can readily be made. However, if the information has been previously recorded, the information should be corrected, and accompanied by a notation that it has been. The member agencies may have identified a person or area responsible for corrections, as well as processes to be followed such as when the information was documented by another organization. Where other organizations have accessed or used the information, they should be advised of the correction. In a situation where the individual is requesting a change to non-factual information, such as an opinion, an annotation should be made, indicating what the individual is requesting, but the opinion should not be changed.
9. **Access**		
9.1 Information Access	Accessing required information	Users (staff) of organizations should be provided credentials that allow their access to the appropriate electronic information management system. Authorized users are permitted to access the system and the information they require of the individuals they are providing services to. That means only accessing the information of the individuals that have been assigned to the user/user's organization. Once authorized (such as through the initial Consent

Area	Item	Notes
		form signed by the individual) additional authority should not be required.
9.2 Unauthorized Access	Reporting unauthorized/ inadvertent access	The member organizations and their staff are working together as part of a larger collaborative to ensure the individuals receive supports in as comprehensive and effective a manner as possible. All members have a role in ensuring the personal and health information of those individuals is managed in a secure and privacy conscious manner, which means taking steps necessary to prevent unauthorized access and use. As well, unauthorized access can create risk situations that can impact the safety of individuals. Users are to report situations if they become aware that someone has accessed or tried to access information without permission/authority. This includes situations such as phishing or other electronic malware attacks. Reports should be made to their manager and to the security lead for the collaborative initiative. It is the policy of the collaborative Initiative to investigate breaches. The responsible area *(to be identified by the member organizations)* will conduct the review, and report to the Office of the Information and Privacy Commissioner where appropriate/necessary. As well, a determination will be made if the breach should be reported to the individual(s) whose information may have been inappropriately accessed. If the user or someone they know has inadvertently accessed information without authority, that should also be reported. Errors made while acting in good faith will not be dealt with in any punitive manner, and by bringing them to the attention of the designated Lead, it allows a review of what may have gone wrong (e.g. system errors). As well, decisions must be made if there is a need to advise the individual to whom the information pertains of the potential breach. Situations such as these should be reviewed on a case-by-case basis.
9.3 Shared Access	Sharing access	Access is not allowed to be shared with a user's co-worker or any other person. The use of credentials is limited to the user as the assigned person. When the user signs on to an electronic system with their

Area	Item	Notes
		credentials, they are confirming that they are the authorized user. Any actions taken or any information access is attributed to those credentials, so in turn, they are deemed to be the person responsible for those actions and information access. Users are required to appropriately safeguard their credentials in order to preclude the potential for unauthorized use or access. Should other staff in the organization require their own credentials, they should be discussing that with their manager/agency liaison who would make the necessary arrangements. There may be situations where more than one staff from an agency is involved with supporting an individual. Their roles should be clearly laid out, and their access should be consistent with those roles.
9.4 Client access	Client access to their own information	One of the underlying tenets of privacy legislation, is the right of an individual to manage their own information, including who can be authorized to access it. This right of ownership also includes their ability to access their own information held by others, subject to limited and specific exceptions. Most, if not all, of the information collected from an individual can likely be provided back to them, and dealing with access requests informally is often the most appropriate and simplest. For example, if the individual provides information that is used to complete any collection forms or the Consent Form, copies of the forms can be provided. Similarly, when a a document is required, it is generally appropriate to make a copy and return the original.
	Formal requests for access	If an individual makes a formal (written) request for their information/ records under legislation, direct them how to or make the request, or submit the request on their behalf to the designated lead.
10. Security		
10.1 Obligations	Shared responsibility	Everyone involved in the provision of services through the collaborative initiative who has a role in managing the personal information of others has an obligation to help protect the information, including: - Protecting the credentials provided as a user to access the electronic information system, not sharing them or storing them where they may be accessible to others;

Area	Item	Notes
		- Ensuring that access to the system is not left unattended; - Ensuring information is not copied, stored, or transmitted in an unsecure manner, including the use of email or messaging, without the appropriate safeguards; - Reporting any instances of unauthorized access, or potential breaches of privacy or security; - Not discussing situations involving clients or their information in open or public settings; - Adhering to all security requirements (See Appendix I: Security Measures)
10.2 Working from Home/Remotely	Additional requirements	Staff working remotely, whether in the field or from home, have an obligation to take the steps necessary to protect and manage the personal information of others in a secure and confidential manner, ensuring other persons cannot access that information, even if inadvertently. Those steps include paying attention to: - Orienting screens so to not allow others to view it; - Clearing the device's cache after a session, so that the information cannot be accessed by another user; - Turning off microphones and cameras when not intentionally in use; - Transporting laptops or other devices securely when travelling. For example, leaving a device locked in a car where it may be seen is not sufficient, even if left in a bag on the floor of the car. It should be locked in the trunk at a minimum, or taken with you.
10.3 Use of personal devices (BYOD)	Additional requirements	When staff are permitted to use their own devices, they have a heightened responsibility to ensure the appropriate level of protection, including: - Appropriate safeguards such as firewalls, anti-virus protection, use of a VPN (virtual private network) where appropriate; - Updating software as it becomes available, as updates often deal with additional security safeguards; - Ensuring other users who might share the device do not have access to any information or systems, putting in place the use of separate user profiles where necessary or appropriate;

Area	Item	Notes
		- Not storing any personal information of others on the device, using wipe software for the deletion of any information that has been stored. See additional resources in Appendix J.

