CONVERGE

REIMAGINING CANADA'S MENTAL HEALTH SYSTEMS – TOGETHER.

Ontario Specific Appendices

List of Ontario Specific Appendices for the Information Sharing Framework

This includes the following appendices. The Capacity Assessment contained in Appendix D is screen prints of the actual tool, which is available as an Excel document.

Notes:

Appendix B is in landscape rather than portrait format.

The remaining appendices are contained in the Generally Applicable set, which do not reference or rely on specific jurisdictional legislation.

Appendix G: Capacity Assessment Tool and Companion Guide
Appendix H: Guide to Using the Information Sharing Framework
Appendix I: Security Measures
Appendix J: Additional Resources
Appendix K: Sample Integrated Cluster – Information Stored in Central Repository

Version Control

v.2	Provides corrections on legislative references in Appendices 1, 2.

Appendix A: Applicable Legislation Back

References to legislation are to those listed and cited below. Note that there may be additional legislation that needs to be considered, depending in part on the areas being served.

The following legislation is available at https://www.ontario.ca/Laws

Child, Youth and Family Services Act, 2017
S.O. 2017, CHAPTER 14
ONTARIO REGULATION 191/18
PERSONAL INFORMATION

Connecting Care Act, 2019
S.O. 2019, CHAPTER 5, Schedule 1

Education Act
R.S.O. 1990, CHAPTER E.2

***Freedom of Information and Protection of Privacy Act* (FIPPA)**
R.S.O. 1990, c. F.31
Freedom of Information and Protection of Privacy General Regulation
R.R.O. 1990, Reg. 460
Freedom of Information and Protection of Privacy Data Integration Regulation
O. Reg. 366/19

Integrated Community Health Services Centres Act, 2023
S.O. 2023, chapter 4, Schedule 1

***Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)**
R.S.O. 1990, CHAPTER M.56

Personal Health Information Protection Act, 2004
S.O. 2004, CHAPTER 3
Personal Health Information Protection Act, 2004
ONTARIO REGULATION 329/04

Regulated Health Professions Act, 1991
S.O. 1991, c. 18

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 *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), which could authorize disclosure by the School Board to the health services provider:

- For the purpose it was collected, [s.32(c)]
- With consent, [s.32(b)], or
- in compelling circumstances affecting the health or safety of an individual [s.32(h)]

The *Personal Health Information Protection Act* (PHIPA), which could authorize disclosure by the health services provider to the school board:

- With the consent of the individual the information pertains to [(29)(a)]
- For the purpose of determining or verifying the eligibility of the individual to receive health care or related goods, services or benefits, provided under
  - an Act of Ontario or Canada and funded in whole or in part by the Government of Ontario or Canada,
  - by a local health integration network
  - by a municipality or

- by the Agency,

or to receive coverage with respect to such health care, goods, services or benefits; [s.39(1)(a)]

- if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. [40(1)]
- to assist an institution or a facility in making a decision concerning,
  - arrangements for the provision of health care to the individual; [40 (3)(a)] or
  - the placement of the individual into custody, detention, release, conditional release, discharge or conditional discharge under Part VI of the Child, Youth and Family Services Act, 2017, the Mental Health Act, the Ministry of Correctional Services Act, the Corrections and Conditional Release Act (Canada), Part XX.1 of the Criminal Code (Canada), the Prisons and Reformatories Act (Canada) or the Youth Criminal Justice Act (Canada). [40 (3)(b)].

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) 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 the consent of the individual, [Principle 3, clause 4.3 of Schedule 1]
- 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)]

2. Provincial Public Sector Organizations (Back)

- FIPPA s.1(3) In this section,
  "institution" means,
  (0.a) the Assembly,
  (a) a ministry of the Government of Ontario,
  (a.1) a service provider organization within the meaning of section 17.1 of the Ministry of Government Services Act,
  (a.2) a hospital, and
  (b) any agency, board, commission, corporation or other body designated as an institution in the regulations;

- MFIPPA s. **2** (1) In this Act,
  "institution" means,
  (a) a municipality,
  (b) a school board, municipal service board, city board, transit commission, public library board, board of health, police service board, conservation authority, district social services administration board, local services board, planning board, local roads board, police village or joint committee of management or joint board of management established under the Municipal Act, 2001 or the City of Toronto Act, 2006 or a predecessor of those Acts,
  (c) any agency, board, commission, corporation or other body designated as an institution in the regulations; ("institution")

3. Health Organizations (Back)
   - PHIPA s. 2 In this Act,
     "Agency" means the corporation continued by section 3 of the Connecting Care Act, 2019;

     "health care practitioner" means,
     (a) a person who is a member within the meaning of the Regulated Health Professions Act, 1991 and who provides health care,
     (c) a person who is a member of the Ontario College of Social Workers and Social Service Workers and who provides health care, or
     (d) any other person whose primary function is to provide health care for payment;

     "prescribed organization" means the organization prescribed for the purposes of Part V.1 and, if more than one organization is prescribed, means every applicable prescribed organization;
     "health information custodian" has the meaning set out in section 3;

4. Private Sector Organizations Subject to Provincial/Territorial Legislation (Back)
   Private Sector organizations in Ontario are not generally subject to privacy legislation unless managing personal and health in the course of a commercial activity, in which case the information managed under that activity is subject to PIPEDA; or when managing personal and health information on behalf of an organization that is (e.g. for an institution under a contract or agreement).

   They may also be subject to the Personal Health Information Protection Act if they are deemed a "health care practitioner" as noted under 3 above.

5. Private Sector Organizations Subject to PIPEDA (Back)
   - PIPEDA s. s. 4 (1) This Part applies to every organization in respect of personal information that
     (a) the organization collects, uses or discloses in the course of commercial activities; or
     (b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

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.

8. Collection (Back)
   - FIPPA s.38 (2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

   - MFIPPA s.28 (2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

   - PHIPA – See also Note 11 below.
     s. 29 A health information custodian shall not collect, use or disclose personal health information about an individual unless,
     (a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
     (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act.

   - PIPEDA s. 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
   - PIPEDA Schedule 1, 4.4 Principle 4 — Limiting Collection
     The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

   - 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.
   - FIPPA s.39(2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
     (a) the legal authority for the collection;
     (b) the principal purpose or purposes for which the personal information is intended to be used; and
     (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection. R.S.O. 1990, c. M.56, s. 29 (2).
     (3) Subsection (2) does not apply if,
     (a) the head may refuse to disclose the personal information under subsection 8 (1) or (2) (law enforcement), section 8.1 (Civil Remedies Act, 2001) or section 8.2 (Prohibiting Profiting from Recounting Crimes Act, 2002);
     (b) the Minister waives the notice; or
     (c) the regulations provide that the notice is not required.

- MFIPPA s.29 (2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
  (a) the legal authority for the collection;
  (b) the principal purpose or purposes for which the personal information is intended to be used; and
  (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection. R.S.O. 1990, c. M.56, s. 29 (2).
  (3) Subsection (2) does not apply if,
  (a) the head may refuse to disclose the personal information under subsection 8 (1) or (2) (law enforcement), section 8.1 (Civil Remedies Act, 2001) or section 8.2 (Prohibiting Profiting from Recounting Crimes Act, 2002);
  (b) the Minister waives the notice; or
  (c) the regulations provide that the notice is not required.

- PHIPA s. 16 (1) A health information custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that,
  (a) provides a general description of the custodian's information practices;
  (b) describes how to contact,
  (i) the contact person described in subsection 15 (3), if the custodian has one, or
  (ii) the custodian, if the custodian does not have that contact person;
  (c) describes how an individual may obtain access to or request correction of a record of personal health information about the individual that is in the custody or control of the custodian; and
  (d) describes how to make a complaint to the custodian and to the Commissioner under this Act.
  (2) If a health information custodian uses or discloses personal health information about an individual, without the individual's consent, in a manner that is outside the scope of the custodian's description of its information practices under clause (1) (a), the custodian shall,
  (a) inform the individual of the uses and disclosures at the first reasonable opportunity unless, under section 52, the individual does not have a right of access to a record of the information;
  (b) make a note of the uses and disclosures; and
  (c) keep the note as part of the records of personal health information about the individual that it has in its custody or under its control or in a form that is linked to those records.

- PIPEDA 4.2 Principle 2 — Identifying Purposes
  The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

- 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 (Back)

(6.3.3) refers to Manner of Collection. Relevant legislative provisions may include:

- FIPPA s.39 (1) Personal information shall only be collected by an institution directly from the individual to whom the information relates unless,
  (a) the individual authorizes another manner of collection;
  (b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act;
  (h) another manner of collection is authorized by or under a statute

- MFIPPA s. 29 (1) An institution shall collect personal information only directly from the individual to whom the information relates unless,
  (a) the individual authorizes another manner of collection;
  (b) the personal information may be disclosed to the institution concerned under section 32 or under section 42 of the Freedom of Information and Protection of Privacy Act;
  (h) another manner of collection is authorized by or under a statute.

- PHIPA s. 36 (1) A health information custodian may collect personal health information about an individual indirectly if,
  (a) the individual consents to the collection being made indirectly;
  (b) the information to be collected is reasonably necessary for providing health care or assisting in providing health care to the individual and it is not reasonably possible to collect, directly from the individual,
  (i) personal health information that can reasonably be relied on as accurate and complete, or
  (ii) personal health information in a timely manner;
  (c) the custodian is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act, or is acting as part of such an institution, and the custodian is collecting the information for a purpose related to,
  (i) investigating a breach of an agreement or a contravention or an alleged contravention of the laws of Ontario or Canada,
  (ii) the conduct of a proceeding or a possible proceeding, or
  (iii) the statutory function of the custodian;
  (g) the custodian collects the information from a person who is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to disclose it to the custodian; or
  (h) subject to the requirements and restrictions, if any, that are prescribed, the health information custodian is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to collect the information indirectly.
  (2) A health information custodian may collect personal health information about an individual directly from the individual, even if the individual is incapable of consenting, if the collection is reasonably necessary for the provision of health care and it is not reasonably possible to obtain consent in a timely manner. 2004, c. 3, Sched. A, s. 36 (2).

