An Information Sharing Framework:

Supporting Enhanced Collaboration Between Alberta Organizations Providing Mental Health Services

CONVERGE

Reimagining Canada's Mental Health Systems, Together

Acknowledgements

The materials and development of the following Information Sharing Framework were undertaken with the input and contributions of a number of organizations representing the sectors involved in the delivery of mental health services. The development was made possible with funding provided by the Hunter Family Foundation, through Converge Mental Health Coalition.

The author would like to thank the following individuals and organizations for their input and participation in the Framework's development.

Alberta College of Social Workers, Alberta Health, Alberta Justice, Alberta Mental Health and Addiction, Calgary Board of Education, Calgary Counselling Centre, Calgary Food Bank, Calgary Foothills Primary Care Network, Calgary Homeless Foundation, Calgary Police Service, Calgary United Way, Capitalize for Kids, Canadian Mental Health Association, City of Calgary Addiction and Mental Health Strategy, College of Alberta Psychologists, Distress Centre Calgary, Edmonton Catholic School Board, Edmonton Police Service, Edmonton Public School Board, Help Seeker Technologies, Hull Services, Immigrant Services Calgary, Islamic Family Services, Kindred (Catholic Family Services), PolicyWise for Children and Families, Sagesse, The Alex, Turner Consulting, and various department members from the University of Calgary.

The Framework is being used by various groups and organizations in Alberta. Converge and its members recognizes the potential value for its use in other jurisdictions, as the issues are the same across the country, and beyond. Given that, Converge is interested in supporting the adaptation of the Framework materials for use in other jurisdictions.

This version has been updated given changes to legislation in Alberta. In order to make it more readily adaptable for use in other jurisdictions, the legislative references are now placed in the appendices. The Framework and sets of appendices are being updated by jurisdiction.

Version Control

v.3	Updates Due to Changes in the Health Information Act.

CONVERGE

Table of Contents:

Introduction

It is estimated that 1 in 5 Canadians will suffer a mental health disorder in their lives.[1] Addictions and Mental Health[2] supports have been an area of focus across many sectors, as the impacts of mental health include areas such as employability, education, suicide, domestic violence, homelessness, law enforcement and the criminal justice system. "In order to respond to the needs of youth and adults, mental health services in Alberta have developed across several settings (health, community, and education). While providing mental health supports in multiple settings is beneficial, the current structure presents a challenge to provide care in a timely, consistent, and coordinated way."[3]

The intent of this framework is to enhance the degree of collaboration and integration among client-serving organizations providing mental health supports across all relevant sectors. Organizations work across a variety of areas: Addictions, Health, Education, Law Enforcement, Children's Services, Justice, supports for those impacted by Domestic Violence, and supports for the Homeless, amongst others. The organizations may hire staff, contract, and work with individuals who come from a variety of disciplines, including medical practitioners, nurses, social workers, psychologists and other allied health professionals, educators, teachers, police services, corrections, and probation. The organizations and those they work with may be subject to different privacy and other legislation, or in some cases, may not have any legislative oversight. The result is an environment that creates complexity when it comes to the sharing of personal and health information that is necessary to provide consistent, holistic care when more than one organization is involved. Good collaborative practice should allow for a more comprehensive case management approach, and should reduce the need for individuals to repeat their story, reducing the potential for re-traumatization in the process. It also requires organizations to consider the information needs from a continuity of care perspective, rather than a sometimes-narrow perspective of dealing only with the issue at hand. This is where clarity around the purpose for collaboration becomes so important. While privacy legislation is at times interpreted to only allow the collection, use and disclosure of information for a 'here and now' purpose, rather than 'just-in-case' scenarios, early intervention programs and processes are a critical means of preventing the issues an individual is facing from becoming more serious, requiring potentially more significant and intrusive intervention. As such, it is important to identify the relationship between what information is required, and the outcomes and objectives that are identified when determining the purpose for working collaboratively.

While many services are currently being provided by organizations who work together to some degree, the relationships between those organizations may be enhanced by the implementation and use of a framework that will guide those relationships. There are a number of advantages or ways by which the use of such a framework may not only enhance and improve the services

[1] *Mental Illness and Addiction: Facts and Statistics* (CAMH)
[2] For ease of reference, while the Framework refers to mental health supports it should be read as inclusive of addictions.
[3] "Lifeso, N., Parker, N., McInnes, S., Babins-Wagner, R., Scott, C., & Brown, K. (2020) "*Understanding the Current Landscape of Emerging Adult Mental Health Services and Needs in Calgary and Surrounding Area*". Edmonton: PolicyWise for Children & Families. Emerging Adult - Final Report

being delivered, but as well may serve to enhance the management of the personal and health information of the client that is required for the provision of services.

Connecting with other organizations requires a degree of trust in how those other organizations will work with the client, as well as how they will manage the personal and health information that needs to be shared. Trust is often predicated on the relationships that staff individually build with others as they work through the delivery of supports for the clients they may have in common. However, with the successful implementation of a framework approach, partnering organizations will develop a level of trust with each other, with the knowledge that staff working in any of the member organizations meet the requirements for participation, and can be trusted equally.

The degree to which organizations need to work together depends on a number of factors, including the level and type of service required by the client, the degree of interdependency between the client's issues or factors being addressed by the various organizations, and the capacity of the initial and subsequent organizations to provide the breadth and depth of services required. The greater the number of issues, and the interdependency of those issues, likely means an increase in the number of organizations and/or sectors that need to be involved, and often, an increased need for collaboration.

Using the Framework

Information sharing in and of itself is not the end goal, but rather a means of facilitating organizations to collectively work with individuals and families to provide them with the supports and services they may require. This Framework is meant to provide guidance on the areas that should be considered and addressed as organizations determine there is a need to develop or enhance their existing collaborative service delivery approaches. While not all elements will be required in every situation, consideration should be given to the areas that do apply. As noted in the section on the Collaborative Continuum (below), the greater the degree of collaboration, especially when organizations start to work in an integrated manner, the greater the amount of formalization, and potentially changes, in processes and policies are required. Additionally, the greater the degree of collaboration, the greater the need for the partnering organizations to ensure the appropriate application of the provisions in the privacy legislation they are subject to.

To that end, the Framework is meant to support organizations to collectively apply an *'information sharing lens'* in how they apply those provisions. It will assist such organizations to put in place processes where personal and health information is readily shared where required, to support a holistic approach to meeting the needs of the individuals they support, as they will have gone through the process of applying and validating the necessary authorities to do so; and to do so in a privacy conscious manner. It should be noted that there already exists a robust number of resources developed to support the application of the various individual privacy legislations. However, those resources are often developed with a relatively narrow focus on compliance with the individual legislation, without balancing the risks that may emerge if information is not made available for legitimate uses. As such, the application of an 'information sharing lens' through the use of the framework is meant to augment those

resources by demonstrating how the various legislations can be collectively applied in support of a collaborative approach such that all the members can see how the integration can work.

Given the broad range of supports and services provided by an even broader range of organizations from different sectors that are subject to differing legislation, the Framework is at times written at a relatively high level. For this reason, it is important that as organizations work through the template, they determine in a more detailed approach what applies in their specific circumstances. Support from privacy and legal professionals may be required, and in some situations, there may be a need to conduct and submit a Privacy Impact Assessment (PIA) to the appropriate Information and Privacy Commissioner or Ombudsman. The Privacy Commissioners/Ombudsmen across Canada are also a strong resource and have prepared many publications for use by organizations that manage personal and health information in Canada. The good news is that the completion of the template will serve to inform and therefore minimize the amount of work required in completing a PIA.

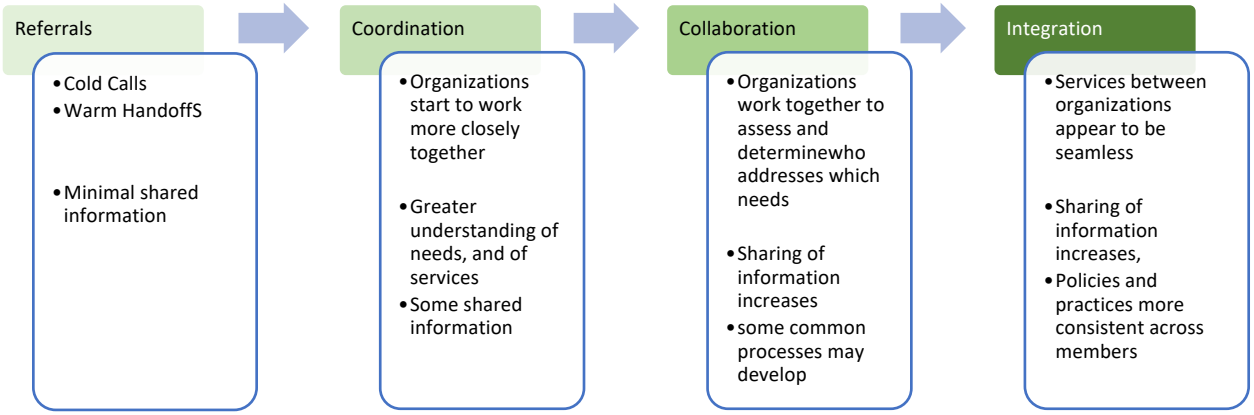
Collaborative Continuum

Back

The following graphic demonstrates the Collaborative Continuum. As engagement between organizations shifts along the continuum from left to right, the increase in collaboration requires organizations involved to share increasing amounts and details of the personal and health information of the individual or family being supported in order to be effective. As well, as collaboration moves closer to the right side of the continuum, the need for formalized processes in support of collaboration and integration of those services between the partnering organizations also increases.

It is quite possible that as organizations support the clients they engage with, they may provide services that touch on various points and degrees of collaboration across the continuum[4]. As such, the framework addresses those potential variations in service delivery approaches. The Guide to Using the Information Sharing Framework (Appendix H) outlines which sections of the Framework should be considered for what type of collaboration. (i.e. Referrals, Coordination, Collaboration, Integration).

[4] For purposes of clarity, the overall approach is referred to as the Collaborative Approach, while each of the areas identified in the continuum will be identified as Coordinated, Collaborative or Integrated Service Delivery.



Collaborative Continuum

The intent of the Framework is to create an environment within which the participating organizations can readily understand what information can and should be shared, and with whom. Providing a level of clarity, allowing the development of trusting relationships between partnering organizations, will also allow them to determine what additional supports or capacity may need to be enabled.

The following is an example of categories of information that may need to be shared dependent on the service provided, and the type of collaborative process occurring. Note that there still needs to be a determination made on what or how much in any of the types of personal and health information would need to be shared for the service and level of collaboration.