Appendix E: Sample Agreement Back

Appendix E: Sample Commitment Agreement

Collaborative Approach Participation Agreement

This Agreement is between:

and

and

and

and

and

Preamble

Whereas each party is involved in the *<Identify the community or area where services are being delivered>* delivering or assisting in *<identify the services to be delivered to individuals and families>*;

And Whereas the parties recognize the services they provide can be better coordinated and delivered through collaboration and integration, to achieve *<Identify the outcomes or objectives>* for individuals, families and the community;

And Whereas in order to deliver coordinated services information about individuals will need to be collected, used and disclosed amongst the parties;

And Whereas the parties wish to put into place this Agreement governing the processes for such information sharing, including the collection, use, disclosure and protection of such information;

Therefore the parties agree as follows:

1.0 Definitions

In this Agreement:
1.1 **"Agreement"** means this Agreement, including any Schedules;

1.2 **"Collaborative or integrated services"** means the delivery of services across the parties that are delivered in a collaborative manner, where the parties are working together towards common goals with the supported individuals and families;

1.3 **"Information"** means:
(a) any personal information about an identifiable individual collected by a party under this Agreement;
(b) any health information about an identifiable individual collected by a party under this Agreement; and
(c) any non-identifying information collected by a party under this Agreement;
contained in a party's possession or control;

1.4 **"health information"** means diagnostic, treatment and care information, and/or registration information as defined by the *Health Information Act*:

1.5 **"personal information"** means personal information about an identifiable individual as defined by the *Protection of Privacy Act*, the *Personal Information Protection Act*, and the *Privacy Act* (Canada).

1.6 **"responsible party"** means a party who has been identified as having a role to play in the assessment and delivery of services to an individual or family through the collaborative/integrated service.

2.0 Purpose

2.1 The parties agree to co-operate in the delivery of collaborative or integrated services to individuals and families in the *<identify geographic or other location>* designed to benefit the *<health, safety, welfare and well-being of individuals and families>*. These services will include:

(a) identifying situations and providing supports and services where there would be a benefit to addressing the particular needs of *<identify target population or sector…>* through a collaborative approach to the delivery of appropriate *<identify services and resources>* provided by the parties; *and*

(b) specific and limited research and analysis of non-identifying data to identify issues within the community, and recommend changes to address those issues through longer term initiatives, strategies or systemic changes. <optional, adjust as required>

This Agreement sets conditions on the collection, use or disclosure of Information by the parties for the purpose of assessing, planning and delivering collaborative or integrated services.

3.0 Collection, Use and Disclosure of Information

3.1 Each party is responsible for the personal and health information that it collects in the course of performing the services, duties or functions of that party.

3.2 All Parties agree that the following will apply to all personal and health information collected under this Agreement:

(a) no party will collect or record personal and health information unless it is required to provide services or determine if a service should be provided;

(b) personal and health information which is collected will be used solely for the purposes for which it was collected under this Agreement and for no other purpose unless:
  (i) if the party is subject to, and such use is specifically authorized under, the *Protection of Privacy Act*; or
  (ii) if the party is subject to, and such use is specifically authorized under, the *Health Information Act*; *or*
  (iii) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection Act*; *or*
  (iv) if the party is subject to, and such use is specifically authorized under the federal *Privacy Act*; *or*
  (v) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection and Electronic Documents Act*; *or*
  (vi) the individual to whom the information pertains has consented to the use;

(c) personal and health information disclosed to and collected by a party will become part of the records of that party;

(d) a party agrees to keep personal and health information disclosed to it confidential and will not further disclose it except as required to fulfill the purpose of this Agreement and for no other purpose unless:
  (i) if the party is subject to, and such use is specifically authorized under, the *Protection of Privacy Act*; or
  (ii) if the party is subject to, and such use is specifically authorized under, the *Health Information Act*; or
  (iii) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection Act*; or
  (iv) if the party is subject to, and such use is specifically authorized under the federal *Privacy Act*; or
  (v) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection and Electronic Documents Act*; or
  (vi) the individual to whom the information pertains has consented to the disclosure;

3.3 Each party agrees to disclose specific and limited personal and health information with another party to assist that party to carry out the purpose of this Agreement and to assist in the provision of services to a subject individual or that individual's family, in accordance with the following:

(a) if the party is subject to the *Protection of Privacy Act* (POPA),
    i. sections 13(1)(b), (c), (g), (h), (k), (p), (q), (cc), or (ee) and
    ii. sections 7 and 8 of the POPA Regulation, or
(b) if the party is subject to the *Health Information Act*
    i. section 34, 35(1)(b), 35(1)(m), 35(n), 35(p), 36(a); or
(c) if the party is subject to the *Children First Act*,
    i. section 4(2)(b).; or
(d) if the party is subject to the *Personal Information Protection Act* (PIPA)
    i. section 7; or
(e) if the party is subject to the (federal) *Privacy Act*,
    i. section 8; or
(f) if the party is subject to the *Personal Information Protection and Electronic Documents Act*
    i. section 6.1, Schedule 4.3,
    ii. section 7(3); or
(g) if a party is not subject to privacy legislation, the party agrees to disclose specific and limited personal and health information with another party to assist that party to carry out the purpose of this Agreement and to assist in the provision of services to a subject individual or that individual's family, in accordance with the following requirements:
    i. the party will only disclose personal or health information:
        A. with the consent of the individual to whom the information pertains,
        B. with the consent of the guardian or of a duly authorized representative of the individual, or
        C. without consent where required or authorized by law;
    ii. ensure a record is created and maintained of what information has been disclosed to whom, and for what purpose, such record to be maintained for the same period for which the information disclosed is maintained, and to be made available to the individual should a request be made, unless otherwise restricted;
    iii. further, the party agrees to comply with the confidentiality and access to personal information requirements of the *Personal Information Protection Act* (PIPA) as if those provisions applied to that party.

3.4 All Parties agree that personal and health information disclosed will be limited to that which is necessary for the Receiving Party to know for the assessment and provision of services.

4.0 Case Management Committee (CMC) Meetings and Plans *<Delete if not Required>*

4.1 The Parties will assign specific staff to attend Case Management Meetings. All personnel being assigned by a Party will be employees or service providers:

(a) involved in delivery of program services provided by that Party applicable to the collaborative or integrated services to be provided under this Agreement; and
(b) have completed access and privacy training or if not, will do so prior to having access to any personally identifying information; and
(c) have been oriented to the requirements pertaining to the management of personal and health information outlined in this agreement.