- PIPEDA s. 7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if
  (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
(e) the collection is made for the purpose of making a disclosure
(i) under subparagraph (3)(c.1)(i) or (d)(ii), or
(ii) that is required by law.

- 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)

- FIPPA s. 41 (1) An institution shall not use personal information in its custody or under its control except,
(a) where the person to whom the information relates has identified that information in particular and consented to its use;
(b) for the purpose for which it was obtained or compiled or for a consistent purpose;
(c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act;

- MFIPPA s. 31 An institution shall not use personal information in its custody or under its control except,
(a) if the person to whom the information relates has identified that information in particular and consented to its use;
(b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
(c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the Freedom of Information and Protection of Privacy Act.

- PHIPA s. 37 (1) A health information custodian may use personal health information about an individual,
(a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual or under clause 36 (1) (b) and the individual expressly instructs otherwise;
(b) for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the custodian;
(c) for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them;

(d) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian;
(e) for educating agents to provide health care;
(f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual;
(g) for the purpose of seeking the individual's consent, or the consent of the individual's substitute decision-maker, when the personal health information used by the custodian for this purpose is limited to the name and contact information of the individual and the name and contact information of the substitute decision-maker, where applicable;
(h) for the purpose of a proceeding or contemplated proceeding in which the custodian or the agent or former agent of the custodian is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding;
(i) for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;
(j) for research conducted by the custodian, subject to subsection (3), unless another clause of this subsection applies; or
(k) subject to the requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada.

- PIPEDA s. 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. See also s. 7(2) **Use without knowledge or consent**

- 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)

- FIPPA s.43 Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose under clauses 41 (1) (b) and 42 (1) (c) only if the individual might reasonably have expected such a use or disclosure.

- MFIPPA s. **33** The purpose of a use or disclosure of personal information that has been collected directly from the individual to whom the information relates is a consistent purpose under clauses 31 (b) and 32 (c) only if the individual might reasonably have expected such a use or disclosure. R.S.O. 1990, c. M.56, s. 33.

- 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
(b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;

- PIPEDA Schedule 1, 4.5 Principle 5 —Limiting Use, Disclosure, and Retention
  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
  4.5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

- 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)

- FIPPA s. **42** (1) An institution shall not disclose personal information in its custody or under its control except,
  (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

- MFIPPA s. **32** An institution shall not disclose personal information in its custody or under its control except,
  (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;

- PHIPA s. 40(1) A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

- 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)

- FIPPA s. 42 (1) An institution shall not disclose personal information in its custody or under its control except,
(b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;
(c) for the purpose for which it was obtained or compiled or for a consistent purpose;
(d) where disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions;
(e) where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada;
(f) where disclosure is by a law enforcement institution,
    (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or
    (ii) to another law enforcement agency in Canada;
(g) to an institution or a law enforcement agency in Canada if,
    (i) the disclosure is to aid in an investigation undertaken by the institution or the agency with a view to a law enforcement proceeding, or
    (ii) there is a reasonable basis to believe that an offence may have been committed and the disclosure is to enable the institution or the agency to determine whether to conduct such an investigation;
(h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

- MFIPPA s. 32 An institution shall not disclose personal information in its custody or under its control except,
(b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
(c) for the purpose for which it was obtained or compiled or for a consistent purpose;
(d) if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions;
(e) where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada;
(f) if disclosure is by a law enforcement institution,
    (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or
    (ii) to another law enforcement agency in Canada;
(g) to an institution or a law enforcement agency in Canada if,
    (i) the disclosure is to aid in an investigation undertaken by the institution or the agency with a view to a law enforcement proceeding, or

(ii) there is a reasonable basis to believe that an offence may have been committed and the disclosure is to enable the institution or the agency to determine whether to conduct such an investigation;

(h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;

(i) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased;

- PHIPA

Disclosures related to providing health care:

38 (1) A health information custodian may disclose personal health information about an individual,

(a) to a health information custodian described in paragraph 1, 3 or 4 of the definition of "health information custodian" in subsection 3 (1), if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, but not if the individual has expressly instructed the custodian not to make the disclosure;

(b) in order for the Minister, another health information custodian or the Agency to determine or provide funding or payment to the custodian for the provision of health care; or

(c) for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or ill and unable to give consent personally.

Disclosures for health or other programs:

39 (1) Subject to the requirements and restrictions, if any, that are prescribed, a health information custodian may disclose personal health information about an individual,

(a) or the purpose of determining or verifying the eligibility of the individual to receive health care or related goods, services or benefits provided under an Act of Ontario or Canada and funded in whole or in part by the Government of Ontario or Canada, by a municipality or by the Agency, or to receive coverage with respect to such health care, goods, services or benefits;

(b) to a person conducting an audit or reviewing an application for accreditation or reviewing an accreditation, if the audit or review relates to services provided by the custodian and the person does not remove any records of personal health information from the custodian's premises;

(c) to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances; or

(d) where,

(i) the disclosure is to another custodian described in paragraph 1, 3 or 4 of the definition of "health information custodian" in subsection 3 (1),

(ii) the individual to whom the information relates is one to whom both the disclosing custodian and recipient custodian provide health care or assist in the provision of health care or have previously provided health care or assisted in the provision of health care, and

(iii) the disclosure is for the purpose of activities to improve or maintain the quality of care provided by the receiving custodian to the individual to whom the information relates or individuals provided with similar health care.

Disclosures related to risks:
40 (1) A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

Disclosures related to care or custody
40 (2) A health information custodian may disclose personal health information about an individual to the head of a penal or other custodial institution in which the individual is being lawfully detained or to the officer in charge of a psychiatric facility within the meaning of the Mental Health Act in which the individual is being lawfully detained for the purposes described in subsection (3).

- PIPEDA s. 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
- 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
  (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
  (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
    (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,
    (iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or
    (iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;
  (d) made on the initiative of the organization to a government institution or a part of a government institution and the organization
    (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
    (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
  (d.1) 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 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;
  (d.3) 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
    (i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,
    (ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and

(iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;
(d.4) 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;
(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;
(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;
(i) required by law.

- PIPEDA Schedule 1, 4.3 Principle 3 - Consent
  The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
  Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual.
- PIPEDA Schedule 1, 4.5 Principle 5 —Limiting Use, Disclosure, and Retention
  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

- 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)

- FIPPA s. 47 (2) Every individual who is given access under subsection (1) to personal information 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 statement of disagreement be attached to the information reflecting any correction that was requested but not made; and
(c) require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement.

- MFIPPA s.36 (2) Every individual who is given access under subsection (1) to personal information is entitled to,
(a) request correction of the personal information if the individual believes there is an error or omission;
(b) require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and
(c) require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement.

- PHIPA s.55 (1) If a health information custodian has granted an individual access to a record of his or her personal health information and if the individual believes that the record is inaccurate or incomplete for the purposes for which the custodian has collected, uses or has used the information, the individual may request in writing that the custodian correct the record.
(2) If the individual makes an oral request that the health information custodian correct the record, nothing in this Part prevents the custodian from making the requested correction.

- PIPEDA Principle 4.9 – Individual Access

4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

- 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)

- FIPPA s. 47 (1) Every individual has a right of access to,
(a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution;

- MFIPPA s.4 (1) Every person has a right of access to a record or a part of a record in the custody or under the control of an institution unless,
(a) the record or the part of the record falls within one of the exemptions under sections 6 to 15; or
(b) the head is of the opinion on reasonable grounds that the request for access is frivolous or vexatious.

- PHIPA s. 52 (1) Subject to this Part, an individual has a right of access to a record of personal health information about the individual that is in the custody or under the control of a health information custodian unless,
(a) the record or the information in the record is subject to a legal privilege that restricts disclosure of the record or the information, as the case may be, to the individual;
(b) another Act, an Act of Canada or a court order prohibits disclosure to the individual of the record or the information in the record in the circumstances;
(c) the information in the record was collected or created primarily in anticipation of or for use in a proceeding, and the proceeding, together with all appeals or processes resulting from it, have not been concluded;
(d) the following conditions are met:
(i) the information was collected or created in the course of an inspection, investigation or similar procedure authorized by law, or undertaken for the purpose of the detection, monitoring or prevention of a person's receiving or attempting to receive a service or benefit, to which the person is not entitled under an Act or a program operated by the Minister, or a payment for such a service or benefit, and

(ii) the inspection, investigation, or similar procedure, together with all proceedings, appeals or processes resulting from them, have not been concluded;

(e) granting the access could reasonably be expected to,

(i) result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to the individual or another person,

(ii) lead to the identification of a person who was required by law to provide information in the record to the custodian, or

(iii) lead to the identification of a person who provided information in the record to the custodian explicitly or implicitly in confidence if the custodian considers it appropriate in the circumstances that the identity of the person be kept confidential; or

(f) the following conditions are met:

(i) the custodian is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act or is acting as part of such an institution, and

(ii) the custodian would refuse to grant access to the part of the record,

(A) under clause 49 (a), (c) or (e) of the Freedom of Information and Protection of Privacy Act, if the request were made under that Act and that Act applied to the record, or

(B) under clause 38 (a) or (c) of the Municipal Freedom of Information and Protection of Privacy Act, if the request were made under that Act and that Act applied to the record.

- PIPEDA 4.9 Principle 9 — Individual Access
  Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.

- 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)

- FIPPA s.40 (1) Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information.
  FIPPA General Regulation: s5. (1) An institution that uses personal information shall retain the information for at least one year after use, except if,
  (a) the individual to whom the information relates consents to its earlier disposal; or
  (b) the information is credit or debit card payment data. O. Reg. 123/15, s. 1.
  (2) Despite subsection (1), an institution that uses personal information that is contained in a telecommunication logger tape in the custody or under the control of the institution shall retain the information for at least 45 days after use, except if the individual to whom the information relates consents to its earlier disposal.

- MFIPPA s. 30 (1) Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information.
  MFIPPA General Regulation: s.5. An institution that uses personal information shall retain it for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, except if,
  (a) the individual to whom the information relates consents to its earlier disposal; or
  (b) the information is credit or debit card payment data.