Service Required	Collaborative Process	Type of Information								
		Name	Contact Information	Initial Needs Identification	Initial Needs Assessment	In Depth Needs Assessment	Health Information	Financial Information	Safety Information	Case Management Plan
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
Supports 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
Supports 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
Supports 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, Intervention, Assessment	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	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 Required	Collaborative Process	Name	Contact Information	Initial Needs Identification	Initial Needs Assessment	In Depth Needs Assessment	Health Information	Financial Information	Safety Information	Case Management Plan
		Type of Information								
Risk of harm to minor	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 adult	Warm handoff	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

Case Management Plan Levels

A. Basic: no true dependencies per se, but relationship between needs may exist.
B. Collaborative: some dependencies may exist, some increased level of information sharing required, such as reporting on progress.
C. Comprehensive/integrated: relationships and dependencies exist, potentially requiring organizations to regularly update a coordinated or comprehensive case management plan, or each other.

Organizations who provide collaborative case management should be clear on how they expect to work together, what information is necessary to facilitate that approach, when do the services and each other's involvement begin and end, what the objectives are, and wherever possible or appropriate involve the individual as part of the case planning process to foster transparency and buy-in.

Note that the categories are broadly defined, as are the types of information, and is meant to provide a sense of the information types that may be required and need to be authorized to provide for an effective service. Organizations using this as a starting point will need to work through it in more detail, depending on the collaborative initiative.

Sample Scenario:

A school board is working with a health services provider to ensure there are sufficient and effective mental health supports for the students they have responsibility over. Both the school board and the health services provider are subject to privacy legislation, although the legislation may differ for each depending on the jurisdiction. The **purpose** of the collaboration is to effectively support students with mental health concerns, which may vary in degree from situations where the issues can be readily managed by the student with a relatively low-level intervention, perhaps by seeing a counsellor on a regular but infrequent basis; to ones where there are concerns about the health and safety of the student or those around him/her, such that there is the potential for harm, and possibly the need for a significant level of intervention. This **purpose** may be described in a number of ways, such as identifying that the school

environment includes supporting the students' well-being, or the environment is meant to be a safe and healthy one. Outlining it in this manner not only demonstrates transparency, but it also sets out that should the school need to address health and safety concerns, they have the authority to do so. (Purpose for the collection of information includes the support of a healthy safe environment, and using or disclosing information to address issues related to health and safety is linked to that purpose.)

Legislation that might apply in this scenario is listed in Appendix A applicable to your jurisdiction.[5]

Other Considerations: While the legislation allows for disclosures between both parties, there are other things to be considered, and the parties would benefit by agreeing on how to address various situations.

The health service provider might be a psychologist, social worker or other allied health professional who may be a member of a Professional College, in which case would also be required to follow their Professional College's Standards of Practice, Codes of Conduct or Codes of Ethics. Such Standards may impose additional requirements, such as ones related to the use of informed consent before disclosing the personal information of their client. They also generally recognize that information can be disclosed without consent in situations where there is a risk of significant, severe, or imminent harm, or where authorized and required by law.

Other legislation may also apply, and organizations must ensure they familiarize themselves with the potential application of such. Privacy legislations generally have provisions that authorize disclosure without consent where other legislation authorizes or requires the disclosure of information.[6]

The parents or guardians of the student are not necessarily required to consent to the disclosure of the information if the student has the capacity to understand and provide consent, nor do they necessarily need to be involved in the situations where disclosure can be provided without consent. However, there may be a requirement for them to consent to any treatment, an area the health services provider would need to determine, based on the applicable health or other legislation. While parents/guardians of the student can and should be involved in the majority of situations, there may be occasions where it is appropriate for some information disclosure without their involvement (e.g., emancipated youth, or situations at home potentially impacting on the youth's mental health).

Information Needs to support the student's well-being may include:

i) The compiling of observed interactions and issues by the school that led to the determination of the need to address the mental health concerns. Observational data can assist in the assessment by the health service provider, as the environment in which the assessment occurs may at times be somewhat insular, such as when the therapist sees the individual in their office or remotely.

[5] See Appendix A - Specific Legislative References, Note 1, Legislation that Might Apply to the Scenario.
[6] See Appendix A - Specific Legislative References, Note 15, Disclosure.

ii) A summary of the assessment and potential need for some intervention may be information that is of value not only for the student, but for the school as well so it can prepare to support the student when they return to school,

iii) Any referrals or intervention provided on an ongoing basis may also be of benefit for the student and the school for the same reasons. Note that the amount of information the school requires may vary, and would not likely be exhaustive. However, as noted in i), the school is in a position to monitor the student and to gauge whether there are any changes in behaviours during or following the intervention/sessions. In this context, the school can become the 'eyes and ears' for the health services provider(s), and report back on their observations. Ideally, this approach could be part of a plan that all parties, including the student, have agreed upon. This may be an area where there would be value in having a standardized agreement template.

The involvement and role of the parent/guardian in all of this needs to be determined, but irrespective of the desires of the parent/guardian, it may be in the best interest of the student to ensure the school has the information it needs to support the student and the family.

Note: Planning for these types of situations is critical, and policies or guidance to be followed regarding assessing risk, actions to be taken, and roles and responsibilities of the appropriate parties should be determined in advance, with staff receiving the appropriate training. The ability to appropriately assess levels of risk would be of value to the schools and the students.

The **Framework** can serve to set out the purpose for the collaboration, the legislation that authorizes the disclosures, and the practices and policies that the partnering organizations would agree on. There may be additional areas that need to be outlined, such as the identification of key personnel, such that the flow of necessary information occurs in a relatively efficient and seamless manner. If it takes too long to find out who the organization sharing information needs to speak to, that also can become a barrier.

This example is relatively straight-forward, and if enabled would need additional work to be fleshed out, but is meant to illustrate the approach that can be put in place.

1. Purpose

Back

As organizations start to work together, they need to be able to both identify the purpose for doing so, as well as explain that purpose to the individuals and families they support through the collaborative approach in a manner they would understand.

1.1. **Purpose** (for Working Collaboratively):

The purpose should be clearly articulated and agreed upon by all the members. At a minimum, the core members should be involved in determining/agreeing on the purpose, and the objectives or outcomes meant to be achieved through the collaborative approach.

Identifying the purpose will not only serve to provide clarity and understanding to all member organizations and their staff as to why they are working together, it will also support transparency for clients when the staff who are supporting them can reframe the purpose for them in understandable terms. It also starts to create or outline the authority required for the collection, use, and disclosure of the personal and health information that is needed to provide the services to the individual being supported.

As noted in the Collaborative Continuum (page 8), there are a variety of touch points, reasons why organizations may work together, and degrees of interaction and relationships as they work together. The following examples will serve to illustrate why it is important to outline the degree to which the members intend to collaborate:

- Coordinated Example: The members working together in a coordinated approach may determine that when a preliminary identification of services required or requested by the individual is conducted, perhaps by the first point of contact, there will be a sharing of that initial information, along with the individual's contact information, after which any member organization who determines they may be able to provide services would work independently with the client. In this situation, only the initial collection of information is shared between the member organizations. There is no development of a case plan through the coordinated approach per se, although the identified service needs may serve to provide a direction for the client. The main thrust of this approach may be to ensure referrals are appropriate.

- Collaborative Example: The members working together in a collaborative service delivery may determine that they will conduct an initial assessment of needs and strengths of the individual, with the intent of sharing that initial information, after which each member organization who determines they may be able to provide services would work independently with the client. In this situation, the initial collection of information that is shared between the member organizations may include the initial assessment. Alternatively, they may also determine that they will "report back', or provide information back to the collaborative service delivery members to indicate whether or not their involvement has been of benefit for the client, so as to close the loop, and potentially identify if further re-assessment and services are required. In this situation, there may be a case management plan developed, outlining the areas that individual member organizations are taking responsibility for, especially if there are any service dependencies identified.

- Integrated Service Example: The members working together in an integrated service delivery may determine that an initial assessment of needs and strengths of the individual will be conducted. The members may determine that any of the member organizations can conduct the initial assessment, or they may identify that as the responsibility of one member, acting on behalf of the others. A cohort of members may be involved in the development of a comprehensive or coordinated case management plan that identifies the responsibilities of the involved member organizations. The involved members would use the case plan as their starting point, and may need to update it periodically, indicating progress, although additional information they individually collect as they provide their mandated services may not need to be shared. Decisions regarding the sharing would be at the discretion of the organization, depending on the relevance and relationship to the initial assessment and case plan (and likely in consultation with the client). The member organizations may also determine if there is a need to identify a case-plan coordinator who will play a lead role in its management. In this situation, the information collected for the initial assessment and the subsequent case plan and activities is being collected by the integrated service partners as a whole, rather than each member having to collect and disclose the information between them.
  Note that depending on the jurisdiction, legislation may specifically support the delivery of integrated services.[7]

For these reasons, the purpose should be carefully considered and stated in plain language where possible. As well, consideration should be given to including within the purpose a description of the environment the services are to be delivered in. If, for example, the intent of organizations working together is to provide "X" services in a safe and healthy environment, that should be clearly stated. By doing so, the collaborative approach starts to articulate that one of the purposes, from which authority can be determined, is the promotion or maintenance of health and safety. Individuals would then be informed that the use and disclosure of personal and health information where necessary to prevent or minimize risks to health and safety of any person might occur should the need arise, notwithstanding consent.

1.2. Objectives/Outcomes:

In order to determine the success of the collaborative approach, whether at an individual client level, or at the system level, the objectives or outcomes should be identified and listed. This will also assist in identifying what information or data may be required to measure and evaluate the desired outcomes.

2. Membership / Partners

Back

Member organizations that will be involved may fall into a number of categories. Identifying them will assist in a number of areas, including defining the roles they will play within the collaborative approach, the legislation that may impact how those roles are enabled, and the type and level of detail of the information they may require to fulfill those roles. It's also

[7] See Appendix A – Specific Legislative References, Note 8, Common or Integrated Programs or Services (CIPS); and Appendix B Addendum: CIPS

important to recognize the potential for different roles to exist within an organization, which may influence not only what information is required by the staff in those different roles, but also how the information will be managed within the organization (e.g., degree or amount of access). Examples of different roles within an organization include: intake, which may involve an initial high-level assessment of need, and counselling, which could require a deeper dive into underlying issues; or the difference in the roles police services may play between community engagement, which may require members to be involved in assessment, early intervention and support, and law enforcement, which may require urgent responses to crisis situations.

Consideration should be given to identifying the organizations that will be the ones most likely to be involved, given the area(s) being addressed. As well, depending on where along the continuum they are interacting, the roles played may shift.