4.2 The purpose of the Case Management Meetings is to provide a forum where participating parties can jointly assess and provide direction regarding the needs of an individual, and develop a coordinated case management plan. A meeting will occur:

(a) when an individual has been assessed by one of the parties as being in need of supports in a number of areas; and
(b) where the individual consents to, or where it may be in their best interests to participate in the collaborative or integrated service delivery approach to address their needs; and
(c) when a Coordinated Case Management Plan may be required.

4.3 Case Management Meetings:

(a) may be scheduled:
    (i) on a regular basis, involving personnel from all participating parties, to which situations would be brought forward as required; or
    (ii) may be scheduled as needed, once a situation is identified as requiring coordinated case management;
(b) may be held in person, or virtually, or a combination of both, as required;
(c) will, where deemed appropriate for the situation, result in the development of a coordinated case management plan, such plan:
    (i) to be developed jointly and signed by the parties that have agreed to take on an area of responsibility in supporting its execution,
    (ii) to be maintained in such location as to be available for the responsible parties,
    (iii) to be accessed only by the identified responsible parties,
    (iv) to be updated as actions are taken or as otherwise required, and
    (v) to be closed once the identified goals have been met, or where circumstances have changed such that the plan is no longer appropriate, and cannot be modified to address the changes.

4.4 Participation in the Case Management Meetings may include personnel from all parties, and specifically personnel from parties who are deemed to be able to assess and deliver services required by the individual or family.

4.5 The Coordinated Case Management Plan referred to in 4.2(c) shall contain the following information:

(a) name, contact information of the subject individual;
(b) date of birth;
(c) gender;
(d) information regarding the subject individual that has led to the determination they are in need of supports, including issues, supports, and factors that may place the individual at risk;
(e) the party that referred the situation to the Case Management Meeting;
(f) the services that are to be provided;
(g) the party that will be responsible for leading service delivery and the parties involved in service delivery; and
(h) whether consent of the subject individual has been obtained for collection, use and disclosure of personal information.

4.6 The Coordinated Case Management Plan will be created by participating parties and will be stored and maintained by *<identify where a plan will be located/maintained>*. Identified/signatory parties are authorized to maintain a copy of the coordinated case management plan to track their progress, providing updates as required to all responsible parties.

4.7 Personally identifying information of individuals for whom coordinated case management plans have been developed may be linked and used for the following purposes, in support of the services as outlined in this agreement:

(a) evaluation of the specific services being provided to the individual in order to track and manage progress in achieving the goals outlined in the plans; or

(b) evaluation of the overall effectiveness of the collaborative approach, on a population trend basis, subject to the following:

(i) once the data is linked, identifiers must be removed in such manner that the data is not identifiable, rendering it anonymous;

(ii) to be used in an aggregate form;

(iii) only participating members of the *<Identify the name of a data management committee or area identified as responsible for this area>* may use the de-identified or aggregate information for the purposes of data management, data linkage and analysis, including but not limited to supporting, reviewing, evaluating and improving the quality of the collaborative or integrated services approach.

(iv) no party will attempt to re-identify de-identified or aggregate information;

(v) the de-identified or aggregate information shall not be provided to a third party unless such is provided for in this Agreement or authorized by law.

5.0 <Advisory/Coordination/Management (ACM) Committee Meetings>

<Comment: This section may not be required or may need to shift depending on the structure required to support the collaborative partnership.

If it is used, need to identify the committee's name as well as its purpose or role, and level of personnel required. E.g. if advisory or direction setting, likely need supervisory or management level participation.

If it is not used, there needs to be some mechanism that outlines the governance/decision-making authority.>

5.1 The Parties will assign specific staff to attend *<Name of Committee>* Meetings. All personnel being assigned by a Party will be employees or service providers:

(a) involved in managing or supervising programs/services provided by that Party applicable to the collaborative or integrated services to be provided under this Agreement; and

(b) have completed access and privacy training or if not, will do so within three months of the date they are assigned, and prior to having access to any personally identifying information;

(c) have been oriented to the requirements pertaining to the management of personal and health information outlined in this agreement; and

(d) are authorized to make recommendations *(or decisions)* on behalf of their organization relative to this Agreement.

5.2 The purpose of the *<Name of Committee>* Meetings is to provide a forum where member parties will:

(a) jointly assess and provide direction regarding the delivery of the collaborative services by the parties;

(b) provide guidance on issues brought forward by the Case Management Committee;

(c) review and evaluate progress of the initiative; and

(d) recommend *(or decide on)* changes to the collaborative approach as required, based on the reviews and evaluations vis-à-vis stated objectives.

5.3 *<Name of Committee>* Meetings will be managed as follows:

(a) Meetings will be scheduled on a regular basis, involving personnel from all member parties;
(b) Meetings are chaired by .
(c) Meetings may be held in person, or virtually, or a combination of both, as required;
(d) Meetings will not involve discussions of or access to the identifying information of individuals receiving services through Coordinated Case Management, except where:
    (i) problem resolution requires escalation to the level of this committee; and
    (ii) only the responsible parties involved are present for the discussion or have access to the identifying information;
    (iii) Where there may be benefit for having input from non-involved/responsible parties present for the discussion, they are not to have access to identifying information, including through the discussions.
(e) Minutes will be recorded, and are not to include information that may identify individuals being provided services.

6.0 Responsibilities, Dispute Resolution and Costs

6.1 Responsibilities

Each party shall be responsible for the actions of its employees and service providers with respect to the collection, use and disclosure of the personal information and personal health information that is governed by this Agreement and related de-identified or aggregate information.

6.2 Dispute Resolution

(a) In the event of a dispute between the parties with respect to the meaning and intent or any conflict, uncertainty or ambiguity in this Agreement, the senior management for each of the parties shall consult as to an appropriate resolution of the dispute.
(b) During the resolution of the dispute mentioned in subsection (a), the parties shall make reasonable efforts to minimize and mitigate any costs or delays associated with the resolution of the dispute.

6.3 Costs

Costs incurred by a party pursuant to this Agreement shall be the responsibility of that party.