- PHIPA s. 13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.
  (2) Despite subsection (1), a health information custodian that has custody or control of personal health information that is the subject of a request for access under section 53 shall retain the information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request. 2004, c. 3, Sched. A, s. 13 (2).

- PIPEDA 4.5 Principle 5 —Limiting Use, Disclosure, and Retention
  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
  4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
  4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

- 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)

- FIPPA s. 2 (1) In this Act,
  "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
  (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and

(b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution;

- MFIPPA s. **2** (1) In this Act,
"record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
(b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution; ("document")

- PHIPA s.2
"record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record;

  s. 55.1(1)
  "electronic health record" means the electronic systems that are developed and maintained by the prescribed organization for the purpose of enabling health information custodians to collect, use and disclose personal health information by means of the systems in accordance with this Part and the regulations made under this Part;

- PIPEDA s. 2(1)
'record' includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

- 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)

- FIPPA – This legislation authorizes the collection of information only for the reasons outlined (See Note 9 above) and not through consent. However, the use or disclosure of personal information may be authorized by consent among other reasons.
  41 (1) An institution shall not use personal information in its custody or under its control except,
  (a) where the person to whom the information relates has identified that information in particular and consented to its use;

  42 (1) An institution shall not disclose personal information in its custody or under its control except,

(b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;

- MFIPPA – This legislation authorizes the collection of information only for the reasons outlined (See Note 9 above) and not through consent. However, the use or disclosure of personal information may be authorized by consent among other reasons.

  31 An institution shall not use personal information in its custody or under its control except,

  (a) if the person to whom the information relates has identified that information in particular and consented to its use;

  32 An institution shall not disclose personal information in its custody or under its control except,

  (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;

- PHIPA s. 18 (1) If this Act or any other Act requires the consent of an individual for the collection, use or disclosure of personal health information by a health information custodian, the consent,
  (a) must be a consent of the individual;
  (b) must be knowledgeable;
  (c) must relate to the information; and
  (d) must not be obtained through deception or coercion. 2004, c. 3, Sched. A, s. 18 (1).
  Implied consent
  (2) Subject to subsection (3), a consent to the collection, use or disclosure of personal health information about an individual may be express or implied. 2004, c. 3, Sched. A, s. 18 (2).
  (3) A consent to the disclosure of personal health information about an individual must be express, and not implied, if,
  (a) a health information custodian makes the disclosure to a person that is not a health information custodian; or
  (b) a health information custodian makes the disclosure to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care. 2004, c. 3, Sched. A, s. 18 (3).
  (4) Subsection (3) does not apply to,
  (a) a disclosure pursuant to an implied consent described in subsection 20 (4);
  (b) a disclosure pursuant to clause 32 (1) (b); or
  (c) a prescribed type of disclosure that does not include information about an individual's state of health.

- PIPEDA s. 6.1 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.
  4.3 Principle 3 - Consent
  The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
  4.3.2 The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated

in such a manner that the individual can reasonably understand how the information will be used or disclosed.

- 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).

  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).

  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.

  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 Colleges (Back)

- Regulated Health Professions Act, 1991
  1 (1) In this Act,
  "College" means the College of a health profession or group of health professions established or continued under a health profession Act;
  "health profession" means a health profession set out in Schedule 1;

  36 (1) Every person employed, retained or appointed for the purposes of the administration of this Act, a health profession Act or the Drug and Pharmacies Regulation Act and every member of a Council or committee of a College shall keep confidential all information that comes to his or her knowledge in the course of his or her duties and shall not communicate any information to any other person except,
  (e) to a police officer to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
  (h) where disclosure of the information is required by an Act of the Legislature or an Act of Parliament;
  (i) if there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons;
  (j) with the written consent of the person to whom the information relates;

SCHEDULE 1
SELF GOVERNING HEALTH PROFESSIONS

Health Profession Acts	*Health Profession*
Audiology and Speech-Language Pathology Act, 1991	Audiology and Speech-Language Pathology
Chiropody Act, 1991	Chiropody

Health Profession Acts	*Health Profession*
Chiropractic Act, 1991	Chiropractic
Dental Hygiene Act, 1991	Dental Hygiene
Dental Technology Act, 1991	Dental Technology
Dentistry Act, 1991	Dentistry
Denturism Act, 1991	Denturism
Dietetics Act, 1991	Dietetics
Homeopathy Act, 2007	Homeopathy
Kinesiology Act, 2007	Kinesiology
Massage Therapy Act, 1991	Massage Therapy
Medical Laboratory Technology Act, 1991	Medical Laboratory Technology
Medical Radiation and Imaging Technology Act, 2017	Medical Radiation and Imaging Technology
Medicine Act, 1991	Medicine
Midwifery Act, 1991	Midwifery
Naturopathy Act, 2007	Naturopathy
Nursing Act, 1991	Nursing
Occupational Therapy Act, 1991	Occupational Therapy
Opticianry Act, 1991	Opticianry
Optometry Act, 1991	Optometry
Pharmacy Act, 1991	Pharmacy
Physiotherapy Act, 1991	Physiotherapy
Psychology and Applied Behaviour Analysis Act, 2021	Psychology and applied behaviour analysis
Psychotherapy Act, 2007	Psychotherapy
Respiratory Therapy Act, 1991	Respiratory Therapy
Traditional Chinese Medicine Act, 2006	Traditional Chinese Medicine

21. Security of Information (Back)

- FIPPA s.10.1 Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution.
  FIPPA General Regulation: s.4. (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 460, s. 4 (1).

- MFIPPA s.4.1 Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution.
  MFIPPA General Regulation: s.3. (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 823, s. 3 (1).
  (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 823, s. 3 (3).

- PHIPA s.12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure

that the records containing the information are protected against unauthorized copying, modification or disposal.

- PIPEDA 4.7 Principle 7 — Safeguards
  Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
  4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
  4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.
  4.7.3 The methods of protection should include
  (a) physical measures, for example, locked filing cabinets and restricted access to offices;
  (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
  (c) technological measures, for example, the use of passwords and encryption.
  4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
  4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

22. Breaches (Back)

- FIPPA s.40.1 (1) The head of an institution shall report to the Commissioner any theft, loss or unauthorized use or disclosure of personal information in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is real risk that a significant harm to an individual would result or if any other prescribed circumstances exist.

- PHIPA s.12 (2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
  (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
  (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.
  (3) If the circumstances surrounding a theft, loss or unauthorized use or disclosure referred to in subsection (2) meet the prescribed requirements, the health information custodian shall notify the Commissioner of the theft or loss or of the unauthorized use or disclosure.

- PIPEDA s. 10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.
(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.
(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.
(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred. (7) For the purpose of this section, significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.
(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include
(a) the sensitivity of the personal information involved in the breach;
(b) the probability that the personal information has been, is being or will be misused; and
(c) any other prescribed factor.
2015, c. 32, s. 10

23. Evaluation (Back)

- FIPPA The following section is contained in Part III.1, Data Integration, which authorizes the collection, use and disclosure by "extra-ministerial data integration units".
  49.2 The purpose of the collection of personal information under this Part is to compile information, including statistical information, to enable analysis in relation to,
  (a) the management or allocation of resources;
  (b) the planning for the delivery of programs and services provided or funded by the Government of Ontario, including services provided or funded in whole or in part or directly or indirectly; and
  (c) the evaluation of those programs and services. 2019, c. 7, Sched. 31, s. 6.

24. Research (Back)

- FIPPA s. 21 (1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,
  (e) for a research purpose if,
  (i) the disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained,
  (ii) the research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form, and
  (iii) the person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations;

- MFIPPA s. 14 (1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,
  (e) for a research purpose if,
  (i) the disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained,
  (ii) the research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form, and
  (iii) the person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations;
  See also MFIPPA General Regulation s.10

- PHIPA s. 44 (1) A health information custodian may disclose personal health information about an individual to a researcher if the researcher,
  (a) submits to the custodian,
  (i) an application in writing,
  (ii) a research plan that meets the requirements of subsection (2), and
  (iii) a copy of the decision of a research ethics board that approves the research plan; and
  (b) enters into the agreement required by subsection (5).

- 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 13, section 8

Appendix B: Ontario Privacy Legislation Disclosure Matrix

Back

The following legislative provisions are extracts from the various privacy legislations that apply in Ontario. 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, use, and 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 that collaborating organizations determine what information is required to enable the services being delivered through the collaborative approach, 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 that collaborative approach.

Notes:

Organizations working collaboratively that intend to share information need to determine what specific provisions would apply to the circumstances within which they provide supports or services. 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.

The introduction of the Connecting Care Act, 2019 has facilitated the ability for organizations that are registered and named therein to work collaboratively, including sharing information between them, such as those identified under the Ontario Health Teams. In addition, there is capacity for organizations to collaborate even if not working under that particular Act, in compliance with and through the authorities identified under the legislation listed below.

Listed Legislation:

APPLICABLE PROVINCIAL LEGISLATION

Freedom of Information and Protection of Privacy Act (FIPPA)

Collection under FIPPA:

Who (Organization)	Can Collect What Information	Comments
Institutions under FIPPA, (Includes provincial ministries, service provider organizations as per the *Ministry of Government Services Act*, hospitals, ...)	No person shall collect personal information on behalf of an institution unless the collection is:	Note: Personal information must be collected directly from the individual unless otherwise authorized as per section 39(1).
	• expressly authorized by statute,	• recognizes the legitimacy of other legislation where that legislation authorizes the collection.
	• used for the purposes of law enforcement or	• recognizes the collection of information for law enforcement purposes. Note that law enforcement is defined to mean policing, investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or the conduct of proceedings referred above.
	• necessary to the proper administration of a lawfully authorized activity. [38 (2)]	• "Necessary to administer a lawfully authorized activity" refers to instances where institutions need to collect personal information in order to deliver a service or program that is authorized by the government. For provincial ministries, authorization may include legislation, regulations or orders-in-council."[1]

[1] Taken from: Chapter 7: Privacy Fundamentals | Freedom of Information and Protection of Privacy Manual | ontario.ca

Use under FIPPA:

Who (Organization)	Can Use What Information	Comments
Institutions under FIPPA, (Includes provincial ministries, service provider organizations as per the *Ministry of Government Services Act*, hospitals.)	An institution shall not use personal information in its custody or under its control except,	Use should be limited to those authorized and required to use the information as part of their area of responsibility.
	• where the person to whom the information relates has identified that information in particular and consented to its use; [41(1)(a)]	• Individuals can provide consent for a specific use of their information. Use of their information is restricted to the stated purpose(s). Generally, consents should be in writing, subject to certain exceptions.
	• for the purpose for which it was obtained or compiled or for a consistent purpose; [41(1)(b)]	• 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 a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*; [41(1)(c)] (See below)	• Supports the disclosure and use of information as a two-way process. Authority to disclose information needs to be matched by the authority to collect and use information by the receiving party.