Note that regardless of their role, staff must only access the information they require, and are authorized to access, to provide the services required, for the clients they serve.

2.1. Core Members:

The core members are typically involved on a regular or continuous basis, and form the nucleus or core of the collaborative approach. Core members should be involved in the initial determination of the overall approach, including governance, decision-making, practices and policies, training, minimum requirements for onboarding of new members, information management, and evaluation.

Core members will generally meet on a regular basis, as laid out in the Governance structure (below).

If an information system is enabled to manage the client information, access should be authorized for the organizations involved in providing services to the clients, based on the need for specific information as required for their role. Common records may exist for use by partnering organizations.

Core Members for this initiative should be identified and listed, along with their representatives for any groups or committees.

2.2. Extended Members:

Extended members are those organizations that may be involved on a somewhat frequent but not full-time basis, and are not expected to be as involved in the day-to-day deliberations and activities of the collaborative approach, if at all. They may provide input to the management of the process, but not likely to be actively participating in the decision-making and governance of the collaborative approach. Staff working for these organizations should likely be trained on the collaborative approach, including the management of information where they are involved in its sharing and use.

Alternatively, extended members may refer to organizations who do not require the sharing of significant amounts of personal and health information, if any. For example, the agency may

only need to know the name and some contact information of the person(s) being referred, and perhaps that the individual being referred is involved with the collaborative approach (perhaps as evidence of the eligibility for the referred to services).

If an information system is enabled to manage the client information, access would be significantly restricted, if deemed necessary, or an alternative method of sharing necessary information may be required.

Extended Members should be identified and listed if they will require some level of information being shared with them. Otherwise, they may simply form part of a common list of referrals.

2.3. Ad Hoc Members:

Ad hoc members include organizations or individuals who are rarely or less frequently involved in the services being delivered under the collaborative approach. They may include those who can provide a specific type of expertise that might be required in specific situations, or perhaps they are involved due to the circumstances of the individual, or they referred the individual. These entities may not need to follow the processes and practices of the collaborative approach, and as such may not require training to the same degree. They should be made aware of, and agree to, any expectations required on the involvement with the client, and the management of their information. Information that needs to be shared with an ad hoc member would be driven by the reasons for their engagement, and the level of detail may vary accordingly.

If an information system is enabled to manage the client information, access would be severely restricted, if deemed necessary.

2.4. Other Members:

The above types of members are not an all-inclusive list, and other types of members may be identified as necessary. When doing so, it will be important to determine the type of information and the level of access they may require.

3. Roles and Responsibilities

Back

The roles and responsibilities will vary according to the type of membership, the services being delivered by the member organization and their staff, and to the type of engagement along the Collaborative Continuum. The responsibilities for the various roles identified here are separate from those that exist under Governance.

Clearly articulating the roles and responsibilities of the individual members will clarify what information they require to fulfill those roles. This serves to further detail and outline the authorities for their collection, use, and disclosure of personal and health information.

Sample Table of Roles and Required Information
Information listed in the table below should be specific to the collaborative approach and membership.

Role	Description	Requires Type of Information
E.g., Intake, (Service Provider)	*Completes initial intake/ assessment*	*Contact information, needs/ presenting issue identification*
E.g., Counselling, (Service Provider)	*Provides counselling support*	*More in-depth client information e.g. what may impact mental health– may include personal and health information*
E.g., Eligibility for Needs, (Service Provider)	*Determines eligibility for and ongoing management of benefits and services*	*Client information required to determine and maintain eligibility*
Advisory Committee (e.g. lived experience, youth)	*Provides input into areas, based on their perspective*	*General, no identifying information*
Peer Support (e.g., lived experience)	*Provides support to individuals being served.*	*Some basic personal information based on what individual is willing to share*

4. Governance and Accountability

Back

Organizations working in the delivery of mental health services are privy to significant amounts of very sensitive personal and health information, and as such, need to ensure that governance in the management of that information demonstrates the necessary accountability and responsibility. The fact that organizations and professional staff who work together may be subject to different privacy legislation, if any, makes this not only more complex, but even more critical.

Ensuring the appropriate accountabilities are identified, developed, and in place, serves to not only demonstrate a level of responsibility to individuals who are being supported by the collaborative approach, it also engenders trust between the participating member organizations. Trust relationships allow for staff of the various member organizations to make decisions on sharing information knowing that the member organizations will manage the information with the same level of confidentiality as their own. Adherence to Legislation is one of the ways for organizations to demonstrate their accountability and is dealt with in the next section.

4.1. Lead Organization Structure

There are a number of options in how governance can be structured, and a decision that best suits the circumstances or initiative should be made by the partners at the table. Where organizations with significant levels of responsibility, such as government departments or institutions, or larger health organizations (who, depending on the jurisdiction, may be subject to separate privacy legislation) are involved, it is recommended that they play a significant role

in the governance. The governance role of other organizations should be determined in consultation with them.

The following options are not all-inclusive, and other ones may exist that are more suitable to the circumstances and jurisdictions within which you operate. What is important, is the need to identify accountability that not only reflects how the various member organizations manage the personal and health information they require and use, but also provides assurance to the individuals and families they support that their personal information will be managed in a privacy-conscious manner.

Option 1: Lead (Primary) Organization:

Responsibility rests with one lead organization, acting on behalf of the partnering organizations, by agreement, working in unison with a leadership table representing the core partners. Decision making could be allocated to various areas, with day-to-day policy and practices being determined and approved by all partners, perhaps through consensus. The Lead would be responsible for ensuring that the practices and policies are followed, and would represent the partnership as required.

A variation on this could have rotating leads, with the various core organizations taking on the lead role for set periods of time.

The development of policies, practices and procedures could be undertaken by a working group or contracted out; while vetting and adopting them would rest with the leadership table. The Lead's role would include overseeing development and the processes for adoption and implementation.

Area of Responsibility	**Activities**
Lead Organization	Responsible to coordinate the leadership team and activities, which includes to: • chair the leadership table, including regular meetings and communications, • represent the needs and best interests of the collaborative approach in decision making, (given this role, a decision should be made if the lead should have a different person represent their home organization at the leadership table) • provide oversight and direction, built on a consensus approach where possible, • act as lead representative for the collaborative partnership with external organizations as required (e.g. Privacy Commissioner/Ombudsman, regulatory body(-ies), should the need exist), • contract for/manage any support areas, and oversee the secretariat activities as required on behalf of the partnership, as required.

Area of Responsibility	Activities
	• responsible for oversight/management of (common) records and information
Leadership Table	Membership includes the leads for each of the core partners (should be determined and agreed to by all partners) of the collaborative partnership. Responsible to: • as the representative for their organization in the collaborative approach, bring forward their organization's perspectives and needs, • act to balance and support a two-way perspective that also considers the needs of the collaborative approach, • participate in the development and implementation of any policies and practices identified for use within the collaborative approach, as required, (Note – the level of participation may vary dependent in part on the capacity of the organization, and the potential use by the supporting organization(s) to develop draft policies, but at a minimum, there should be a process agreed to that includes vetting and approval of drafts put forward for approval.) • commit to meaningful engagement and regular attendance, • commit to ensuring the decisions agreed to by the collaborative approach members are implemented and followed by their organization's participating staff and provide appropriate training, • participate in problem-solving processes developed to deal with potential areas requiring conflict-resolution, • identify and bring forward any areas of concern as they emerge so that they can be dealt with expeditiously, • report any areas that have been identified as necessary to report, including potential information breaches, and participate openly with any required investigations.

Option 2: Shared Leadership

The responsibility for governance is shared by the core organizations (the Leadership Table), working through the decision-making processes as a leadership table comprised of all core members. Decision making could be allocated to various levels or areas, with policy and practices being determined and approved by all partners, through consensus; while the responsibility for implementation within their own organization could fall to each member, or to a secretariat/support organization. The Leadership Table members would be equally responsible for ensuring that the practices and policies are followed, and work through issues as they arise.

In this model, the leadership could be structured to have more than one level, the Leadership Table itself, comprised of executive/senior level representatives of the partners, who would

provide oversight and upper-level decisions; as well as a team made up of middle management or other level representatives who could be largely responsible for the day-to-day decisions and management.

Similar to the single lead option, the development of the policies, practices and procedures could be developed by a working group or contracted out; while vetting and adopting them would rest with the Leadership Table. The Leadership Table's role would include overseeing the development, adoption and implementation processes.

Area of Responsibility	**Activities**
Leadership Table (Core Organizations)	Responsible for the coordination of relevant activities, which includes to: • identify a chair or co-chair for the Leadership Table, (potentially on a rotating basis) • chair and support the chair activities, which includes regular meetings and communications, • commit to representing the needs and best interests of the collaborative partnership in decision making, • provide oversight and direction, built on a consensus approach where possible, potentially with a management table reporting on a regular basis, • identify a leadership representative for the collaborative partnership to liaise with external organizations as required (e.g. Privacy Commissioner/Ombudsman, regulatory body(ies) should the need exist), • identify any responsibility to contract for and manage support areas, and oversee the secretariat activities as required on behalf of the partnership. • responsible for management of (common) records and information.
Middle Management Table	Membership includes the leads for each of the core partners (should be determined and agreed to by all partners) of the collaborative partnership. Responsible to: • as the representative for their organization in the collaborative partnership, bring forward their organization's perspectives and needs, • act to balance and support a two-way perspective that also considers the needs of the collaborative partnership, • participate in the development and implementation of any policies and practices identified for use within the collaborative, as required, (Note – the level of participation may vary dependent in part on the capacity of the organization, and the potential use by the supporting organization(s) to develop draft policies, but at a minimum,

Area of Responsibility	Activities
	there should be a process agreed to that includes vetting and approval of drafts put forward for approval.) • commit to meaningful engagement and regular attendance, • commit to ensuring the decisions agreed to by the collaborative partnership are implemented and followed by their organization's participating staff, • participate in problem-solving processes developed to deal with potential areas requiring conflict-resolution, • identify and bring forward any areas of concern as they emerge so that they can be dealt with expeditiously, • report any areas that have been identified as necessary to report, including potential information breaches, and participate openly with any required investigations.

Option 3: Fully Autonomous Organizations

In this option, each organization is individually responsible for all aspects of the information they manage. While this approach may be seen to be less complicated, and more in line with the existent areas of responsibility, it does not easily support the overall objectives of collaborating or integrating services. While one organization could be responsible for the development and implementation of the approach, implementing and maintaining processes would be more difficult, limited oversight would exist, and any efficiencies would be harder to achieve.

Any information that needs to be stored in a central repository would require individual service agreements between the organization responsible for the information, and the organization responsible for the repository.