7.0 Administrative, Technical and Physical Safeguards

7.1 Each party shall protect the Information which is in its possession or control pursuant to this Agreement according to its policies, procedures or guidelines regarding how it will maintain administrative, technical and physical safeguards for such information.

7.2 If a party does not have policies, procedures or guidelines mentioned in subsection (.1) that party shall create or adopt policies, procedures or guidelines *<within 3 months of entering into / and prior to having access to any personally identifying information through* this Agreement.

7.3 The administrative, technical and physical safeguards mentioned in subsection (1) must:

(a) Protect the integrity, accuracy and confidentiality of the Information;
(b) Protect against any reasonably anticipated:
    (i) Threat or hazard to the security or integrity of the Information;

(ii) Loss of the Information; and
(iii) Unauthorized access to or use, disclosure, modification or deletion of the Information.

7.4 Where personally identifying information is maintained in a central repository or system for access and use by participating parties, the repository will be managed by *<Identify responsible party>* in such manner that:

(a) the repository meets all of the technical safeguards required as noted in 7.3 above;
(b) only those parties authorized to access it are able to.

8.0 Incident Management

8.1 Each party shall respond to an event of inappropriate collection, accidental or unauthorized access, use, disclosure, modification or deletion of personal information or personal health information according to its policies, procedures or guidelines for incident management. Such policies will include the notification of the individual of such incident unless the party involved is of the view that such could result in harm to any person.

8.2 If a party does not have policies, procedures or guidelines mentioned in subsection (.1), that party shall adopt or create policies, procedures or guidelines *<within 3 months of / or prior to>* entering into this Agreement.

8.3 In the event of accidental or unauthorized access, use, disclosure, modification or deletion of information, including de-identified or aggregate information, the party responsible shall promptly:

(a) notify all of the other parties of the event;
(b) take all reasonable steps to contain the disclosure; and
(c) take all reasonable steps to prevent a recurrence of the event.

8.4 Where personally identifying information is maintained in a central repository for access and use by participating parties, incident management will also apply in like manner to the information stored therein, with the following requirements:

(a) steps will be taken as required to prevent any further unauthorized access, as required;
(b) the incident will be reported to all members of the *(ACM)* Committee;
(c) a determination will be jointly made by the *(ACM)* Committee on the steps to be taken regarding reporting of the incident.

9.0 Retention and Disposition

9.1 Retention

(a) Each party shall retain the Information according to its policies, procedures or guidelines regarding retention periods.
(b) If a party does not have policies, procedures or guidelines mentioned in subsection (a), that party shall exercise due diligence in adopting or creating policies, procedures or guidelines, in keeping with the standards outlined in the adopted framework.
(c) The policies, procedures or guidelines mentioned in subsection (a) must ensure the Information stored in any format is retrievable, readable and useable for the full retention period.
(d) Where personally identifying information is maintained in a central repository for access and use by participating parties, retention of records will be managed in accordance with (c), with the following provisions:

(i) Personally identifying information will be kept for a period of *<Identify the agreed upon/legislated time frame>* years;
(ii) Non-identifying information will be maintained for an additional *<Identify the agreed upon/legislated time frame>* years to enable ongoing trend analysis. *<If required>*

9.2 Disposition

(a) Each party shall dispose of the Information in a secure manner and according to its policies, procedures or guidelines.
(b) If a party does not have policies, procedures or guidelines mentioned in subsection (a) will be disposed, that party shall exercise due diligence in adopting or creating policies, procedures or guidelines.
(c) The policies, procedures or guidelines mentioned in subsection (a) must state how the Information will be disposed of in a manner that protects the privacy of the subject individual.
(d) Where personally identifying information is maintained in a central repository for access and use by participating parties, disposition of records will be completed in such manner that it protects the privacy of the subject individual, managed in accordance with (c).

10.0 Access Requests

10.1 Each party shall follow its own process to be used in responding to an access request made by a subject individual for her or his information.

10.2 If a party does not have a process mentioned in section 10.1, that party shall create a process within 3 months of entering into this Agreement which is consistent with PIPA or access to information legislation applicable to that party.

10.3 Where personally identifying personal information is maintained in a central repository for access and use by participating parties, access requests will be managed by *<Identify the responsible party/area>* as per the following:

(a) Consultation will take place with the parties responsible for the provision (disclosure) of the individual's information. If the providing party is of the view the information should not be disclosed, they should identify the (legal) rationale, and be prepared to assist in defending that decision, should there be a challenge.
(b) Alternatively, the individual may be directed to contact the providing organization for access to specific information/records.

11.0 Accuracy

11.1 Each party shall use reasonable efforts to ensure the completeness and accuracy of personal and health information collected, used or disclosed pursuant to this Agreement.

11.2 It is understood and agreed that the parties cannot guarantee the accuracy and shall therefore not be held responsible for any damage to the other party resulting from the collection, use or disclosure of any personal and health information that is inaccurate, incomplete or out-of-date.

11.3 Each party shall correct any inaccuracies of personal and health information collected, used or disclosed pursuant to this Agreement.

11.4 Should a subject individual indicate to a Party that personal and health information collected by that party is incorrect, that Party shall, and in keeping with the party's applicable legislation:

(a) correct the information and advise any other Parties of the need to correct their information should they have the same information, if the Party agrees that the information is incorrect; or
(b) make a notation on the record that the subject individual requested a correction, where the Party is not satisfied that the information is incorrect;
(c) opinions and other non-factual information cannot be corrected, so a notation on the record should be made indicating the request of the subject individual for a correction.

12.0 Indemnification <Delete if not required>

12.1 Subject to section 12.2, each party agrees to indemnify and save harmless all of the other parties and all of its employees, agents, volunteers and contractors from and against any damages, costs, losses or expenses or any claim, action, suit or other proceeding which they or any of them may at any time incur or suffer as a result of or arising out of any injury or loss which may be or be alleged to be caused by or suffered as a result of the acts or omissions of the other parties and its employees, agents, volunteers and contractors relating to, attributable to or in connection with the performance of this Agreement.