Disclosure under FIPPA:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under FIPPA, (Includes provincial ministries, service provider organizations as per the *Ministry of*	An institution shall not disclose personal information in its custody or under its control except:		This section outlines specific circumstances under which personal information may be disclosed.
	• where the person to whom the information relates has identified that	• to any person or staff of an organization	• Supports the individual having some control over who can access their

Who (Organization)	Can Disclose What Information	To Whom	Comments
Government Services Act, hospitals.)	information in particular and consented to its disclosure; [42(1)(b)]	identified in the consent responsible for the purposes for which consent was given.	information. Generally, the consent should name an organization rather than an employee within it. Disclosure is not limited to institutions.
	• for the purpose for which it was obtained or compiled or for a consistent purpose, [42(1)(c)]	• to whomever is authorized and requires the information as part of their area of responsibility.	• May apply to staff beyond those delivering the specific program. (e.g. may include staff responsible for administrative support, data analysis, etc.)
	• where disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions; [42(1)(d)]	• to any employee of the institution 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.) This disclosure is limited to staff (including agents) of the organization.
	• where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada; [42(1)(e)]	• to any person responsible for or identified within the named organization.	• Includes both a 'permitted', i.e. can respond and 'required', i.e. must respond, depending on the enactment's wording.
	• to an institution or a law enforcement agency in Canada if, (i) the disclosure is to aid in an investigation undertaken by the institution or the agency with a view to a law enforcement proceeding, or (ii) there is a reasonable basis to believe that an offence may have been committed and the disclosure is	• to any institution, 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 an institution as well as to a law enforcement agency that may require it for an investigation and proceeding. It would not be unreasonable to ask for some information to support that a proceeding, investigation, or reasonable basis for such is underway from the requestor, to validate their authority.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under FIPPA	to enable the institution or the agency to determine whether to conduct such an investigation; [42(1)(g)]		
	• where disclosure is by a law enforcement institution, (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or (ii) to another law enforcement agency in Canada; [42(1)(f)]	• to any law enforcement agency in Canada and outside of Canada, as identified under the covering document.	• Authorizes disclosure of information between a law enforcement institution to other law enforcement agencies.
	• in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates; [42(1)(h)]	• to any person who may be involved in addressing the risk to the health and safety of an individual.	• Institutions relying on this should be prepared to provide rationale/argument of the potential for risk. This provision can be in response to, or despite there not being, a request for information. Where a request is made, there may be a need to provide the institution with information to assist in their decision making. The provision also requires for notice to be provided to the individual to whom the information pertains, once the disclosure has been made.
	• in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased; [42(1)(i)]	• to either party	• Limited to the information required to facilitate the contact between the parties. There may be occasion where information of one party is provided to the other party who can then decide whether or not to make contact.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under FIPPA	Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public. [11 (1)]	• to the appropriate member or members of the public, dependent on the circumstances and focus of the hazard or risk.	• Requires the disclosure of a record or records, (including those containing personal information if appropriate), where there is a significant risk (grave hazard) and where the disclosure is in the public interest. It also requires notice be provided to the person the information is about, in advance if practicable.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA (Back)

Collection under MFIPPA:

Who (Organization)	Can Collect What Information	Comments
Institutions under MFIPPA, (applies to local government institutions in Ontario, including municipalities, police service boards, school boards, conservation authorities, boards of health and transit commissions.)	No person shall collect personal information on behalf of an institution unless the collection is	Note: Personal information must be collected directly from the individual unless otherwise authorized as per section 39(1).
	• expressly authorized by statute,	• recognizes the legitimacy of other legislation where that legislation authorizes the collection.
	• used for the purposes of law enforcement or	• recognizes the collection of information for law enforcement purposes. Note that law enforcement is defined to mean policing, investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or the conduct of proceedings referred above.
	• necessary to the proper administration of a lawfully authorized activity. [28(2)]	• "Necessary to administer a lawfully authorized activity" refers to instances where local

Who (Organization)	Can Collect What Information	Comments
Institutions under MFIPPA		government institutions need to collect personal information in order to deliver a service or program that is authorized by the institution. For municipal institutions, authorization may include statute, by-law or regulation."[2]

Use under MFIPPA:

Who (Organization)	Can Use What Information	Comments
Institutions under MFIPPA, (applies to local government institutions in Ontario, including municipalities, police service boards, school boards, conservation authorities, boards of health and transit commissions.)	An institution shall not use personal information in its custody or under its control except,	Use should be limited to those authorized and required to use the information as part of their area of responsibility.
	• if the person to whom the information relates has identified that information in particular and consented to its use; [s.31(a)]	• Individuals can provide consent for a specific use of their information. Use of their information is restricted to the stated purpose(s). Generally, consents should be in writing, subject to certain exceptions.
	• for the purpose for which it was obtained or compiled or for a consistent purpose; or [s.31(b)]	• 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 a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the Freedom of Information and Protection of Privacy Act. [s.31(c)]	• Supports the disclosure and use of information as a two-way process. Authority to disclose information needs to be matched by the authority to collect and use information by the receiving party.

[2] Taken from: Chapter 7: Privacy Fundamentals | Freedom of Information and Protection of Privacy Manual | ontario.ca

Disclosure under MFIPPA:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under MFIPPA, (applies to local government institutions in Ontario, including municipalities, police service boards, school boards, conservation authorities, boards of health and transit commissions.)	An institution shall not disclose personal information in its custody or under its control except,		This provision outlines specific circumstances for the disclosure of personal information.
	• if the person to whom the information relates has identified that information in particular and consented to its disclosure; [32(b)]	• 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 should name an organization rather than an employee within it. Disclosure is not limited to institutions.
	• for the purpose for which it was obtained or compiled or for a consistent purpose; [32(c)]	• to whomever is authorized and requires the information as part of their area of responsibility.	• May apply to staff beyond those delivering the specific program. (e.g. may include staff responsible for administrative support, data analysis, etc.)
	• if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions; [32(d)]	• to any employee of the named organization 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.) This disclosure is limited to staff (including agents) of the organization.
	• where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada; [32(e)]	• to any person responsible for or identified within the referenced document.	• Includes both a 'permitted',(i.e. can respond) and 'required', (i.e. must respond), depending on the wording.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under MFIPPA	• if disclosure is by a law enforcement institution, (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or (ii) to another law enforcement agency in Canada; [32(f)]	• to any law enforcement agency in Canada and outside of Canada, as identified under the covering document.	• Authorizes disclosure of information between a law enforcement institution to other law enforcement agencies.
	• to an institution or a law enforcement agency in Canada if, (i) the disclosure is to aid in an investigation undertaken by the institution or the agency with a view to a law enforcement proceeding, or (ii) there is a reasonable basis to believe that an offence may have been committed and the disclosure is to enable the institution or the agency to determine whether to conduct such an investigation; [32(g)]	• to any institution, 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 an institution as well as to a law enforcement agency that may require it for an investigation and proceeding. It would not be unreasonable to ask for some information to support that a proceeding, investigation, or reasonable basis for such is underway from the requestor, to validate their authority.
	• in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates; [32(h)]	• to any person who may be involved in addressing the risk to the health and safety of an individual.	• Institutions relying on this should be prepared to provide rationale/argument of the potential for risk. This provision can be in response to, or despite there not being, a request for information. Where a request is made, there may be a need to provide the institution with information to assist in their decision making. This also requires notice to be provided to the individual to whom the information pertains, once the disclosure's made.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Institutions under MFIPPA	• in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased; [32(i)]	• to either party.	• Limited to the information required to facilitate the contact between the parties. There may be occasion where information of one party is provided to the other party who can then decide whether or not to make contact.
	Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public. [5 (1)]	• to the appropriate member or members of the public, dependent on the circumstances and focus of the hazard or risk.	• Requires the disclosure of a record or records, (including those containing personal information if appropriate), where there is a significant risk (grave hazard) and where the disclosure is in the public interest. It also requires notice be provided to the person the information is about, in advance if practicable.

Personal Health Information Protection Act (PHIPA) (Back)

Generally under PHIPA:

Who (Organization)	Collection, Use, and Disclosure	Comments
Health Information Custodians as identified in the Act (Includes those working on their behalf, defined as 'agents'.)	A health information custodian shall not collect, use or disclose personal health information about an individual unless, • it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; [29(a)]or • the collection, use or disclosure, as the case may be, is permitted or required by this Act. [29(b)]	Sets out limitations on the collection, use, or disclosure to that required for the stated purpose(s). • Requires consent and there must be legal authority for the collection, use, or disclosure. • Recognizes there are specific authorities for the collection, use, and disclosure without consent.

Who (Organization)	Collection, Use, and Disclosure	Comments
Health Information Custodians as identified in the Act	A health information custodian shall not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure. [s. 30 (1)]	• Restricts the collection, use, or disclosure of personal information if other information will suffice (presumably non-identifying information).
	A health information custodian shall not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be. [s. 30 (2)]	• Limits the collection, use, or disclosure of personal information to that which is required for the identified purposes(s).
	This section does not apply to personal health information that a health information custodian is required by law to collect, use or disclose. [30 (3)]	• Recognizes there may be legal requirements for the custodian to collect, use, or disclose personal health information.