Area of Responsibility	Activities
No Lead Organization(s)	Each organization would maintain its own responsibility for their organization's activities, as well as their participation in the collaborative partnership including to: • attend regular meetings and maintain internal and external communications, • commit to representing the needs and best interests of the collaborative partnership in decision making, • make decisions on a consensus approach where possible, • potentially represent themselves rather than the collaborative partnership with external organizations as required (e.g. Privacy Commissioner/Ombudsman should the need arise), although a decision to have a representative for the collaborative partnership could be made,

Area of Responsibility	Activities
	• similarly, one organization could be given the responsibility to contract for and manage any support areas and oversee the secretariat activities as required on behalf of the partnership, • determine responsibility for management of (common) records and information – individually or collective.
Management Table	Membership includes the leads for each of the core partners of the collaborative partnership. Responsible to: • bring forward their organization's perspectives and needs, • act to balance and support a two-way perspective that also considers the needs of the collaborative partnership, • participate in the development and implementation of any policies and practices identified for use within the collaborative partnership, as required, (Note – the level of participation may vary dependent in part on the capacity of the organization, the potential use by the supporting organization(s) to develop draft policies, but at a minimum, there should be a process agreed to that includes vetting and approval of drafts put forward for approval.) • commit to meaningful engagement and regular attendance, • commit to ensuring the decisions agreed to by the collaborative partnership are implemented and followed by their organization's participating staff, • participate in problem-solving processes developed to deal with potential areas requiring conflict-resolution, • identify and bring forward any areas of concern, as they emerge so that they can be dealt with expeditiously, • report any areas that have been identified as necessary to report, including potential information breaches, and reports of unprofessional conduct under section 57 of the HPA, and participate openly with any required investigations.

Across All Options:

Area of Responsibility	Activities
Participating Agency Staff	This includes staff who are selected by their organization to participate in the collaborative service delivery approach. These staff are responsible to: • become educated on and implement any policies and practices that have been developed and identified for use within the collaborative partnership, • represent the best interests of the clients first, the intended objectives identified by the collaborative partnership second, and the needs of their own organization. Where any conflict between those intended streams may emerge, they will identify them to their organization's representative, • maintain confidentiality of any and all client information that they are involved with, • access only the information they require and are authorized to access to perform their duties for the clients that they are responsible for, • report any potential breaches, areas of conflict, or conflicts of interest.
Specific Roles/Functions Privacy Officer/Lead Security Officer/Lead	These roles or functions may be required as part of the collaborative support team, or may be embedded within each organization and relied on as needed. It may be beneficial that they work together and report at a high enough level within the organization(s) to ensure accountability. In certain circumstances it may be appropriate that the functions are part of other roles, and may also be contracted out, or accessed as required. • This role may be responsible for ensuring a privacy-conscious approach is in place for the organizations, including providing training and guidance on all aspects of privacy, managing breach investigations and reports. • The security role may be responsible for the security of information, including ensuring the infrastructure within which it is stored and managed is secure, managing credentials if used, investigating breaches, and providing training and guidance.

4.2. Committees/ Advisory Structure

Any additional committees should be identified, including membership, roles or activities, scheduling and other pertinent information. That includes whether the members on the committee would require any access to personally identifying information. Examples could include 'lived experience' or youth advisory committees, peer support groups, evaluation committees, and so forth. **Differences between advisory roles and peer support roles should be clearly stated.**

4.3. Decision Making

The decision-making process should be outlined, at a high level, in keeping with the governance model decided on. Consensus, majority, lead with inputs, etc.

4.4. Decision Socialization

The process by which decisions are published or made available to those staff, organizations or clients for which there are implications or changes required should be outlined. Updates to policies, practices and procedures should be made, with effective dates identified and logged. It may be necessary to demonstrate what policies, etc. were applied when, so records of previous policies and their effective dates should be maintained as needed.

4.5. Responsibility for Records/Information

Decisions regarding the management of any records will be critical, and dependent in part on the following factors:

- Governance model
- Existence of common records
- Use of a centralized platform or database
- Manner of distribution or access to information by members

4.6. Demonstrated Commitment:

Organizations who decide they will be working together in a collaborative manner have to recognize and demonstrate the commitment that is required by the organization and their staff. That commitment may be ratified in a number of ways, including signing on as participants in the framework, through agreements, MOUs, or other. A sample commitment agreement is attached in Appendix E: Sample Commitment Agreement.

The Collaborative Approach Member Organizations agree and support the outlined policies and procedures for their involvement and provision of services through this initiative. Information that is collected, used and disclosed by the members for the purposes of the initiative will be managed in accordance with these policies and applicable legislation. Where there is a disparity between the Member Organization's home policies and these, these policies and procedures will take precedence as they apply to the work undertaken within the initiative. Information that is managed within the individual organizations will continue to be managed in accordance with the member organization's own policies and procedures.

Member Organizations demonstrate their commitment to the initiative, and follow the policies and processes outlined herein, by signing the Commitment Agreement.

Organizations that sign on as member organizations of the Collaborative Approach do so with the full understanding that they agree to:

- manage personal and health information in accordance with the policies and practices developed under the framework,
- ensure their staff are trained on the framework, and any changes that may be required in their roles,
- work with all member organizations, and

- address any issues or concerns, including potential privacy or security breaches, through the identified area responsible (may be an individual, specific role or position, or a committee).

Member organizations will demonstrate their commitment to:

4.6.1. The Collaborative Approach:

Member organizations will ensure that decisions made within their home organization that have potential implications for the collaborative approach will consider those impacts and potential changes to their processes if appropriate, before making decisions. Where there will be impacts on the collaborative approach, they will be brought to the attention of the area responsible to address them (examples may include a specific role that liaises with members, or a cross-member committee).

Organizations may have to adopt new ways or processes in decision-making where there are implications for the collaborative approach. This is likely to increase significantly the greater the degree of collaboration and integration. Unilateral decisions that may be the norm within an organization may have the potential to impact the outcomes and objectives of the collaborative approach. As such, a review of situations where such processes may need to shift should be undertaken and changes explored. Examples of this may include:

- The use of different forms. For example, if consent to disclosure is a requirement for the sharing of information necessary to supporting the individual in a holistic or comprehensive manner by collaborating organizations, it may be necessary to come to an agreement about a common consent form for disclosure that potentially differs from the one their organization has in place;
- Determining what evaluation processes and reporting requirements will be agreed on. (E.g., consideration of data requirements, efficiencies in collection, and reporting by whom, …);
- The use, obligations and language of contracts with agencies who may also contract with other members, ensuring alignment so to eliminate any areas of confusion.

Similarly, if organizations have determined that they need to address risks to health and safety, either as their primary purpose for collaborating, or as part of ensuring a healthy, safe environment in which services are provided, they should ensure they have a common understanding of when the threshold for involvement or escalation may occur. That may differ from the processes or definitions of risks that may be in place within the individual organizations themselves. Further, the individual member organizations may play different roles, or become involved at different points, depending on the areas of responsibility. For example, police services may be involved in different roles – Community Engagement, where they are actively engaged in assessing and proactively trying to find solutions with their partners, and Enforcement, which would include being involved when there is a high risk of danger to health and safety. Police service members operating within the parameters of the first role can work well with other member organizations, becoming involved earlier, when there is the potential for early intervention, or to de-escalate or prevent the risk from evolving to a higher level that requires significantly more intrusive measures. These roles will not always be immediately clear, nor always well defined, but by discussing them in advance members can realize the benefits of each other's participation.

4.6.2. Ensuring staff are trained:

Staff who participate in a collaborative approach must be trained on the relevant policies and procedures required of them, prior to accessing information and providing services. Building relationships with their clients will now entail providing information about the collaborative approach, so staff need to not only understand the purpose(s) and objectives of the collaboration, but be prepared to explain them to their clients in a manner they will understand. See Appendix D: Sample Collaborative Approach Training Resource.

Training may also include areas such as the following:

- Changes to their duties: Staff who collaborate with others may see their roles change to some degree. For example, their role may evolve to include providing or eliciting feedback on the effectiveness of actions taken or required by their colleagues in a coordinated case plan – in a sense becoming the 'eyes and ears' of their colleagues.
- Changes to, or the addition of new, practices and procedures,
- Requirements and restrictions on the management of information, including collection, use and disclosure (sharing),
- Expanded knowledge of their partnering collaborative approach organizations.

5. Applicable Legislation

Back

The following discussion on applicable legislation deals primarily with personally identifying information. It is important to note that it is not only the provisions dealing with collection, use, and disclosure that need to be taken into consideration, as legislation contains a number of other provisions that may also have an impact. For example, privacy legislation expressly or implicitly requires organizations to only disclose information to the extent necessary to carry out the purposes identified in a reasonable manner and to the highest degree of anonymity that is possible in the circumstances. These and other provisions must be considered within the context of what the organizations are intending within their collaborative approach[8].

The collection, use and disclosure of non-identifying information is generally authorized by the legislation, either explicitly, or by being silent in regards to it. Note, however, that simply removing what is generally known as an identifier (e.g. Name, DoB, SIN, etc.) does not necessarily remove the risk of re-identifying the individual. As such, the information must be managed accordingly, taking precautions to not enable users to re-identify the individual(s), and to continue to manage the information with appropriate security provisions in place.

Each jurisdiction in Canada has developed their own suite or single instances of privacy legislation. The legislation generally applies to the public sector, that is government organizations at the federal/provincial/territorial level, the municipal and other similar levels,

[8] Note that the implementation of the collaborative framework and its objectives should outline the circumstances for disclosure in such a manner that the amount of information, and the degree of anonymity required should be clearly understood. For example, agencies working together on a comprehensive case plan likely need to identify the individual as they use information on how they are progressing; but an agency that is seeking advice regarding potential referral for services for a client may not need to identify the individual to obtain the advice.

and to other organizations generally seen to fall within their domain, such as publicly funded school boards, police services, and the like.

Health sector organizations may also have their own privacy legislation, as may private sector organizations. Where no such legislation applies, the federal *Personal Information Protection and Electronic Documents Act* may apply.

See also Appendix A for the references to the applicable legislation for your jurisdiction.

5.1. Provincial/Territorial Privacy Legislation

5.1.1. Protection of Privacy Act (POPA)

The *Protection of Privacy Act* applies to public bodies in Alberta, defined to include provincial and local government organizations, including municipalities, housing management bodies, police services as defined in the *Police Act*, Metis Settlements, educational bodies (including post-secondary institutions, school boards and charter schools as defined in the *Education Act*), and health care bodies, amongst others.