12.2 Each party agrees to give notice to the other parties of any claim, action, suit or proceeding relating to or in connection with the management of the information that is the subject of this Agreement. Each party must, at its own expense and to the extent reasonably requested by the other parties, participate in or conduct the defense of any such claim, action, suit or proceeding and any negotiations for the settlement of the same, but one party will not be liable to indemnify the other party or any other
indemnified persons for payment of settlement of claim, action, suit or proceeding unless the other party has given prior written consent to the settlement.

13.0 Review of Agreement

13.1 The parties shall, on a periodic basis, review the Agreement, and the policies, procedures and guidelines mentioned in it, to ensure it is up-to-date and being followed.

13.2 Such reviews are to minimally occur and be reported on, on an annual basis.

14.0 Amendments

14.1 At any time during the term of this Agreement a party may, by written notice to all of the other parties, request changes to the Agreement.

14.2 Amendments requested pursuant to section 14.1 which are acceptable to all of the parties must be set out in a document executed by all parties and attached as an additional Schedule to this Agreement, whereupon this Agreement must be deemed to be amended in accordance with the provisions of such Schedule.

15.0 Application / Assignability

15.1 This agreement applies to all signatory parties, including their employees and contracted service providers involved in the delivery or management of services under this Agreement.

15.2 By signing this Agreement, a party commits to the terms herein, and the responsibility of ensuring its employees and contracted service providers involved in the delivery or management of services under this Agreement.

15.3 This Agreement or any part hereunder, or any actual or any beneficial interest herein, shall not be assignable by the record holder without the written consent of all of the parties.

16.0 Withdrawal

16.1 Subject to section 16.3, a party may withdraw from this Agreement by providing ___ (days) (months) written notice to all other parties of its intent to do so.

16.2 The obligations created by Articles 3.0, 4.0, 5.0, 7.0, 8.0, 9.0 and 10.0 in relation to the Information will continue to apply to any party that withdraws from this Agreement under section 16.1.

16.3 Where the *<Identify the party should this clause be required E.g. if party's continued involvement is critical to the collaboration>* is the withdrawing party, this agreement will terminate and the provisions of Article 17.0 will apply.

17.0 Termination

17.1 The parties may agree to terminate this Agreement.

17.2 In the event that this Agreement is terminated, the obligations created by Articles 3.0, 4.0, 5.0, 7.0, 8.0, 9.0 and 10.0 in relation to the Information will continue to apply to the parties.

18.0 Coming into force

18.1 This Agreement comes into force on the date that the last of the Parties have executed this Agreement and remains in force until it is terminated in accordance with Article 17.

19.0 General

19.1 Any notice, amendment, request or communication pursuant to this Agreement must be in writing and must be delivered or mailed to all of the other parties:
in the case of the [name party]:
Name, Position
Branch/Area
Division [if applicable]
Organization
Address

19.2 This Agreement and its Schedules shall constitute the entire Agreement of the parties and supersedes all previous agreements between the parties, which relate to the collection, use and disclosure of information and de-identified information covered by this Agreement.

19.3 The headings used in this Agreement are for convenience only and are not to be used in the interpretation of the Agreement.

19.4 This Agreement shall be governed by and interpreted in accordance with the laws in force in the Province of Alberta.

20.0 Signatures, Signing Dates and Appendices

Agreed to behalf of the [name party] this day of _____, 20__

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

Agreed to behalf of the [name party] this day of _____, 20__

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

Agreed to behalf of the [name party] this day of _____, 20__

…

Appendix F- Sample Consent Forms

Back

As noted, the consent requirements under the *Health Information Act* (HIA) are the most stringent, and if used, will meet the requirements under other legislation. For this reason, and given that many collaborative service delivery circumstances will involve health information, the enclosed sample consent form templates meet the HIA requirements.

Requirements under the HIA[2]:

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

(a) an authorization for the custodian to disclose the health information specified in the consent,
(b) the purpose for which the health information may be disclosed,
(c) the identity of the person to whom the health information may be disclosed,
(d) 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,
(e) the date the consent is effective and the date, if any, on which the consent expires, and
(f) 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.

HIA Regulation[3]:

6(1) In this section, "electronic consent" means a consent provided electronically.

(2) For the purposes of sections 34 and 59 of the Act, an electronic consent or a revocation of an electronic consent is valid only if the level of authentication is sufficient to identify the individual who is
granting the consent or revoking the consent, as the case may be.

HIA Guidelines and Practices[4]:

For the purposes of section 34(1), consent must include:

- an authorization for the custodian to disclose the health information specified in the consent;
- the purpose for which the health information may be disclosed;
- the identity of the person to whom the health information may be disclosed;
- an acknowledgement that the consenting individual 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 to the disclosure;

[2] *Health Information Act* Revised Statutes of Alberta 2000 Chapter H-5 Current as of December 31, 2021
[3] *Health Information Regulation* Chapter/Regulation: 70/2001
[4] *Health Information Act* Guidelines and Practices Manual ISBN 978-0-7785-8292-2 Online

- the date the consent is effective and the date on which the consent expires; and
- a statement that the consent may be revoked at any time by the individual providing it.

A consent or revocation of consent must be provided in writing or electronically (34(2)). Under section 6(1) of the Health Information Regulation, an "electronic consent" means one that is provided electronically. An "electronic consent or revocation of consent" (see section 8.4.3 following) means the granting or revoking of an authority that is provided electronically. A disclosure of health information with consent must be carried out in accordance with the terms of the consent (34(3)).

A consent that is provided in writing must be signed by the person providing it (34(5)). A consent that is provided electronically is valid only if it complies with the requirements set out in the regulations (34(6)). Under section 6(2) of the Health Information Regulation, an electronic consent or revocation of consent is valid only if the level of authentication is sufficient to identify the individual who is granting or revoking the consent.

Except for the provisions of the Act which authorize the disclosure of individually identifying diagnostic, treatment and care information without consent (section 35, 37.1, 37.3), and other individually identifying health information, registration information (sections 36 to 40), the absence of consent is interpreted as the absence of authority. True consent is informed and voluntary. Individuals cannot be penalized for refusing to consent to certain disclosures through the denial of the provision of health services, particularly if that was the purpose for which the information was originally collected.