Collection under PHIPA:

Who (Organization)	Can Collect What Information	Comments
Health Information Custodians as identified in the Act (Includes those working on their behalf, defined as 'agents'.)	A health information custodian may collect personal health information about an individual indirectly if,	• Sets out various authorities for the indirect collection of personal health information.
	• the individual consents to the collection being made indirectly; [36(1)(a)]	• This speaks only to consent for indirect collection. Authority must exist separately for the collection.
	• the information to be collected is reasonably necessary for providing health care or assisting in providing health care to the individual and it is not reasonably possible to collect, directly from the individual, (i) personal health information that can reasonably be relied on as accurate and complete, or	• Authorizes indirect collection without consent, limited to that which is reasonably required, and the ability to collect directly is not possible from the perspective of the collecting entity.

Who (Organization)	Can Collect What Information	Comments
Health Information Custodians as identified in the Act	(ii) personal health information in a timely manner; [36(1)(b)]	
	• the custodian is an institution within the meaning of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act, or is acting as part of such an institution, and the custodian is collecting the information for a purpose related to, (iii) the statutory function of the custodian; [36(1)(c)]	• Authorizes the indirect collection of personal health information without consent, by an institution under FIPPA or MFIPPA where required for a legislated purpose(s).
	• the custodian collects the information from a person who is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to disclose it to the custodian; [36(1)(g)] or	• Recognizes there may be legislated authorities that permit or require indirect disclosure without consent, to a custodian by another organization.
	• subject to the requirements and restrictions, if any, that are prescribed, the health information custodian is permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada to collect the information indirectly [36(1)(h)]	• Recognizes there may be legislated authorities that permit or require a custodian to collect personal health information indirectly without consent.
	A health information custodian may collect personal health information about an individual directly from the individual, even if the individual is incapable of consenting, if the collection is reasonably necessary for the provision of health care and it is not reasonably possible to obtain consent in a timely manner. [36(2)]	• Authorizes the direct collection of information without consent if required, and the ability to obtain consent is not likely in a timely way.

Use under PHIPA:

Who (Organization)	Can Use What Information	Comments
Health Information Custodians as identified in the Act (Includes those working on their behalf, defined as 'agents'.)	A health information custodian may use personal health information about an individual,	• Sets out various authorities for the use of personal health information.
	• for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual or under clause 36 (1) (b) and the individual expressly instructs otherwise; [37 (1)(a)]	• Allows the use of personal and health information for the stated purpose(s), subject to any restrictions imposed through consent if consent was provided for the use.
	• for a purpose for which this Act, another Act or an Act of Canada permits or requires a person to disclose it to the custodian; [37(1)(b)]	• Supports the disclosure and use of information as a two-way process. Authority to disclose information needs to be matched by the authority to collect and use information by the receiving party.
	• for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them; [37(1)(c)]	• Recognizes the legitimate use of information, and ties the use to the stated and consistent purpose(s).
	• subject to the requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada. [37 (1)(k)]	• Allows the use of personal health information if required by legislation, subject to any identified requirements.

Disclosure under PHIPA :

Who (Organization)	Can Disclose What Information	To Whom	Comments
Health Information Custodians as identified in the Act (Includes those working on their behalf, defined as 'agents'.)	A health information custodian shall not … disclose personal health information about an individual unless it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; [(29)(a)]	To any person/entity and for the purpose(s) identified in the consent.	This circumstance authorizes disclosure with consent of the individual to whom it pertains.
	A health information custodian may disclose personal health information about an individual,		The circumstances listed here authorize disclosure without consent.
	• to a health information custodian described in paragraph 1, 2 or 4 of the definition of "health information custodian" in subsection 3 (1), if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, but not if the individual has expressly instructed the custodian not to make the disclosure; [38(1)]	• to health care practitioners, or those custodians who operate facilities, programs or services, including a centre, program or service for community health or mental health whose primary purpose is the provision of health care, (or their agents).	• This provision allows for the disclosure of health information without consent, to provide health care when consent is not easily obtained, and no express wish to not disclose exist.
	Subject to the requirements and restrictions, if any, that are prescribed, a health information custodian may disclose personal health information about an individual,		
	• for the purpose of determining or verifying the eligibility of the individual to receive health care or	• to the staff responsible for determining eligibility for those	• This may include goods, services or benefits that may not be direct health care, but are related in some manner,

Who (Organization)	Can Disclose What Information	To Whom	Comments
Health Information Custodians as identified in the Act	related goods, services or benefits provided under ○ an Act of Ontario or Canada and funded in whole or in part by the Government of Ontario or Canada, ○ by a local health integration network ○ by a municipality or ○ by the Agency, or to receive coverage with respect to such health care, goods, services or benefits; [39(1)(a)]	goods, services, or benefits delivered, or to receive such coverage: ○ by an entity identified under an Act, ○ by a local health integration network, ○ by a municipality, or ○ by the Agency	such as those identified as social determinants of health, where there is a relationship to the health of the individual. • "Agency" refers to the corporation as identified under the *Connecting Care Act, 2019* • "Local health integration network" is not defined, and may therefore include health service providers and Ontario Health Teams as defined in the *Connecting Care Act, 2019*
	• where, (i) the disclosure is to another custodian described in paragraph 1, 2 or 4 of the definition of "health information custodian" in subsection 3 (1), (ii) the individual to whom the information relates is one to whom both the disclosing custodian and recipient custodian provide health care or assist in the provision of health care or have previously provided health care or assisted in the provision of health care, and (iii) the disclosure is for the purpose of activities to improve or maintain the quality of care provided by the receiving custodian to the individual to whom the information relates or	• to health care practitioners, or those custodians who operate facilities, programs or services, including a centre, program or service for community health or mental health whose primary purpose is the provision of health care, (or their agents).	• This provision allows for the disclosure of involved custodians to improve or maintain the quality of care for an individual they have been or are involved with.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Health Information Custodians as identified in the Act	individuals provided with similar health care. [39(1)(d)]		
	• A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. [40(1)]	• to any person who may be involved in addressing the risk of serious bodily harm to any person	• Organizations approaching custodians for this disclosure, or custodians acting on their own should be prepared to provide rationale/argument of the risk. Additional information may be required to assist in the decision making.
	• A health information custodian may disclose personal health information about an individual to the head of a penal or other custodial institution in which the individual is being lawfully detained or to the officer in charge of a psychiatric facility within the meaning of the Mental Health Act in which the individual is being lawfully detained for the purposes described in subsection (3). [40(2)].	• to the head of the penal or custodial institution, or to the person in charge of a psychiatric facility as defined.	• Allows for disclosure to maintain or support the health of an individual under the care of one of the identified organizations.
	• A health information custodian may disclose personal health information about an individual under subsection (2) to assist an institution or a facility in making a decision concerning, ○ arrangements for the provision of health care to the individual; [40 (3)(a)] or	• see above	• This provision outlines the type of circumstances for which the health information may be disclosed, including not only the provision of health care, but as well can be provided for the purposes of discharge planning.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Health Information Custodians as identified in the Act	○ the placement of the individual into custody, detention, release, conditional release, discharge or conditional discharge under Part VI of the Child, Youth and Family Services Act, 2017, the Mental Health Act, the Ministry of Correctional Services Act, the Corrections and Conditional Release Act (Canada), Part XX.1 of the Criminal Code (Canada), the Prisons and Reformatories Act (Canada) or the Youth Criminal Justice Act (Canada). [40 (3)(b)]. • Section 49	• applies to non-custodians and custodians to whom health information was disclosed.	• Limits the use of any disclosed health information by the recipient non-custodian or custodian to the purpose(s) for which the information was disclosed.

Child, Youth and Family Services Act	(Back)
Service providers as defined in the Act, including the Minister, a licensee, a person or entity including a society that provides a service funded under this Act, or a prescribed person or entity.	A service provider shall not collect personal information about an individual for the purpose of providing a service or use or disclose that information unless, (a) the service provider has the individual's consent under this Act and the collection, use or disclosure, to the best of the service provider's knowledge, is necessary for a lawful purpose; or (b) the collection, use or disclosure without the individual's consent is permitted or required by this Act. [286]

Collection under the CYFSA:

Who (Organization)	Can Collect What Information	Comments
Service providers as defined in the Act, including the Minister, a licensee, a person or entity including a society that provides a service funded under this Act, or a prescribed person or entity.	**Indirect Collection** A service provider may collect personal information indirectly for the purpose of providing a service if the individual to whom the information relates consents to the collection being made indirectly. [288 (1)]	Allows for the service provider to collect personal information with consent of the individual to whom the information pertains.
	Without consent A service provider may collect personal information indirectly for the purpose of providing a service and without the consent of the individual to whom the information relates if,	The listed provisions allow the service provider to collect personal information without consent.

	• the information to be collected is reasonably necessary to provide a service or to assess, reduce or eliminate a risk of serious harm to a person or group of persons and it is not reasonably possible to collect personal information directly from the individual,
	  • that can reasonably be relied on as accurate and complete, or
	  • in a timely manner; [288 (2)(a)]
		• Allows for the collection of personal information to provide a service or to reduce a risk of harm to any person(s), and direct collection is not reasonably possible.

	• the information is to be collected by a society from another society or from a child welfare authority outside of Ontario and the information is reasonably necessary to assess, reduce or eliminate a risk of harm to a child; [288 (2)(b)]	• Allows a society to collect personal information from another society or a child welfare authority outside of the province where it is required to manage a risk of harm to a child.
	• the information is to be collected by a society and the information is reasonably necessary for a prescribed purpose related to a society's functions under subsection 35 (1); [288 (2)(c)]	• Allows a society to collect personal information where it is required to provide the services mandated in the legislation.