The Act deals with personal information, which is defined to mean recorded identifying information about an individual, including but not limited to the individual's contact information. Note that health information managed by public bodies is deemed to be personal information. By way of example, a custodian under the *Health Information Act* (HIA), such as a physician, may use medical information to fill in a public body's disability application form. The medical information held by the physician is defined as health information and is subject to the provisions under the HIA. However, once the form is provided to the public body and used for their authorized purpose, it is deemed personal information under POPA, and bound by the provisions therein.

'Employee' is defined to include any person working on behalf of a public body, for the purposes of the Act. This allows information to be managed by that 'person' or 'employee' so that they can provide the services they are expected or engaged to provide. It does not reflect an employer/employee relationship.

The Act outlines a set of purposes that include: a public body providing an individual access to their own information; or by anyone to general records held by the public body, subject to certain specific exceptions; controlling the manner in which a public body collects, uses, and discloses personal information about individuals; allowing individuals to request corrections of their personal information held by a public body; and providing for independent reviews (Oversight) of decisions made by public bodies under the Act.

5.1.2. Health Information Act (HIA)

The *Health Information Act* applies to custodians in Alberta, defined to include the designated departments (Primary and Preventative Health Services, Hospital and Surgical Health Services, Mental Health and Addiction, Assisted Living and Social Services), hospital boards, regional health authorities, and regulated health service providers who provide a health service, as currently defined in the regulations (Dental Hygienists, Optometrists, Pharmacists, Denturists, Chiropractors, Dental Surgeons, Dietitians, Midwives, Opticians, Physicians and Surgeons, Physiotherapists, Podiatric Physicians, Registered Nurses), among others. Many of these health professionals are employed by organizations who may in fact be defined as a custodian under the Act, such as Health Authorities, in which case they are deemed affiliates to that custodian.

An individual may be registered as a health service provider with their professional college, but if they do not provide a health service they are not deemed a custodian. (E.g., a nurse or physician who is only a professor in a post-secondary institution; or a physician who is only appointed as the Director of the *Occupational Health and Safety Act*.)

The Act deals with health information, which is defined to mean diagnostic, treatment and care information (which includes any other information about an individual that is collected for the purpose of providing a health service), and registration information. It must be managed in accordance with the Act if it is individually identifying, such that the identity of the individual can be readily ascertained from the information.

'Affiliates' are defined to mean any individual employed by the custodian, or any person working on behalf of the custodian, for the purposes of the Act. This allows information to be managed by that 'affiliate' so that they can provide the services they are expected or engaged to provide. It does not reflect an employer/employee relationship.

The Act sets out a set of purposes that include: establishing strong and effective mechanisms to protect the privacy of individuals and the confidentiality of their health information; enabling health information to be shared and accessed, where appropriate, to provide health services and well-being services[9]; prescribing rules for the collection, use and disclosure of health information, which are to be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances; providing individuals with a right of access to their own health information, subject to limited and specific exceptions; providing individuals with a right to request correction of health information about themselves; establishing strong and effective remedies for contraventions of this Act; and providing for independent reviews of decisions made by custodians under this Act .

5.1.3. Personal Information Protection Act (PIPA)

The *Personal Information Protection Act* applies to organizations (including corporations, unincorporated associations, trade unions, partnerships as defined in the *Partnership Act*, and individuals acting in a commercial capacity) but does not apply to non-profit organizations incorporated under the *Societies Act, Agricultural Societies Act*, or registered under Part 9 of the *Companies Act*, or to any personal information held by them except for personal information that is collected used or disclosed in connection with a commercial activity. By way of example, a non-profit agency that charges fees for counselling services would in and of itself would not be subject to the Act, but the information that is collected and managed through the counselling services would be, as that would be deemed a commercial activity. Note that Health professionals that provide services independently or through an incorporated office are likely to be subject to the Act. The Act deals with personal information about an identifiable individual, including employee information.

'Employees' is defined to mean an individual employed by the organization, and any person acting on behalf of the organization, including under contract, and as a volunteer, student, or apprentice.

The purpose of the Act is to govern the collection, use and disclosure of personal information by organizations for purposes that are reasonable, and in a manner that recognizes the rights of the individual to have their information protected.

[9] "well-being service" means a service relating to an individual's health and well-being that is provided within a common or integrated program or service for the purpose of supporting health services. HIA s.1(1)(x)

Federal Privacy Legislation

5.1.4. Privacy Act

The federal *Privacy Act* applies to government institutions in Canada, including Government of Canada departments, ministries, bodies or offices listed in the schedule, and Crown corporations.

The Act deals with personal information, which is defined to mean information recorded in any form about an identifiable individual, including but not limited to contact, employment, educational, criminal, financial, and health information. Note that health information managed by federal institutions is deemed to be personal information.

The purpose of the Act is to provide protection of privacy to the personal information of individuals held by a government institution, and to provide individuals a right of access to that information.

5.1.5. Personal Information Protection and Electronic Documents Act (PIPEDA)

The *Personal Information Protection and Electronic Documents Act* applies to every organization (as defined within the Act) that, in respect to personal information, the organization collects, uses, and discloses in the context of a commercial activity. It also applies to employee information. An 'organization' is defined to include an association, a partnership, a person and a trade union.

The Act deals with personal information, defined to mean information about an identifiable individual, and personal health information, defined to mean information concerning: the physical or mental health of the individual; any health service provided to the individual; the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; as well as information that is collected: in the course of providing health services to the individual; or incidentally to the provision of health services to the individual.

The Act does not apply to an organization that conducts its business within a province that has been deemed to have substantially similar legislation, including Alberta, BC, and Quebec.[10] who have passed their respective private sector privacy laws. Several provinces have enacted health sector legislation that is also deemed substantially similar to PIPEDA. These include New Brunswick, Newfoundland and Labrador, Nova Scotia, and Ontario. However, if an organization transports personal or health information in a commercial context across provincial boundaries, the information is likely subject to PIPEDA.[11]

[10] To see which legislation applies, see *Provincial laws that may apply instead of PIPEDA - Office of the Privacy Commissioner of Canada*, and "*Find the right organization to contact about your privacy issue*" - Office of the Privacy Commissioner of Canada.

[11] For additional guidance, see *Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts - Office of the Privacy Commissioner of Canada*.

The Act contains a set of Privacy Principles in Schedule 1, which form the basis for the appropriate management of personal and health information. Organizations subject to the Act are required to comply with the obligations set out in Schedule 1.

5.2. Other Legislation

Any legislated requirements that impact the member organizations should be outlined, identifying both the requirements, and any implications for the manner in which the member can participate. For example, a government organization that is involved in supporting youth who have been involved in criminal activities may be subject to the requirements of the *Youth Criminal Justice Act*. Strict restrictions on access to and management of records and information about a young person who has been dealt with under the Act are in place and may have implications on the manner in which a young person is supported, and by whom.

In addition to the listed privacy legislation, there may be other legislation that applies to the organizations involved, or circumstances you are working with. Such legislation may be specific to certain organizations such as schools or police services, or apply more broadly similar to the that dealing with privacy.

For a list of other potential legislation see: Appendix A: Applicable Legislation.

5.3. Matrix

A matrix that outlines the provisions in applicable privacy legislation most likely to apply or support collaborative service delivery is a useful tool to demonstrate which organizations subject to their legislation are able to share personal and health information. The matrix also allows for staff working under other legislation to develop a better understanding as to what their colleagues are authorized to do in similar circumstances.

See Appendix B: Privacy Legislation Disclosure Matrix.

5.4. Disclosure Tool

The disclosure tool builds on the matrix and outlines which provisions under which legislation can be used to share personal and health information in various scenarios. Outlining the type of information that will typically be required across various scenarios will assist in streamlining the decision-making on the disclosure of information. While exceptions exist and individual circumstances may differ, in the majority of situations staff should have a good understanding of what information they require to assess and provide the supports to their clients. This, in combination with the trusting relationships that the framework will enable between organizations will serve to facilitate more efficient and effective collaborative practices.

See Appendix C: Disclosure Tool.

6. Policies, Practices, Procedures

Back

Applicable to Collaborative partnership:
The policies, practices and procedures outlined and adopted by the Collaborative Approach are in addition to those of the member organizations, and should be agreed upon by all participating member organizations, for use during activities that come under the collaborative approach. Where there is a discrepancy between these policies and the organization's own

internal ones, there should be agreement that these will apply. Any areas of conflict should be brought to the attention of the home organization's lead for the collaborative partnership for resolution. In situations where the Lead is not able to resolve the conflict in keeping with the direction of the collaborative approach, they matter can be addressed by the identified position(s) or committee responsible for resolution.

6.1. Minimum Requirements

Legislation serves as a minimum standard that should be applied across the board. 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.

The following is an example of how the responsibilities and policies could be outlined or stated, and should be considered by the members involved in collaborative or integrated services:

The following areas have been approved by the Collaborative Leadership Table and apply to all member organizations in regards to the information that is managed under this collaborative approach. Staff participating in the approach are expected to follow the outlined expectations. Questions or concerns about potential conflicts or issues should be raised with the staff's lead for the collaborative, who will in turn bring it to the committee or lead(s) responsible for addressing them.

6.2. Collection, Use, and Disclosure in General:

Personal and health information will only be collected, used and disclosed in accordance with the authorities granted under the organization's legislation, in keeping with and in support of the collaborative partnership's stated purpose and objectives. Member organizations must identify what information is required for them to be able to best assess the needs of the client, match them against the services they deliver, and to provide those services. Working together, and based on that identification, the organizations should broadly determine what information needs to be collected, used, and how it will be accessed by the member organizations that require it. By going through the process of identifying what information is required to be shared between them in order to facilitate the delivery of the identified programs and services, and what authorities exist for enabling that sharing, the member organizations are enabling a streamlined approach whereby individual staff do not have to decide what can be done in each particular circumstance. Rather, they can simply review that the information requested to be shared falls within that approved set. Note that this refers generally to the type of information, as it is often not always feasible to determine which specific data elements are going to be required. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to. Participating organizations need to be comfortable with the notion that the default position is that 'information will be shared' (where necessary and authorized) rather than starting with a response that is 'No, it will not be shared', (unless proven to be required and necessary). In other words, the organizations have already worked through what is required and authorized.

The intent in using the framework is to develop or outline a set of criteria that if met enables an effective and efficient flow of information. The degree of comfort with this may evolve over time. If situations emerge where reasons to not disclose appear, further discussion at the appropriate group or committee may be necessary. **Note that having been approved as a member organization in the initiative does not give a user authority to access information broadly.** Rather, the user is only authorized to access the information they require of individual clients they are assessing or providing support to.