Provision by an individual of his or her personal health number is not the same as consent for disclosure of individually identifying health information.

Electronic or Oral Consent
Privacy legislation deals with electronic and oral consent differently.

The *Protection of Privacy Act* (POPA) requires the Head (which may be delegated) of a public body to establish rules respecting the purposes for which consent in an electronic or oral form is acceptable; ensuring the purpose for which consent is collected falls within those identified purposes; and the public body has explicitly stated that it will accept consent in an electronic or oral form. Beyond that, the electronic form must include an acceptable electronic signature, the oral consent must be provided in such a manner that the individual is appropriately authenticated, and records must be maintained and available. Details of the above are in the POPA Regulations.

The HIA does authorize the use of electronic consent, requiring that the means of authentication is sufficient to identify the individual providing consent. The Act does not recognize the use of oral consent. However, if oral consent is collected electronically, and in a manner that meets the requirements of being able to authenticate the individual's identity, that could be deemed to be electronic consent.

The *Personal Information Protection Act* (PIPA) also allows for the use of oral consent, and written consent is acknowledged to include electronic consent. The Act does not go into the same level of detailed requirements as POPA or the HIA.

So, out of all of this, a best practice is to ensure the organization sets out how it will manage consent, use a form that meets the requirements of the HIA as far as the form itself, and be clear about when it will allow the use of oral or electronic consent (depending on its authority), with the appropriate processes in place to authenticate and manage the information.

Sample Forms:

The sample templates included here have incorporated the above requirements, and in addition, outline the provisions under other legislation that they are authorized under. If there is legislation where there are no subject to organizations involved in the collaborative approach, and those provisions are not being depended on, they may be removed from the consent form. Organizations that adopt these forms should ensure they are adjusted to their particular circumstances(s). In addition, they may choose to place their logos on the forms so to be more transparent.

(See also *"An Information Sharing Framework: Supporting Enhanced Collaboration between Organizations Providing Mental health Services"* - Integrated Service Delivery [G(1)(i)(B)], Consent Forms [H(5)]

Sample 1: Simple consent

Useful for many common consent situations, especially where consent may be on a one-to-one basis.

Sample 2:

Consent for the disclosure of information to/between multiple organizations working collaboratively, where the client can specify which organizations they are consenting to. The consent would only be valid for organizations that have been consented to by the client, and only if they are providing a service.

Sample 3:

Consent for the disclosure of information to/between multiple organizations working collaboratively, where the specific services are listed by organization. This form of consent may be useful to assist organizations and the client identify which organizations to refer the client to.

Sample 4:

Consent for the disclosure of information to organizations working together to provide seamless, integrated services. Disclosure is deemed to be to all of the organizations, provided that the organizations have enabled an integrated service delivery process.

Sample 1: Consent to Disclosure for the Purposes of the _____ Collaborative

CONSENT TO DISCLOSE INDIVIDUALLY IDENTIFYING PERSONAL AND/OR HEALTH INFORMATION	
Authorized by and in accordance with: • The *Health Information Act* (HIA) s.34 • The *Protection of Privacy Act* (POPA) s.13(1)(C) and s.7 of the POPA Regulation • The *Personal Information Protection Act* (PIPA) s.8 • The *Personal Information Protection and Electronic Documents Act* (PIPEDA) s.6.1, Schedule 1(4.3) • The *Privacy Act* s.8	
Client Information:	Full Legal Name:
	Also Known As:
I authorize the following personal and/or health information: (*description of the information)*	
to be disclosed by: *(name of organization(s))*	
to: *(name of recipient/role/organization)*	
for the following purpose(s) *(how the information will be used)*:	
I understand why I have been asked to disclose my individually identifying information, and am aware of the risks and benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent in writing or electronically at any time.	
Effective Date:	Expiry date (valid for 2 years if no date provided)
Signature of client/authorized representative. *	X
*If you are signing as an Authorized Representative on behalf of the client, please provide: Name: _____ Circle Source of Representative's Authority: (HIA s.104 / POPA s.54(1) / PIPA s.61(1)) _____ Relationship to client if confirming to be the nearest relative:	
The information collected on this form is collected for the purposes outlined herein, under the authority of: HIA s.20-22; POPA s.4; PIPA s.; PIPEDA Sched.1, 4.3; Privacy Act s.4. If you have questions about the collection and use of the information on this form, contact *<insert title, business address and phone number >*.	

Page 1/1

Instructions for the completion of the *Sample 1* Consent Form:

This Consent Form can be adapted by the following steps.

1. Identify in the Title the Name of the Organization or Collaborative Partnership if there is one.
2. Remove any references to legislation where it is not applicable. For example, if personally identifying information is not going to be collected by or disclosed with a federal government institution, the references to the Privacy Act can be removed.
3. In the "*description of the information"*, list or insert the type of information the consent is meant to authorize disclosure of.
4. In the *"name of organization(s)"*, list or insert the organization or organizations from whom the information is being sought.
5. In the *"name of recipient / role / organization"*, list or insert the organization or organizations that are seeking the information, or to whom the information is to be disclosed.
6. In the *"how the information will be used"*, identify for what purpose the information is to be used.
7. In the Collection statement at the end of the form, insert the title, business address and phone number of a staff member who is able to respond to any questions regarding the collection of the information.

Complete the following steps when the client or their representative is present.

1. Insert the date from which the consent is to be effective, and the expiry date.
2. Once the client has been given Notice, and understands the purpose for which the information identified in the consent form is to be used, ask them to sign.
3. If a legally authorized representative is signing on behalf of the client, ask them to provide evidence of the authority they indicate they are acting under, and indicate what that authority is.
4. If the legally authorized representative indicates they are the client's nearest relative as per the *Personal Directives Act* or the *Mental Health Act*, indicate what their relationship is with the client.