Who (Organization)	Can Collect What Information	Comments
Service providers as defined in the Act	**Direct collection without consent** A service provider may collect personal information directly from the individual to whom the information relates, even if the individual is not capable, if, • the collection is reasonably necessary for the provision of a service and it is not reasonably possible to obtain consent in a timely manner; [289(a)] • the collection is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons; [289(b)]or • the service provider is a society and the information is reasonably necessary to assess, reduce or eliminate a risk of harm to a child. [289(c)] Where a service provider collects personal information directly from an individual, the service provider shall give the individual notice that the information may be used or disclosed in accordance with this Part. [290]	• Allows a service provider to collect information directly without consent if the information is needed to provide a service, • Allows a service provider to collect information directly without consent if the information is needed to assess, reduce or eliminate a risk of harm to a person or persons. • Allows a service provider to collect information directly without consent if the information is needed to assess, reduce or eliminate a risk of harm to a child. When relying on these provisions, the person to whom the information must be provided with a notice about the use or disclosure.

Use under the CYFSA:

Who (Organization)	Can Use What Information	Comments
Service providers as defined in the Act, including the Minister, a licensee, a person or entity including a society that provides a service funded	A service provider may use personal information collected for the purpose of providing a service, • for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, including providing the information to	• Allows the service provider to use information for the purpose(s) it was collected for. Despite an instruction by the individual to not use information in providing consent, the service

Who (Organization)	Can Use What Information	Comments
under this Act, or a prescribed person or entity.	an officer, employee, consultant or agent of the service provider, but not if the information was collected with the consent of the individual or under clause 288 (2) (a) and the individual expressly instructs otherwise; [291(a)]	provider may use the information to deliver the services outlined in section 35, or where there is a risk of harm to a child or a person(s).
	• if the service provider believes on reasonable grounds that the use is reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons; [291(b)]	• Allows the service provider to use information to assess, reduce, or eliminate risk.
	• for planning, managing or delivering services that the service provider provides or funds, in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them; [291(d)]	• Allows the service provider to use information for managing or delivering services that it provides or funds
	• for the purpose of activities to improve or maintain the quality of a service. [291(f)]	• Allows the service provider to use information for evaluating the services.

Disclosure under the CYFSA:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Service providers as defined in the Act, including the Minister, a licensee, a person or entity including a society that provides a service funded	A service provider may, without the consent of the individual, disclose personal information about an individual that has been collected for the purpose of providing a service, • to a law enforcement agency in Canada to aid an investigation undertaken with a view to a law	• to staff of any law enforcement agency authorized in Canada.	These provisions relate to the personal information of an individual that has been collected to provide a service. The legislation does not restrict such information to that of the individual receiving the service. • recognizes the disclosure of information for law enforcement purposes. Law enforcement is not defined, so could

Who (Organization)	Can Disclose What Information	To Whom	Comments
under this Act, or a prescribed person or entity.	enforcement proceeding or to allow the agency to determine whether to undertake such an investigation; [292(1)(a)]		include policing, investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings.
	• for the purpose of contacting a relative, member of the extended family, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or otherwise not capable; [292(1)(d)]	• to any identified relative, extended family member, friend, or substitute decision maker who may need to be contacted.	• Allows the service provider to provide necessary personal information of an individual where they do not have the ability to make the decision. There must be a need to contact someone on the individual's behalf.
	• subject to section 294, for the purpose of complying with, (i) a summons, order or similar requirement issued in a proceeding by a person having jurisdiction to compel the production of information, or (ii) a procedural rule that relates to the production of information in a proceeding; [292(1)(f)]	• to whomever has the requirement for the information as identified in the summons, order or other relevant document/rule.	• Allows the service provider to provide information as outlined in the requesting documents or rule. Where the service provider does not intend to disclose the identified information, they would need to object through whatever means are identified. (e.g. courts)
	• if the service provider believes on reasonable grounds that the disclosure is necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons; [292(1)(g)] or	• To any person who should be involved in the assessment, reduction, or elimination of risk of harm.	• Allows the service provider to disclose personal information where it is required for the purpose of managing or addressing a potential risk of serious harm to any person.
	• if permitted or required by law or by a treaty, agreement or arrangement	• To any person identified in the law,	• Allows the service provider to disclose personal information where legislation

Who (Organization)	Can Disclose What Information	To Whom	Comments
Service providers as defined in the Act	made under an Act or an Act of Canada, subject to the requirements and restrictions, if any, that are prescribed. [292(1)(h)]	treaty, agreement, or arrangement, subject to requirements and restrictions that may exist.	authorizes or requires the disclosure. This section may be subject to a broad interpretation.

Connecting Care Act	(Back)
Outlines the intent for the delivery of an integrated health care system based in the community, among other areas of focus; establishes the Ontario Health Teams as an authorized entity; and recognizes that Indigenous peoples have a role in the planning and delivery of health services in their communities. The Act also defines 'health service providers' to mean: • The Service Organization. • A person or entity that operates a hospital within the meaning of the Public Hospitals Act or a private hospital within the meaning of the Private Hospitals Act. • A person or entity that operates a psychiatric facility within the meaning of the Mental Health Act except if the facility is, i. a correctional institution operated or maintained by a member of the Executive Council, other than the Minister, or ii. a prison or penitentiary operated or maintained by the Government of Canada. • The University of Ottawa Heart Institute/Institut de cardiologie de l'Université d'Ottawa. • A licensee within the meaning of the Fixing Long-Term Care Act, 2021, other than a municipality or board of management described in paragraph 5. • A municipality or board of management that maintains a long-term care home under Part IX of the Fixing Long-Term Care Act, 2021. • A not-for-profit entity that provides **home and community care** services. • A not-for-profit entity that operates a community health centre. • A not-for-profit entity that provides community mental health and addiction services. • A not-for-profit entity that operates a family health team. • A not-for-profit entity that operates a nurse practitioner-led clinic.	• The service organization has been designated as "Ontario Health atHome" • "**home and community care services**" are defined in the Regulations to include Professional services, Personal support services, Homemaking

Connecting Care Act (Back)	
• A not-for-profit entity that operates an Aboriginal health access centre. • A person or entity that provides primary care nursing services, maternal care or inter-professional primary care programs and services. • A not-for-profit entity that provides palliative care services, including a hospice. • A person or entity that provides physiotherapy services in a clinic setting that is not otherwise a health service provider. • An integrated community health services centre within the meaning of the Integrated Community Health Services Centres Act, 2023. • Any other person or entity or class of persons or entities that is prescribed. [1(2)]	services, Community support services, Indigenous services, Care co-ordination services, Home and community care services that include residential accommodation.
The Minister may, subject to any terms and conditions that the Minister determines, designate as an Ontario Health Team a person or entity, or a group of persons or entities, that has the ability to deliver, in an integrated and co-ordinated manner, at least three of the following types of services, or such higher number of types of services as may be prescribed: 1. Hospital services. 2. Primary care services. 3. Mental health or addictions services. 4. Home and community care services. 5. Long-term care home services. 6. Palliative care services. 7. Any other prescribed health care service or non-health service that supports the provision of health care services. [29 (1)]	• The regulations contain a fairly extensive list of services that fall under the health care services, and the non-health services. See "Ontario Regulation 187/22 Home and Community Care Services"

Regulated Health Professions Act (Back)

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Members of a College listed under	36 (1) Every person employed, retained or appointed for the		•

Who (Organization)	Can Disclose What Information	To Whom	Comments
the Act (includes the following College: Physicians and Surgeons, Nurses, Psychologists and Behaviour Analysts,	purposes of the administration of this Act, a health profession Act or the Drug and Pharmacies Regulation Act and every member of a Council or committee of a College shall keep confidential all information that comes to his or her knowledge in the course of his or her duties and shall not communicate any information to any other person except, • (e) to a police officer to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result; • (h) where disclosure of the information is required by an Act of the Legislature or an Act of Parliament; • (i) if there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons; • (j) with the written consent of the person to whom the information relates;	• As stated, to a police officer • To whomever is identified or authorized under the legislation being referenced • To whomever is appropriately involved in eliminating or reducing the risk • To whomever the person has indicated in their written consent	

APPLICABLE FEDERAL LEGISLATION

Privacy Act (Federal)	(Back)

Collection under the federal Privacy Act:

Who (Organization)	Can Collect What Information	Comments
Federal institutions including GoC departments, ministries, bodies or offices listed in the schedule, and Crown corporations.	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 provision provides authority for the institution to collect information for any purpose identified as a program or activity of that organization. Institutions include any department or ministry of the federal government, body or office listed in the schedule, and any parent Crown corporation, including any wholly owned subsidiary.

Use under the federal Privacy Act:

Who (Organization)	Can Use What Information	Comments
Federal institutions including GoC departments, ministries, bodies or offices listed in the schedule, and Crown corporations.	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 under the federal Privacy Act:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federal institutions including GoC departments, ministries, bodies or offices listed in the schedule, and Crown corporations.	**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.
	• to an investigative body specified in the regulations, on the written		

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federal institutions	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)
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. [4.3 Principle 3 – Consent]	A set of principles form part of the Act, and are contained in Schedule 1. Organizations subject to the Act should ensure they are familiar with the applicable sections. Principle 3 deals with consent.

Collection under the Personal Information Protection and Electronic Documents Act:

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.	Personal Information of the individual can be collected • with the consent of the individual, [Principle 3, clause 4.3 of Schedule 1]	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."
	Personal information may be collected by an organization without the knowledge or consent of the individual only if • the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way; [(7(1)(a)]	The provisions listed here allow for the organization to collect personal information without the consent of the individual to whom it pertains. • Allows the organization to collect personal information if it determines that doing so is in the best interests of the individual. Doing so should be carefully considered.
	• it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; [(7(1)(b)]	• Allows the organization to collect information for the purpose(s) of investigating any contravention of laws. This would likely be deemed to be limited to the collection by that organization if it fits within their mandate or role.

Who (Organization)	Can Collect What Information	Comments
Federally Regulated Organizations and Private Sector Organizations	• the collection is made for the purpose of making a disclosure (ii) that is required by law. [(7(1)(e)]	• Allows the organization to collect information for the purpose(s) of disclosing it where it is required to do so by law. This should likely be supported by evidence that doing so fits within their mandate or role.