Only the minimum information that is required to meet the needs the client has identified is to be collected. This includes information that impacts on how those needs are to be assessed and met. Participating staff (users and organizations) should be prepared to identify the relationship between what is collected, and the purpose for which it will be used. Discussions between the members as the processes are being set up will help determine what those sets of information may look like.

Sample Scenario: A number of agencies have decided to work together and have one of their members responsible to conduct intake and a basic needs assessment, on behalf of the other members to whom the individual would be referred. By having one entry point for services, the other agencies can restructure as they no longer would need to perform that function; and the individual client may be referred more appropriately and not have to approach each agency on their own, and repeat their story. When giving up the need for every agency to go through their own needs assessment, the agencies should decide together what is the basic information that must be collected by the entry agency through a collective needs assessment. If there is additional information required by specific agency members beyond that, they can conduct a more in-depth assessment if and when the individual is referred to them. Note that there may be information collected in the initial assessment that is needed by different members. For example, the group may include organizations that offer different services, such as mental health counselling or housing supports. As such, some of the initial collection may include information that is important for the counselling supports that is not required for housing supports. In these situations, the member organizations should only access and use the information they require to assess for and provide their services.

Authority for sharing information must include authority to disclose the information by the organization providing it, and authority to collect the information by the organization receiving it. As organizations determine the desire to work in a collaborative approach with other organizations, they should ensure such an approach and collection is captured under their mandate, or they may need to adjust it.

The following sections reflect the potential application of legislation.

6.2.1. <u>By Public Sector Organizations subject to Provincial/Territorial legislation:</u>

Personal information will only be collected, used and disclosed in accordance with the provisions under the applicable legislation[12], in keeping with and in support of the collaborative

[12] See Appendix A - Specific Legislative References, Note 2, Public Sector Organizations.

partnership's stated purpose and objectives. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to.

6.2.2. By Health Organizations subject to Health Information legislation:

Health information will only be collected, used and disclosed in accordance with the provisions under the applicable health legislation[13], in keeping with and in support of the collaborative partnership's stated purpose and objectives. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to. Such disclosures will be the minimum amount required to achieve those objectives.

6.2.3. By organizations subject to provincial/territorial private sector legislation:

Personal information will only be collected, used and disclosed in accordance with the provisions under the applicable legislation[14], in keeping with and in support of the collaborative partnership's stated purpose and objectives. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to.

6.2.4. By organizations subject to PIPEDA:

Personal information will only be collected, used and disclosed in accordance with the provisions under the *Personal Information Protection and Electronic Documents Act*, complying with the Privacy Principles (known as the Model Code for the protection of personal information) outlined in Schedule 1.[15]

Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to.

6.2.5. By institutions subject to the Privacy Act:

Personal information will only be collected, used and disclosed in accordance with the provisions under the *Privacy Act*, (specifically, Sections 4 - 9)[16], in keeping with and in support of the collaborative partnership's stated purpose and objectives. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to.

6.2.6. By organizations not subject to any privacy legislation:

Where an organization or person is not subject to any privacy legislation17, personal information will only be collected, used and disclosed where required and authorized, in keeping with the collaborative partnership's objectives. The following requirements will be

[13] See Appendix A - Specific Legislative References, Note 3, Health Organizations.
[14] See Appendix A - Specific Legislative References, Note 4, Private Sector Organizations Subject to Provincial/Territorial Legislation.
[15] See Appendix A - Specific Legislative References, Note 5, Private Sector Organizations Subject to PIPEDA.
[16] See Appendix A - Specific Legislative References, Note 6, Federal Institutions.
[17] See Appendix A - Specific Legislative References, Note 7, Organizations Not Generally Subject to Privacy Legislation.

followed, such that the organization is acting as if subject to the *Personal Information Protection and Electronic Documents Act* or substantially similar provincial/territorial legislation. In addition, the non-privacy legislated organization should enter into an agreement with the partner organizations, such as that contained in Appendix E: Sample Commitment Agreement, to demonstrate some level of accountability.

6.3. Collection

Clearly articulating the reasons or purposes[18] for the collection of personal and health information about an individual, along with the manner in which members of the collaborative partnership will undertake that collection, are cornerstones of, and reasons for, the development and implementation of the framework. Privacy legislation generally requires that the personal and health information of an individual be collected directly from the individual it pertains to, subject to specific exceptions. That may seem to preclude the notion of reducing the number of times that an individual needs to repeat his or her story, one of the benefits of a collaborative or integrated service delivery approach. However, the legislation also recognizes and authorizes situations where personal and health information can be collected indirectly. It is critical therefore, that the manner of collecting be defined and that any indirect collection be authorized in accordance with any applicable legislation.

Depending on how the member organizations have set themselves up for the delivery of services under the collaborative approach, there may be additional collection of information by the individual members as they interact with the individual being served.

6.3.1. Direct Collection

While the default position encouraged under privacy legislation and good practice is to collect identifying information directly from the individual that it pertains to, there may be occasions where some or all of it needs to or should be collected indirectly. Those circumstances should be determined and agreed upon in advance, as the collaborative approach is being developed, and staff should be trained on what those circumstances might be.

For the purposes of collaborative partnerships, the collection of personal and health information will generally be a direct collection, that is, the information will be collected directly from the individual to whom it pertains. Exceptions to the direct collection are identified under the following areas.

A. Collaborative Service Delivery

Personal and health information collected by one or more organizations for the stated purposes and use by the members of the collaborative partnership will be deemed to be collected by the organization that is doing the initial collection. Once the information is collected it may subsequently be shared (disclosed) to the other members, and access to the information by those other members will be deemed an indirect collection. Such access will be restricted to those members who require it for the purposes of assessing for and providing services, in keeping with the objectives and outcomes of the collaborative service delivery.

[18] See Appendix A - Specific Legislative References, Note 9, Collection.

B. Integrated Service Delivery:
Personal and health information collected by one or more organizations for the stated purposes and use by the members of the integrated service will be deemed to be collected by the collaborative partnership. That is to say, once the information is collected and made available to the other members, access to the information by those other members will not be deemed a further (indirect) collection, but rather, a use. Such access will be restricted to those members who require it for the purposes of assessing for and providing services, in keeping with the objectives and outcomes of the integrated service approach.

6.3.2. Notice

Staff must understand the rationale and purpose for their involvement with the collaborative approach, how the partnering organizations are working together to support individuals, and must be able to explain it to the clients in a manner that they will understand.

Individuals whose information is being requested directly from them must be provided Notice. Providing Notice means advising the individual of the authority for the collection of their information: what information is being requested, for what purpose (i.e., how it will be used), and to whom it may be disclosed. As well, the contact information of a person/position who can answer any questions the individual may have about the collection must be provided. Legislative references pertaining to informing individuals/providing Notice are listed in Appendix A.[19]

Recognizing that an individual in crisis is not necessarily in the best position or frame of mind to understand or fully comprehend notice or the rationale for consent, there should be a process built in for a review of this with the client once the crisis has been stabilized.

For the purposes of this collaborative partnership, the following position(s) (internal to each member organization or a general administrative role within the collaborative partnership?) could be referenced as that contact person:

Name or title:
Position:
Business Address:
Business Phone Number:
Business Email:

A. Coordinated Service Delivery
When Notice is provided regarding the collection of personal and health information for use by a Coordinated Service Delivery, such Notice shall include information about the coordinated services, and the purpose for which the information is collected, the legal authority for the collection, and indicate that the information necessary for the member organizations to coordinate services will be disclosed.

[19] See Appendix A - Specific Legislative References, Note 10, Notice.

B. Collaborative Service Delivery

When Notice is provided regarding the collection of personal and health information for the use by a collaborative service delivery, such Notice shall include information about the collaborative services, and the purpose for which the information is collected, the legal authority for the collection, and indicate that the information will be disclosed for use by the member organizations involved with the individual in the assessment and delivery of services through the collaborative partnership. Depending on the jurisdiction there may also be a requirement to indicate if the custodian intends to input the information into an automated system.

C. Integrated Service Delivery:

When Notice is provided regarding the collection of personal and health information for the use under an integrated service delivery, such Notice shall include information about the integrated services, and the purpose for which the information is collected, the legal authority for the collection, and indicate that the collection is on behalf of the collective membership and for use by the member organizations involved with the individual in the assessment and delivery of services through the integrated partnership.

Information collected and used in this manner will need to be assessed as to what legislation would apply. For example, in certain jurisdictions, health information legislation applies to the health information of an individual when in the hands of a health information custodian, while the same information when in the custody of or under the control of a public body, or of an organization subject to provincial/territorial privacy legislation, or federal privacy legislation (i.e. PIPEDA or the *Privacy Act*), is defined as 'personal' information. In situations where a custodian is a member of the collaborative approach, the best approach for the management of health information that is required by non-custodians is to manage it as personal information. The same information if required by a custodian should be maintained separately in the custody of or under the control of the custodian.

6.3.3. Indirect Collection

The purpose of the collaborative partnership should be considered when determining if there are occasions where personal and health information should be collected indirectly. Those circumstances should be agreed upon and documented.

Indirect collection (i.e., where information is collected from someone other than the individual to whom it pertains) is authorized by legislation and by the policies of this collaborative partnership in the following situations:[20]

- When the individual has consented to such collection,
- Where there is an urgent need for the information, such as in situations where there are potential or real risks to the health and safety of any person,
- When the individual is not able to provide consent, (e.g., may be due to incapacity, inability to understand the ramifications of consent, or similar situations),

[20] See Appendix A - Specific Legislative References, Note 11, Indirect Collection.

< These are Sample clauses that can be expanded or reduced. References to legislation can be added to as needed. E.g. add the Privacy Act if federal institutions are included in the membership.>

6.4. Use

Privacy legislation restricts the use of information about an individual to the purpose(s) for which it was collected.[21] Personal and health information that is collected for the purposes and objectives set out in this collaborative partnership will only be used for those purposes, unless otherwise authorized. *(The collaborative partnership leads should identify how decisions on what is acceptable to meet the criteria of 'unless otherwise authorized' are made. Sample situations for such uses may include "where authorized or required by law".)*

In addition to the direct or initial purpose, there may be consistent purposes[22] that should be considered. For example, when determining whether or not particular services are beneficial to the individual, conducting an evaluation of the services is consistent with their delivery. Services cannot be effectively provided in isolation of gauging their effectiveness, at both the individual and organizational level.