CONSENT TO DISCLOSE INDIVIDUALLY IDENTIFYING PERSONAL AND/OR HEALTH INFORMATION	
Authorized by and in accordance with: • The *Health Information Act* (HIA) s.34 • The *Protection of Privacy Act* (POPA) s.13(1)(C) and s.7 of the POPA Regulation • The *Personal Information Protection Act* (PIPA) s.8 • The *Personal Information Protection and Electronic Documents Act* (PIPEDA) s.6.1, Schedule 1(4.3) • The *Privacy Act* s.8	
Client Information:	Full Legal Name:
	Also Known As:
I authorize the following personal and/or health information: (*description of the information)*	
to be disclosed by: *(name of organization(s))* To the organizations listed, as attested to by my initials, on the reverse/following page.	
I understand why I have been asked to disclose my individually identifying information, and am aware of the risks and benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent in writing or electronically at any time.	
Effective Date:	Expiry date (valid for 2 years if no date provided)
Signature of client/authorized representative. *	X
*If you are signing as an Authorized Representative on behalf of the client, please provide: Name: _____ Circle Source of Representative's Authority: (HIA s.104 / POPA s.54(1) / PIPA s.61(1)) _____ Relationship to client if confirming to be the nearest relative:	
The information collected on this form is collected for the purposes outlined herein, under the authority of: HIA s.20-22; POPA s.4; PIPA s.; PIPEDA Sched.1, 4.3; Privacy Act s.4. If you have questions about the collection and use of the information on this form, contact < *insert title, business address and phone number* >.	

The following organizations are working together to provide *(list the services)* in a collaborative approach. This approach is intended to *(state the purpose or objectives)*. By signing the consent on the reverse, you are agreeing that the information required can be shared between these organizations if they become involved in assessing and/or providing you with any of these services.	
Organization	*Initials**
*My initials after each organization listed above indicates that I am consenting to their having access to my information as stated on the consent form above. If I do not want them to have access, I understand that I will have to directly provide any information they require if I request services from them, and have not placed my initials after their name.	
The following section is for the inclusion of additional organizations. Any new members of the collaborative who will require access indicated on this consent form are authorized by the placement of my initials.	

Instructions for the completion of the *Sample 2* Consent Form:

This Consent Form can be adapted by the following steps.

1. Identify in the Title the Name of the Organization or Collaborative Partnership if there is one.
2. Remove any references to legislation where it is not applicable. For example, if personally identifying information is not going to be collected by or disclosed with a federal government institution, the references to the Privacy Act can be removed.
3. In the "*description of the information*", list or insert the type of information the consent is meant to authorize disclosure of.
4. In the *"name of organization(s)"*, list or insert the organization or organizations from whom the information is being sought. If the only disclosures or sharing of information will be between the partnering organizations, indicate that.
5. In the table on page 2, list or insert the organizations to whom the information is to be disclosed.
6. In the *"services to be provided"*, on page 2, identify the types of services to be provided through the collaborative approach.
7. In the *"state the purpose or objectives"*, on page 2, identify the purpose behind the collaborative approach and/or what the desired objective(s) is to be achieved through the collaborative approach.
8. In the Collection statement at the end of the form, insert the title, business address and phone number of a staff member who is able to respond to any questions regarding the collection of the information.

Complete the following steps when the client or their representative is present.

1. Insert the date from which the consent is to be effective, and the expiry date.
2. Once the client or their representative has been given Notice, and understands the purpose for which the information identified in the consent form is to be used, ask them to sign.
3. Go through the information on the second page, being clear that the organizations listed will only access the client's information if they assess or provide services to the client.
4. Ask the client or their representative to initial by the names of all organizations they are providing consent to for the disclosure of their information. If they do not consent to disclosure to a particular organization, while you may explore with them why not, you should advise them of the implications, that is, they will need to disclose their information directly to the organizations should they engage with them in the future.
5. If a legally authorized representative is signing on behalf of the client, ask them to provide evidence of the authority they indicate they are acting under, and indicate what that authority is.
6. If the legally authorized representative indicates they are the client's nearest relative as per the *Personal Directives Act* or the *Mental Health Act*, indicate what their relationship is with the client.
7. If any new organizations are added as partners in the collaborative approach, their names should be added and the client or representative should be asked to initial their consent to disclosure.

Sample 3:

CONSENT TO DISCLOSE INDIVIDUALLY IDENTIFYING PERSONAL AND/OR HEALTH INFORMATION

Authorized by and in accordance with:

- The *Health Information Act* (HIA) s.34
- The *Protection of Privacy Act* (POPA) s.13(1)(C) and s.7 of the POPA Regulation
- The *Personal Information Protection Act* (PIPA) s.8
- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) s.6.1, Schedule 1(4.3)
- The *Privacy Act* s.8

Client Information:	Full Legal Name:
	Also Known As:

I authorize the following personal and/or health information: (*description of the information)*

to be disclosed by: *(name of organization(s))*

To the organizations listed, and for the purpose(s) outlined on the reverse/following page.

I understand why I have been asked to disclose my individually identifying information, and am aware of the risks and benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent in writing or electronically at any time.

Effective Date:	Expiry date (valid for 2 years if no date provided)
Signature of client/authorized representative. *	X

*If you are signing as an Authorized Representative on behalf of the client, please provide:

Name: _____
Circle Source of Representative's Authority: (HIA s.104 / POPA s.54(1) / PIPA s.61(1))

_____
Relationship to client if confirming to be the nearest relative:

The information collected on this form is collected for the purposes outlined herein, under the authority of: HIA s.20-22; POPA s.4; PIPA s.; PIPEDA Sched.1, 4.3; Privacy Act s.4. If you have questions about the collection and use of the information on this form, contact < *insert title, business address and phone number*>.

The following organizations are working together to provide the services listed below in a collaborative approach. This approach is intended to *(state the purpose or objectives)*. By signing the consent on the reverse, you are agreeing that the information required can be shared between these organizations if they become involved in assessing and/or providing you with any of these services.