Use under the Personal Information Protection and Electronic Documents 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]	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."
	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 committed, and the information is used for the purpose of investigating that contravention; [7(2)(a)]	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.
	• 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)]	• Allows the organization to use information to address any situations where there is a potential or active risk to the health or safety.

Who (Organization)	Can Use What Information	Comments
Federally Regulated Organizations and Private Sector Organizations	• it was collected under paragraph (1)(a), (b) or (e). [7(2)(d)]	• 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 under the Personal Information Protection and Electronic Documents Act:

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.	Personal Information of the individual may be disclosed • with the consent of the individual, [Principle 3, clause 4.3 of Schedule 1]	• 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."
	Personal Information of the individual without the consent of the individual when: • 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	• to any government institution or part thereof	• "Government Institution" is not defined in PIPEDA, but given that this

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	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)]	and related to law enforcement, or carrying out an investigation related to law enforcement, of Canada or a province.	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 administering any law of Canada or a province, [7(3)(c.1)(iii)]	• 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 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	• 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

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	an injured, ill or deceased individual; [7(3)(c.1)(iv)]		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 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)]	• to any organization that has the capacity and mandate to investigate a breach of an agreement or contravention of the laws of Canada or a province.	• 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.
	• 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 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

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	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)]		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 disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse; [7(3)(d.3)]	• 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.
	• 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.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	• 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: Ontario Disclosure Tool 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 - Ontario											
Identify what legislation applies to you											
(A)	I am subject to privacy legislation: F-FIPPA / M-MFIPPA / H-PHIPA / PI-PIPEDA / PA-Privacy Act / C-CYSFA / N-None										
Identify if one of the listed authorities to disclose applies.											
(B)	Authority to Disclose Under										
FIPPA		**MFIPPA**		**PHIPA**		**CYFSA**		**Privacy Act**		**PIPEDA**	
42(1)(b)	With consent	32(b)	With consent	29(a)	With consent	286(a)	With consent	8(1)	With consent	Sched.1; 4.3	With consent
42(1)(c)	For Stated or consistent purpose	32(c)	For Stated or consistent purpose	29(b)	permitted or required by this Act	286(b)	permitted or required by this Act	8(2)(a)	For Stated or consistent purpose		
42(1)(e)	Where permitted or required under enactment	32(e)	Where permitted or required under enactment	39(1)(a)	determining or verifying the eligibility of the individual to receive health care	292(1)(h)	Where permitted or required under enactment	8(2)(b)	In accordance with Act of Parliament	7(3)(c.1)(ii)	For purpose of enforcing any law of Canada or a province
42(1)(d)	To institution staff who require it for their duties	32(d)	To institution staff who require it for their duties	40(2)	for the purposes of making arrangements for the provision of health						
				38(1)	necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent						
42(1)(g)	To Law Enforcement for investigation	32(g)	To Law Enforcement for investigation			292(1)(a)	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
42(1)(f)	From law Enforcement to law Enforcement	32(f)	From law Enforcement to law Enforcement							7(3)(d)(i)	Where the information relates to the possible commission or intent to commit an offence
				41(1)(d)	To comply with subpoena	292(1)(f)	To comply with subpoena	8(2)(c)	To comply with subpoena	7(3)(c)	To comply with subpoena
42(1)(h)	In compelling circumstances affecting the health or safety of an individual	32(h)	In compelling circumstances affecting the health or safety of an individual	40(1)	necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm	292(1)(g)	to assess, reduce or eliminate a risk of serious harm	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
								8(2)(m)(ii	For any purpose where the public interest in disclosure clearly outweighs any invasion of		
FIPPA		**MFIPPA**		**PHIPA**		**CYFSA**		**Privacy Act**		**PIPEDA**	

To Whom Can I Disclose

I am subject to privacy legislation: F-FIPPA / M-MFIPPA / H-PHIPA / PI-PIPEDA / PA-Privacy Act / C-CYSFA / N-None

Authority to Disclose

	All	F,M,H,PA,C	F,M,PA,C	F,M	H	PA	F,M,H,PI,PA,C
	With Consent of the Individual	**For Stated/ Consistent Purpose**	**Where authorized/ permitted under an act**	**To Org's Staff to Comply w Duties**	**To provide health care & consent not feasible**	**In public interest**	**For health and safety reasons**
Why am I disclosing?	**disclose to: O-Ontario Institution / C-Custodian / PS-Private Sector / I-Federal Institution / A-Any**						
Support to person in need in community	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Supports for youth homelessness	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Supports for adult homelessness	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Service to a youth in crisis	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Service to an adult in crisis	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Assist domestic abuse victim	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Suicide Prevention	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Risk of harm to self	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Risk of harm to minor	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†
Risk of harm to adult	O,C,PS,I,A	O,C,I	O,C,I	O,C,I	O,C,PS,I*	O,C,PS,I,A†	O,C,PS,I,A†

* where non-custodians are defined as "health service providers" under the Connecting Care Act.
† where necessary to disclose to those who have a role to address health and safety

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
Case Management Plan Levels		Name	Contact Info	Identify Needs	Needs Assmnt	In Depth Assmnt	Health Info	Financial Info	Safety Info	Case Mgmt

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 - Ontario

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, 2.2, 3.1, 4.1, 5.1, 5.3, 6.3, 8.3, 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 *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 is often 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, which may include conducting Privacy Impact Assessments, responding to breach incidents)
- What oversight exists (e.g., Privacy Commissioner/Ombudsman)

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 nonprofit 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 must 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.

As well, a non-profit (not-for-profit) may be subject to legislation (The *Personal Health Information Protection Act*) if they provide services as outlined in the *Connecting Care Act*. For more information see "*Appendix B: Privacy Legislation Disclosure Matrix"*, and the specified legislation.

Contracted and Other Service Relationships

Privacy legislation may define someone who acts on behalf of a public body/institution/organization that is subject to legislation using different terminology (e.g. 'employee', 'agent', 'affiliate') but what's important is to recognize that when an individual or agency works on behalf of another organization, they are deemed to be an extension of that organization. In those situations, the rules around the collection, use, and disclosure, that apply to the organization would also apply to them. Note that 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 outlined in Section 5.1.

Privacy Training

There are different training courses or modules available for organizations, including training on the sharing of information Organizations should take steps to ensure staff avail themselves to training appropriate to their roles and responsibilities, including updates as deemed necessary.

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.

Area	Item	Notes
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.
1.4 Roles	Staff Other members Other Areas	Specific role the staff plays. E.g., Initial contact, scheduling/referring/ streaming, initial identification of needs, in-depth assessment, counselling, assistance with ??, The roles that other staff the individual may come into contact with (E.g., could be the other roles listed above). 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 Leadership Team	*Identify the organizations or structures responsible for decisions regarding the overall collaborative service delivery and members.* *Identify any leadership committees or groups and what their roles are in oversight and decision making.*

Area	Item	Notes
	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 Ontario	*Freedom of Information and Protection of Privacy Act* (FIPPA)	FIPPA applies to institutions (provincial ministries in Ontario, hospitals and others). The act sets out the rights of access and responsibilities related to privacy, and the expectations on how the institutions are to manage their obligations regarding the information that is in their custody or under their control.
	Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)	MFIPPA mirrors the FIPPA, but applies to applies to local government institutions in Ontario, (including municipalities, police service boards, school boards, conservation authorities, boards of health and transit commissions). The act sets out the rights of access and responsibilities related to privacy, and the expectations on how the institutions are to manage their obligations regarding the information that is in their custody or under their control.
	Personal Health Information Protection Act (PHIPA)	PHIPA applies to custodians as defined in the Act and those working on their behalf (agents). The act sets out the requirements and obligations custodians must follow in their management of health information, including providing access.
	Connecting Care Act	The *Connecting Care Act* outlines the intent for the delivery of an integrated health care system based in the community, among other areas of focus; establishes the Ontario Health Teams as an authorized entity; and

Area	Item	Notes
		recognizes that Indigenous peoples have a role in the planning and delivery of health services in their communities. The Act recognizes the role that organizations delivering services as defined therein and pulls them under the legislative responsibility of PHIPA if not otherwise legislated.
	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) or who do business in Ontario that involves the management of personal information.
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 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 federal *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. (FIPPA defines them as an

Area	Item	Notes
		employee, PHIPA as an agent.) 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 FIPPA/MFIPPA 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 someone in the organization who can answer their questions about the collection.
	Safety Clause	Legislation generally includes provisions that authorize 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.

Area	Item	Notes
	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.
2.4 Some Differences between Legislation	Type of information	Privacy legislation deals with personally identifying information of individuals, but the scope differs. Personal health information under PHIPA means information in recorded or oral form, that relates to the physical or mental health of an individual, including information that consists of the health history of the individual's family; relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual; is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019; relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual; relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance; is the individual's health number; or identifies an individual's substitute decision-maker. It applies to information managed by a health information custodian, and to a person who is not a custodian but who has received the information from a custodian. Personal information under FIPPA and MFIPPA is defined to mean recorded information about an identifiable individual, including information about the medical,

Area	Item	Notes
		psychiatric, psychological, history, (among other areas). This means that the medical or health information may be subject to either PHIPA or FIPPA/MFIPPA, the determining factor being which organization holds the information. Information about the health of an individual is health information under the PHIPA, if it is in the control or custody of a custodian under that Act. The same information is considered personal information if held by an institution under FIPPA or MFIPPA, or by an organization under PIPEDA.
	Least amount of information	Legislation inherently 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.
	Privacy Impact Assessment (PIA)	PIAs are a requirement under FIPPA, and appropriate assessments are required under PHIPA to ensure electronic records are adequately protected. However, PIAs are strongly encouraged regardless of what legislation applies. They are a due diligence exercise that assesses the risks when new or enhanced changes to the manner in which personal information is managed, including collection.
	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 Information and Privacy Commissioner. The requirement to do so only exists under the PHIPA and FIPPA, but reporting significant breaches is strongly encouraged regardless of what legislation applies.
	integrated program or service	Organizations working together in a collaborative or integrated manner, is supported under the Connecting Care Act, but the provision only applies to the organizations identified therein. That does not necessarily preclude the relationships with other organizations, but other provisions may need to be relied on to provide the authority.
2.5 Examples of other legislation that may come into play	*Child, Youth and Family Services Act* (CYFSA)	The CYFSA applies to the Minister, and to service providers as identified in the Act; provides authority to assess and determine if there is a need to provide services to a child that is in need of protection. 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).