As noted earlier, there may also be situations where information needs to be used to prevent or deal with situations where there is a potential risk to health and safety of individual(s). If the purpose was identified as one of the initial reasons for collection, then it is duly authorized and used for that initial purpose. If however, that purpose was not identified as part of the original purpose, there is then a need to rely on the provisions in the privacy legislation that authorize such collection and use.[23]

6.5. Disclosure[24]

Disclosure, or the sharing of personal and health information, is the reason for the framework to be implemented. However, that is not the end goal, but rather a means of facilitating organizations to collectively work with individuals and families to provide them with the supports and services they may require. It is often the case that no one organization can typically meet the requirements of individuals who are vulnerable and require assistance with health and social concerns. In order to provide the most holistic and beneficial services to meet an individual's needs, organizations need to work together in as seamless or collaborative a manner as they can, which means they need to talk to each other, and share the information necessary to achieve coordinated or comprehensive case management objectives, which typically should be developed in conjunction with the individual.

Individually, each organization may do a deeper dive, and while working with the individual client(s) may collect greater amounts of detailed information specific to the services that they are providing, but that amount of detail is not likely necessary to be shared. (See also subsection (6.3) Collection)

---

[21] See Appendix A - Specific Legislative References, Note 12, Use.
[22] See Appendix A - Specific Legislative References, Note 13, Consistent Purpose.
[23] See Appendix A - Specific Legislative References, Note 14, Health and Safety.
[24] See Appendix A - Specific Legislative References, Note 15, Disclosure.

Legislation requires that any information being disclosed should be kept to the minimum required for the reasons it is being shared. For these reasons, as the organizations determine why they need to collaborate, and how, it is important to also determine generally the type of information they will need to work with, what they will likely need to share, with whom, and in what manner. Doing so will set them up to better understand how they can and will engage with the individuals they assess and support. As they commence working with the individual themselves, the case plan or approach will serve to identify the information needs more specifically.

Disclosure will only take place if authorized, either by the individual to whom the information relates, in keeping with the policies developed and implemented by the collaborative approach, or as authorized or required by law.

6.5.1. Information Flow

It is important to understand and outline how information is expected to flow, that is, shared by which organization to which organization, and for what purpose. Outlining the flow in a flow chart or map, with an accompanying table may be of value to pictorially demonstrate to users and the individuals whose information is impacted how the information will potentially move.

A sample flow table is included in Appendix K.

6.6. Documentation

An underlying tenet of privacy and access legislation is to provide an individual a right of access to information that is retained by organizations who collect, use, and disclose that individual's information. Organizations working together must determine what information will be maintained, by whom, and how it will be accessed, including access by the individual to whom it pertains.

6.7. Indigenous Data Sovereignty

6.7.1. OCAP® - Ownership, Control, Access and Possession

OCAP®[25] refers to the rights of First Nations to establish and manage sovereignty over their own data. The principles of OCAP® outline[26]:

Ownership refers to the relationships of a First Nation community to its cultural knowledge, data, and information. Ownership asserts that a community, as a group, owns information collectively in the same way that an individual owns their personal information. This is distinct from concepts of stewardship.

Control asserts that First Nation people, their communities, and representative bodies must control how information about them is collected, used, and disclosed. This extends to all aspects of information management, from collection to use, disclosure, and ultimately, destruction of data.

[25] OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC). See https://fnigc.ca/ocap-training/ to obtain a better understanding on good information governance by First Nations and how that must be respected.

[26] From: OCAP® FAQ, OCAP®-FAQs-compressed.pdf, Alberta First Nations Information Governance Centre.

Access determines that First Nations must have access to information and data about themselves and their community regardless of where it is held. It is within the rights of First Nation communities and organizations to manage and make decisions regarding who can access their information.

Possession reflects the state of stewardship of data. Possession is the mechanism to assert and protect ownership and control; possession puts data within First Nation jurisdiction and therefore, within First Nation control.

Individuals who come from a First Nations or Metis background have the same requirements and rights in the manner in which their privacy and confidentiality is managed as they access services and supports.

However, when information that identifies their culture and heritage is being considered for collection, organizations need to ensure that they have a specific requirement for that information, what that requirement is, and how it will be managed. Where such information may be used to assess or evaluate services at a population trend level based on cultural background, the principles of OCAP should be applied. This becomes important for organizations who are considering the use of indigenous information in research and evaluation, especially in breaking out or comparing data that involves cultural differences, for example, interest in identifying the frequency of, or access to, the use of counselling services by groups with differing cultural backgrounds. Discussions with the First Nations Information Governance Centre (FNIGC) may provide further support in understanding how to work within these principles.

6.7.2. Tri Agency Framework

The principles of Ownership, Control, Access and Possession (OCAP®) are one model for First Nations data governance, but this model does not necessarily respond to the needs and values of distinct First Nations, Métis, and Inuit communities, collectives and organizations. The agencies recognize that a distinctions-based approach is needed to ensure that the unique rights, interests and circumstances of the First Nations, Métis and Inuit are acknowledged, affirmed, and implemented.[27]

6.7.3. National Inuit Strategy on Research

The National Inuit Strategy on Research (NISR) outlines the coordinated actions required to improve the way Inuit Nunangat research is governed, resourced, conducted, and shared. This strategy builds upon the important strides taken by Inuit towards self-determination in research by offering solutions to challenges our people have grappled with for decades.28

6.8. Correction

Privacy legislation places a requirement on organizations to ensure the information about individual is accurate and provide the individual the ability to request correction of their information where it is not[29].

[27] From Tri-Agency Research Data Management Policy
[28] From National Inuit Strategy on Research
[29] See Appendix A - Specific Legislative References, Note 16, Corrections.

For the purposes of the collaborative approach, where requests for correction of information that is available to or accessed by the member organizations, the following process will apply:

- Requests for correction received by any staff involved in the collaborative approach should be forwarded to the responsible person or area, as designated by the membership, along with whatever documentation supporting the correction might be presented.
- In situations where staff are requested to correct information while they are in the process of collecting and recording it, and have been presented with the accurate information, they can make the necessary adjustments. However, if the information has been previously recorded, a notation should be made that the information is now being corrected, and forwarded to the area responsible.
- The area responsible will make the appropriate correction.
- In situations where the individual is requesting a change to an opinion, an annotation should be made, indicating what the individual is requesting, but the opinion would not be changed.
- The individual making the request should be advised of the outcome.
- Organizations that have accessed or used the information of the correction are to be notified of any corrections or annotations.

6.9. Retention and Disposition

As noted previously, individuals have a right of access to their own information,[30] which lasts as long as an organization has retained it; as well as a right to know who has accessed their information. Legislation should be reviewed to determine:

- Any requirements an organization has to retain information used to make a decision that directly affects the individual, and for what length of time,
- Any requirements on the organization to document and retain information regarding access to or disclosure of an individual's personal information, and for what length of time[31].

For the purposes of this collaborative partnership, the following areas must be put in place for any information or common records managed on behalf of the collaborative:

- The party responsible for managing the retention and disposition of records is to be identified,
- The retention period needs to be determined and followed, commencing once the file activity has completed.
- Once the retention period is reached, records will be disposed of in a secure manner, with a log kept of which records were disposed of, and when. The logs should refer to a series or set of records by date and type, and not contain any identifying information.
- This retention period does not apply to records that are maintained by the individual members, as their own retention and disposition polices and schedules will apply.

6.10. Terminology / Interpretations

Words matter. However, words are also subject to interpretation, and impacted by work environments, areas of specialization, and other factors. If organizations are going to work together, they have to establish or acknowledge what is meant by the terminology that they have in use. This becomes critical not only with various terms, but also with themes and other

[30] See Appendix A - Specific Legislative References, Note 17, Right of Access by Individuals.
[31] See Appendix A - Specific Legislative References, Note 18, Retention.

elements, including those that are identified within the framework. For this reason, it is incumbent on the organizations to work through what is meant and what is required by areas such as Purpose, Outcomes, and Objectives. Policies and practices should also be examined to identify any areas where there may be dissonance or some level of conflict or disagreement.

An additional area that may have an impact is the interpretation of legislation. Interpretations are often developed and adopted, becoming set in how they influence an organization in the management of information. The following are examples of how that might influence a collaborative approach.

The following is an example of an area that may need to be clarified in how they are to be understood within the context of this collaborative approach.

- Health and Safety: As noted previously, privacy legislation contains a 'safety' clause that, in essence, authorizes the disclosure of personal and health information without consent in situations where there is the potential for a risk to the health and safety of an individual or the public. The actual provisions vary, dependent on the legislation, as noted below, but the intent of such provisions must be that the disclosure can occur to allow for some actions to be taken to alleviate the risk. When examining how they are applied, there must be recognition that the capacity to alleviate risk becomes increasingly diminished the shorter the time frame between disclosure and action, and the risk event itself. In other words, if one waits until the last minute to do anything, the likelihood of eliminating or reducing the risk is significantly less than if there is more time to take appropriate steps. This is especially true if the disclosure requires determining who will take what actions, or worse, the need to obtain even more information before any plan can be put in place to take actions.

There may be additional provisions that could be applied to deal with potential risk situations, including those that deal with the best interests of individuals. They should be considered in conjunction with the 'safety' clauses. This might especially apply in situations dealing with children and youth.

In addition to the above, the interpretation of the provisions, and the determination of what constitutes risk, and levels of risk, all have a potential impact on how organizations deal with and react to risk situations. As such, it is important for organizations that may have to collaboratively deal with risks to health and safety to plan for the potential risk situations that might emerge, and work through how they will respond. Areas to be considered should include the following:

- Do the organizations have policies or practices on what constitutes a level of risk that requires a response, and how they respond? If so, do they align with those of the partnering organizations?
- Is there a threat risk assessment tool in use? Does it meet the needs of the collaborative approach, or is there a need to develop or obtain one that does?
- Is there potential for different responses, timing or levels of intervention to be in place for different member organizations?

Legislative provisions that might apply include:

- Health and Safety provisions[32],

Beyond terminology, there may also be a need to review and address differences in policies and practices by member organizations. For example:

- Consent process: an organization may have adopted a policy that requires the use of consent to disclose for all disclosure situations. Working collaboratively with other organizations may require them to adjust that policy in recognition that there may be situations dealt with by the collaborative approach that allow for or require disclosure without consent. Areas to be considered include the following:
  - Is there a specific reason that the organization chose to adopt the strict adherence to the use of consent that continues to exist?
  - Is there potential for situations to emerge whereby the collaborative members may need to disclose information without the consent?
  - If not, are the other members willing to adopt a different policy on the required use of consent?
  - Note that consent forms may indicate that information will only be disclosed in accordance with the terms of the consent, or where require or authorized by law, which then opens the door to any of the legislative provisions that authorize disclosure without consent applying. Reliance on such wording without any explanation as to what that means may not be seen to be as transparent to the individuals being impacted.