	Type of Service	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
The following section is for the inclusion of additional organizations. Any new members of the collaborative who will require access indicated on this consent form are authorized by the placement of my initials.															
Name of Organization															
Name of Organization															

Instructions for the completion of the *Sample 3* Consent Form:

This Consent Form can be adapted by the following steps.

1. Identify in the Title the Name of the Organization or Collaborative Partnership if there is one.
2. Remove any references to legislation where it is not applicable. For example, if personally identifying information is not going to be collected by or disclosed with a federal government institution, the references to the Privacy Act can be removed.
3. In the "*description of the information"*, list or insert the type of information the consent is meant to authorize disclosure of.
4. In the *"name of organization(s)"*, list or insert the organization or organizations from whom the information is being sought. If the only disclosures or sharing of information will be between the partnering organizations, indicate that.
5. In the *"state the purpose or objectives"*, on page 2, identify the purpose behind the collaborative approach and/or what the desired objective(s) is to be achieved through the collaborative approach.
6. In the table on page 2, list or insert the organizations to whom the information is to be disclosed.
7. At the top of the table, list the types of services provided by the members of the collaborative approach, and place an "X" in the boxes corresponding to the organization(s) that provide them.
8. In the Collection statement at the end of the form, insert the title, business address and phone number of a staff member who is able to respond to any questions regarding the collection of the information.

Complete the following steps when the client or their representative is present.

1. Insert the date from which the consent is to be effective, and the expiry date.
2. Once the client or their representative has been given Notice, and understands the purpose for which the information identified in the consent form is to be used, ask them to sign.
3. Go through the information on the second page, being clear that the organizations listed will only access the client's information if they assess or provide services to the client.
4. If a legally authorized representative is signing on behalf of the client, ask them to provide evidence of the authority they indicate they are acting under, and indicate what that authority is.
5. If the legally authorized representative indicates they are the client's nearest relative as per the *Personal Directives Act* or the *Mental Health Act*, indicate what their relationship is with the client.
6. If any new organizations are added as partners in the collaborative approach, their names should be added and the client or representative should be asked to initial their consent to disclosure.

Sample 4:

CONSENT TO DISCLOSE INDIVIDUALLY IDENTIFYING PERSONAL AND/OR HEALTH INFORMATION	
Authorized by and in accordance with: • The *Health Information Act* (HIA) s.34 • The *Protection of Privacy Act* (POPA) s.13(1)(C) and s.7 of the POPA Regulation • The *Personal Information Protection Act* (PIPA) s.8 • The *Personal Information Protection and Electronic Documents Act* (PIPEDA) s.6.1, Schedule 1(4.3) • The *Privacy Act* s.8	
Client Information:	Full Legal Name:
	Also Known As:
I authorize the following personal and/or health information: (*description of the information)*	
to be disclosed by: (name of organization(s))	
To the organizations listed, and for the purpose(s) outlined on the reverse/following page	
I understand why I have been asked to disclose my individually identifying information, and am aware of the risks and benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent in writing or electronically at any time.	
Effective Date:	Expiry date (valid for 1 year if no date provided)
Signature of client/authorized representative. *	X
*If you are signing as an Authorized Representative on behalf of the client, please provide: Name: _____ Circle Source of Representative's Authority: (HIA s.104 / POPA s.54(1) / PIPA s.61(1)) _____ Relationship to client if confirming to be the nearest relative:	
The information collected on this form is collected for the purposes outlined herein, under the authority of: HIA s.20-22; POPA s.4; PIPA s.; PIPEDA Sched.1, 4.3; Privacy Act s.4. If you have questions about the collection and use of the information on this form, contact < *insert title, business address and phone number*>.	

Page 1/2

The following organizations are working together in an integrated manner to provide *(list the services)*. This approach is intended to *(state the purpose or objectives)*. By signing the consent on the reverse, you are agreeing that the information required can be shared between these organizations if they become involved in assessing and/or providing you with any of these services.
Organization

Instructions for the completion of the *Sample 4* Consent Form:

This Consent Form can be adapted by the following steps.

1. Identify in the Title Section the name of the Integrated Service Delivery.
2. Remove any references to legislation where it is not applicable. For example, if personally identifying information is not going to be collected by or disclosed with a federal government institution, the references to the Privacy Act can be removed.
3. In the "*description of the information"*, list or insert the type of information the consent is meant to authorize disclosure of.
4. In the *"name of organization(s)"*, list or insert the organization or organizations from whom the information is being sought. If the only disclosures or sharing of information will be between the partnering organizations, indicate that.
5. In the table on page 2, list or insert the organizations to whom the information is to be disclosed.
6. In the *"services to be provided"*, on page 2, identify the types of services to be provided through the collaborative approach.
7. In the *"state the purpose or objectives"*, on page 2, identify the purpose behind the collaborative approach and/or what the desired objective(s) is to be achieved through the collaborative approach.
8. In the Collection statement at the end of the form, insert the title, business address and phone number of a staff member who is able to respond to any questions regarding the collection of the information.

Complete the following steps when the client or their representative is present.

1. Insert the date from which the consent is to be effective, and the expiry date.
2. Once the client or their representative has been given Notice, and understands the purpose for which the information identified in the consent form is to be used, ask them to sign. The Notice should indicate that the information is being potentially disclosed to all of the organizations involved in the integrated service delivery, given that they operate as one entity[5]. You may choose to indicate that should any new organizations be added as partners, that will only occur once they have gone through a rigorous onboarding process such that they are able to also operate as a seamless member of the integrated approach.
3. If a legally authorized representative is signing on behalf of the client, ask them to provide evidence of the authority they indicate they are acting under, and indicate what that authority is.
4. If the legally authorized representative indicates they are the client's nearest relative as per the *Personal Directives Act* or the *Mental Health Act*, indicate what their relationship is with the client.
5. If any new organizations are added as partners in the collaborative approach, their names should be added and the client or representative should be asked to initial their consent to disclosure.

[5] This should only be available if the integrated service delivery partners have gone through a rigorous formalization such as by adopting the Information Sharing Framework, and ensuring they are fully committed to the agreed upon purpose, processes and governance structure.