Area	Item	Notes
		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.
	Regulated Health Professions Act	The *Regulated 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 Codes of Conduct for its members. These standards may impose additional requirements on its members regarding the management of personal and health information. While standards may not impose requirements that circumvent legislation, there is a need to consider how they can work together. The Act sets out a number of circumstances where information may be disclosed in section 36(1). For example, the standards may indicate that the personal information of an individual receiving services can only be disclosed with the individual's consent, or where permitted or required by law. The member may be approached or become aware of information that indicates the individual or another person is at risk of harm, but obtaining consent of their client is not an option. Section 36(1)(i) of the Act, as well as provisions under privacy legislation may allow for the disclosure of information without the consent of the individual to whom the information pertains, to eliminate or reduce a significant risk of bodily harm to a person or group of persons.
2.6 Contracts and Agreements	Employees and Agents	As noted above, privacy legislation outlines that employees (FIPPA, MFIPPA) and agents (PHIPA) or others working on behalf of the organization, (which may include volunteers, and those working under a contract or agreement) to be subject to the applicable legislation. 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

Area	Item	Notes
		they are involved in collaborative or integrated service delivery approaches.
3. Working with Individuals		
3.1 Authentication / Verification	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.
	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

Area	Item	Notes
		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.
4. **Collection**		
4.1 Purpose for Collection	Purpose	Authority to collect and use information is driven by the stated purpose(s). 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.
	Required Information	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	The authority to collect personal and health information is stipulated in the privacy legislation.
	FIPPA / MFIPPA	FIPPA and MFIPPA restrict the collection of personal information unless: • Expressly authorized by statute, • Used for the purpose of law enforcement, or • necessary to the proper administration of a lawfully authorized activity. (see FIPPA s.38(2), MFIPPA s.28(2)) 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 institution.
	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

Area	Item	Notes
		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).
	PHIPA	PHIPA outlines that personal health information can be collected with consent, or for specific purposes primarily focused on the provision of health services. (See PHIPA s.36).
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 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

Area	Item	Notes
		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 generally 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 (PHIPA s.36(1), FIPPA s.39(1), MFIPPA s.29(1)), 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. (PHIPA s.36, FIPPA s.39, MFIPPA s.29). An example of an exception is collection with the consent of the individual.
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

Area	Item	Notes
		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 (FIPPA s.43) 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 your management team if clear direction has not been provided.
5.3 Risks	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. (FIPPA s.42(1)(h), MFIPPA s.325(h), PHIPA s.40(1)) 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. It should be noted that under both FIPPA and MFIPPA there is a requirement to provide notification of the disclosure to the last known address of the individual to whom the information relates.

Area	Item	Notes
	Safe and healthy environment	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.
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.
	FIPPA/MFIPPA	FIPPA and MFIPPA identify a number of circumstances where, if met, disclosure is authorized. These may include: • if the individual has provided an informed consent, • for the purpose for which it was collected, or a consistent purpose, • to an employee of the institution if the information is necessary for the discharge of their duties • where permitted or required by law or by a treaty, arrangement or agreement under an Act or Act of Canada, • to a law enforcement institution to assist with an investigation, • in compelling circumstances affecting the health and safety of any person. **See FIPPA s. 42 or MFIPPA s.32 for more information, and the exact wording.**

Area	Item	Notes
	PHIPA	PHIPA identifies the circumstances under which health information can be disclosed. They include: • to another custodian for the provision of health care, • to determine eligibility to receive health care or related goods and services under an Act of Ontario or Canada, (this may include non-health care providers in accordance with the *Connected Care Act*) • to any person to avert or reduce the risk of serious bodily harm to the health and safety of a minor, or a significant risk of harm to any person, • to the head of a penal or other custodial facility, or the officer in charge of a psychiatric facility (under the *Mental Health Act*), to assist with decisions regarding health care or arrangements for discharge, • to assist with a proceeding. … **See PHIPA ss. 34, 39, 40 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 information they require

Area	Item	Notes
		to provide supports and services to the individuals they are working with.
	Email	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 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.

Area	Item	Notes
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 the implications of providing consent	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 rely on some other provision that authorizes the collection or disclosure of their information, if applicable.
7.5 Signature	Individuals must sign the consent form	There needs to be some form of verification that the person has actually consented. The most relevant way is for the consent form to be signed. While the legislation is silent on the requirement for written consent, which includes electronic consent, it is deemed to be a best practice. Oral or verbal consent may also be used should written consent not be feasible, but the organization obtaining such consent needs to authenticate that the person signing the consent is who they say they are, and the verbal consent must be properly documented.
7.6 Representative (Substitute decision-maker)	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: - FIPPA in section 66, - MFIPPA in section 54. - PHIPA in sections 23/24.

Area	Item	Notes
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 consent for collection	If the individual does not provide consent for the collection of all or some of their information	If the individual does not provide consent, it's important to ensure they understand they may not be able to participate in the processes being used by the collaborative service delivery approach, 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.

Area	Item	Notes
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.
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

Area	Item	Notes
		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.
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.

Area	Item	Notes
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. 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.

Area	Item	Notes
		(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, 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

Area	Item	Notes
		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	User representatives for 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 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

Area	Item	Notes
		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 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:

Area	Item	Notes
		- 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; - 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; - 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 Ontario Commitment Agreement

Back

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>*[3] 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 **"personal health information"** has the meaning as per section 4 of the *Personal Health Information Protection Act, 2004*.

1.5 **"personal information"** means personal information about an identifiable individual as defined by the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy 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.

[33] Highlighted sections are to be amended as appropriate to the collaboration.

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 *Freedom of Information and Protection of Privacy Act*; or
  (ii) if the party is subject to, and such use is specifically authorized under, the *Municipal Freedom of Information and Protection of Privacy Act*; or
  (iii) if the party is subject to, and such use is specifically authorized under, the *Personal Health 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 *Freedom of Information and Protection of Privacy Act*; or
  (ii) if the party is subject to, and such use is specifically authorized under, the *Municipal Freedom of Information and Protection of Privacy Act*; or
  (iii) if the party is subject to, and such use is specifically authorized under, the *Personal Health 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 *Freedom of Information and Protection of Privacy Act*
    i. sections 42(1)(b), (c), (d), (e), (g), (h), (i) or
(b) *Municipal Freedom of Information and Protection of Privacy Act*;
    i. sections 32(b), (c), (d), (e), (f), (g), (h), (i), or
(c) if the party is subject to the *Personal Health Information Protection Act*
    i. section 38(1), 39(1)(a), (d), 40(1), (2), or (3), or
(d) if the party is subject to the (federal) *Privacy Act*,
    i. section 8; or
(e) 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
(f) 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 and Electronic Documents Act* (PIPEDA) 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 *<Optional Section - 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 *<Optional Section - Delete if not Required>*

<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 Ontario.

20.0 Signatures, Signing Dates and Appendices

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

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

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

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

Add additional lines as required …

Appendix F: Sample Consent Forms – Ontario Back

The consent requirements under the *Personal Health Information Protection Act* (PHIPA) 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 PHIPA requirements.

Requirements under the PHIPA

18 (1) If this Act or any other Act requires the consent of an individual for the collection, use or disclosure of personal health information by a health information custodian, the consent,

(a) must be a consent of the individual;
(b) must be knowledgeable;
(c) must relate to the information; and
(d) must not be obtained through deception or coercion

(2) Subject to subsection (3), a consent to the collection, use or disclosure of personal health information about an individual may be express or implied.

(3) A consent to the disclosure of personal health information about an individual must be express, and not implied, if,

(a) a health information custodian makes the disclosure to a person that is not a health information custodian; or
(b) a health information custodian makes the disclosure to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care. 2004, c. 3, Sched. A, s. 18 (3).

(4) Subsection (3) does not apply to,

(a) a disclosure pursuant to an implied consent described in subsection 20 (4);
(b) a disclosure pursuant to clause 32 (1) (b); or
(c) a prescribed type of disclosure that does not include information about an individual's state of health.

(5) A consent to the collection, use or disclosure of personal health information about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows,

(a) the purposes of the collection, use or disclosure, as the case may be; and
(b) that the individual may give or withhold consent.

Given this, a best practice is to ensure the organizations working together set out how they will manage consent, use a form that meets the requirements of the PHIPA as far as the form itself, and be clear about when it will allow the use of oral or electronic consent, 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 *Personal Health Information Protection Act* (PHIPA) s.18 • The *Freedom of Information and Protection of Privacy Act* (FIPPA) s.42 • The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) s.32 • 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: _____ Source of Representative's Authority: _____ 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: PHIPA s.29; FIPPA s.38(2); MFIPPA s.28(2); 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, indicate what their relationship is with the client.

Sample 2: 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 *Personal Health Information Protection Act* (PHIPA) s.18 • The *Freedom of Information and Protection of Privacy Act* (FIPPA) s.42 • The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) s.32 • 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: _____ Source of Representative's Authority: _____ 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: PHIPA s.29; FIPPA s.38(2); MFIPPA s.28(2); 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, 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 *Personal Health Information Protection Act* (PHIPA) s.18 • The *Freedom of Information and Protection of Privacy Act* (FIPPA) s.42 • The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) s.32 • 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: _____ Source of Representative's Authority: _____ 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: PHIPA s.29; FIPPA s.38(2); MFIPPA s.28(2); 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.

Name of Organization:	*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*

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 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, 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 *Personal Health Information Protection Act* (PHIPA) s.18 • The *Freedom of Information and Protection of Privacy Act* (FIPPA) s.42 • The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) s.32 • 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: _____ Source of Representative's Authority: _____ 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: PHIPA s.29; FIPPA s.38(2); MFIPPA s.28(2); 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 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[4]. 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, 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.

[4] 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.