- Consent forms: as noted, privacy legislation is not generally harmonized, including in the requirements outlined for informed consent to the collection, use, and disclosure of personal and health information. In addition, organizations may have adopted or approved specific consent forms for use by their staff. The result is the potential for situations where a consent form is not seen as acceptable by a receiving organization, even if it does meet the legislative requirements of the organization that is using it. As such, it is important for organizations that desire to work collaboratively review their consent forms and processes to determine if they meet each other's requirements, and if not, to develop or adopt ones that do. Areas to be considered include the following:
  - Are any of the member organizations subject to, or require health information that is subject to health privacy legislation?
  - The best approach would be to put in place a consent form that meets the requirements of the most stringent privacy legislation.
  - If a new consent from is adopted for use by the collaborative members, are there any potential implications for consent forms used individually by the member agencies?

See Section 7.6 Consent, below.

6.10.1. Conflict Resolution

Situations may arise where there may be further interpretation or guidance required. Staff participating in the collaborative approach should refer to the policies and training guidance outlined through the framework, or raise the questions with their identified lead. Where the

[32] See Appendix A - Specific Legislative References, Note 14, Health and Safety.

situation may appear to be in conflict with the member's home organization's policies and processes, there may be a need to bring the matter to the committee or area empowered to address it. The outcome of any discussions should be shared as appropriate, and where they have an impact on the larger membership, should be noted accordingly and brought to all staff's attention, as appropriate.

6.11. Training

All staff participating in this collaborative approach are expected to be trained on the following areas:

- Purpose, including objectives and outcomes
- The membership, including the roles the member organizations have.
- The type of information required in respect to the roles they have in the collaborative approach. This should be augmented by an understanding of the use of the Legislative Matrix and Disclosure Tools.
- The governance structure overseeing the collaborative approach, including who they turn to for advice and any issue resolution.
- Policies and processes that have been outlined in the framework, including those outlined in the attached appendices.

Where the collaborative approach involves member organizations that may be subject to some form of accreditation, there may be value in advising those responsible for their accreditation of their involvement in the approach.

6.12. Onboarding

While the membership will generally be determined at the outset of the collaborative approach, there is potential for new, additional member organizations to be identified. As such, the following process may be used when potential organizations are to be considered and invited to participate. Approvals will involve the core membership through the appropriate leadership table.

- The new/potential organization will be provided a copy of the framework or outlined approach, including a description of the purpose, which in turn includes desired objectives and outcomes.
- At a minimum, the new organization is expected to manage information in a confidential manner, and have the technical and environmental capacity to access any systems appropriately (i.e., confidentially, with appropriate security safeguards in place). The capacity assessment (See: Appendix G: Capacity Assessment Tool and Companion Guide) can be useful to demonstrate any additional requirements. Depending on the outcomes of the assessment, the organization will be
  - Supported to address any shortcomings
  - Expected to address any shortcomings
  - Approved to participate
- Once approved to participate, they will be asked to sign the Commitment Agreement *(or whichever similar tool has been developed and implemented)*, and to train their participating and relevant staff.
- Staff must be trained prior to activating their participation, especially when they will be provided with any credentials for access to systems or databases.

7. Information and Records

Back

7.1. Required Information

As noted previously, information that is required by the member organizations involved in the collaborative approach to provide the services to individuals and families should be identified, at a broad level. The information required should be linked to the stated purpose, including objectives and desired outcomes. The roles and areas of responsibility should also be considered, and any differences in the type of information or access required should be identified.

The following is an example of how the information needed can be outlined. More detail can be added as required.

E.g., Information that is to be or has been collected is as follows, and to be used for the following purposes:

Type of Information	Use	Used by
E.g., Contact information, including name, DoB, address	*E.g., Identification, contact*	*E.g., Intake*
E.g., Identified Needs, capacity	*E.g., Conducting an initial screening and assessment for services*	*E.g., Intake*
E.g., Medical, health, social background	*E.g., Conducting a more in-depth assessment once referred to member organization for counselling*	*E.g.,* Caseworker, counselling
E.g., Family history, educational background, employment history,	*E.g., Identifying underlying issues to determine additional supports if required*	*E.g., Caseworker, housing and employment*

Additional uses

As noted above, the use of information is primarily linked to the supports, services and benefits that are being assessed for and potentially offered. There may be situations where other downstream uses also exist. For example, the need to evaluate the effectiveness of an intervention or service delivery approach is important as it will help gauge the value of the collaborative approach. Such a use is deemed consistent with the purpose for which information is collected, as programs and services cannot be delivered in isolation of evaluating their effectiveness.

As well, if the collaborative operates in an environment that optimizes the health and safety of the individuals being provided supports, working to maintain that safe environment may require information to be collected and used for that purpose, in addition to the above stated purposes. It is important to be transparent about this potential use, and it should be identified as the information is collected. *(Optional, to be used as deemed appropriate.)*

7.2. Creating Records

Organizations that collect and use personal and health information in order to provide services to individuals are bound to keep records of any decisions that may impact on those individuals, including records that contain the information on which those decisions are based. Those records may exist in various formats, including electronic and hard copy (e.g., paper).[33]

The legislation differs somewhat on the language, but by and large requires information about and supporting decisions that impact on an individual to be maintained.

When organizations work in a collaborative or integrated service delivery approach, the information they share may be found in records they hold, and they may also create new records. The disclosure of information between organizations needs to be recorded, so as to allow individuals to know whom has accessed their information. Beyond the individual records that each organization creates and maintains, there may be records created that are used by all of the member organizations. Decisions will need to be made as to whether each organization has its own version of the shared information, or if they will use or refer to a common record or set of records.

7.3. Common Records

Common records are those that are not necessarily under the purview of a specific organization, but rather are meant to be used and available to several or all organizations that are involved in the collaborative approach. A good example is the consent form, where an individual has consented to the disclosure of his or her personal information to the other member organizations. Rather than each organization obtaining their own consent for disclosure, it would be more expedient to have one. An added benefit is that by using one form on behalf of all members, it starts to demonstrate how the organizations are working together.

At the same time, there needs to be a demonstrated accountability or responsibility for the management of any record, including common records. Accountability for the management of information and records is often established under legislation, but should also be considered as part of the overall governance when multiple organizations are working together in a collaborative relationship. When governance is established, it will be important to determine what legislation applies to the records the governance body holds on behalf of the collaborative partnership.

Information may be stored in a number of ways, including hard copy and electronic. Consideration should be given to how the member organizations will access the information they require and are authorized for, in a secure manner.

Samples of records that may be approved/identified as common records for the collaborative approach are listed here:

E.g.,

- *Client profile (Name, DoB, Address)*
- *Consent for disclosure form*
- *Common screening and assessment*

[33] See Appendix A - Specific Legislative References, Note 19, Records.

- *Common risk assessment*
- *Comprehensive case management plan*

7.4. Individual Agency Records

Records that are under the control and custody of individual member organizations continue to be the responsibility of that organization, and subject to its policies and applicable legislation. Disclosure of information under the control of member organizations must be managed in a secure manner, and documented appropriately.

7.5. Single Source of Truth

Information that is held as or within a common record must be managed in such manner that it is readily available to authorized users, such that they are working from the same source. System development must take that into consideration, as well as ensuring there is a tracking of changes to information. Users who access this information and subsequently capture and maintain it within their own systems will need to be alerted or advised of changes to the parent information. For this reason, disclosures of and access to information should be recorded.

7.6. Consent[34]

Consent for disclosure differs from consent to participate or for treatment, which may seem obvious, but is at risk of being misconstrued if the separation of those is not clear. Privacy legislation requires that consent be informed, that is, it must be clear to the individual who is being asked to provide consent:

- **What information** is going to be disclosed. The consent form should be relatively clear when describing the type of information, and while it does not need to identify in detail the various data elements that will be disclosed, staff should be prepared to explain or provide examples of what information is being contemplated.
- **To whom**. Individuals have a right to know who has access to their information. Having that information allows the individual to access records about themselves by whomever has then in their custody. However, it can become quite unwieldy to stipulate in the form itself to whom information will or may be disclosed. An alternative to doing so is to provide a list of participating member organizations on the reverse side of the consent form. That may be framed as information about the collaborative, as a means of providing clarity about the collaborative – its purpose, types of services, and member organizations.
- **For what purpose**. Individuals have a right to know how the information will be used. The purpose should be clearly stated, and is likely linked to the purpose and objectives for the collaborative approach. There may be additional purposes that are not as evident, such as ones where required or authorized by law.

Additional requirements or best practices include:

- An acknowledgement that the individual providing the consent has been made aware of the reasons why their information is needed and the risks and benefits to the individual of consenting or refusing to consent.
- The date the consent commences, and the date it expires, if any, and

[34] See Appendix A - Specific Legislative References, Note 20, Consent.

- A statement that the consent may be revoked at any time. (Individuals who withdraw their consent should be advised of the implications of doing so, and that should they revoke their consent, any further disclosures would cease, but the information that has been disclosed prior to the revocation would still form part of a record of services being or having been rendered).

Legislation may also differ regarding whether consent needs to be in writing, which may include electronic formats, or if oral consent is also deemed to be valid.

As noted, consent for disclosure is common across privacy legislation as a means to authorize the disclosure of personal and health information. Given there are differences across the legislation which may at times create some confusion and impediments to disclosure, it may be beneficial for the members of a collaborative approach to agree on a common or universal consent for disclosure form that meets the most stringent requirements. Sample consent forms can be found in Appendix F: Sample Consent Forms.

Note that the use of a common consent for disclosure form does not negate the responsibility of professional staff to explain how the information managed by the professional will be used and disclosed, so to ensure their client is fully aware. Discussions such as these can only serve to enhance the relationships with the individual and support transparency. This requirement is often outlined in the Standards of Practice developed by health and other profession colleges.[35]

Individuals in crisis may not always attend to what they are being told, and in some situations may agree to whatever they think is needed to enable receiving services or supports they require. Revisiting consent with them once their circumstances have settled somewhat will ensure the individual is fully informed.

7.7. Client Information

Client information is to be deemed as sensitive, and needs to be managed accordingly, in a secure and confidential manner such that only those users who require and are authorized to use it have access. Contact or demographic information may not be seen as particularly sensitive, and may even be publicly available, but when combined with the fact that the individual is seeking supports for services, does become significantly more sensitive.

7.8. Client Access

As previously noted, one of the underlying tenets of privacy legislation is that individuals have a right of access to their information. While organizations will individually continue to be responsible for managing access requests for information they hold, policy or practice under the collaborative approach should outline how an individual would gain access to the information held collectively by the member organizations. A preferred approach for access to common records would be to identify a central point of contact. This not only expedites the process; it also continues to support the notion of the collaborative approach. Responses to formal access requests made under privacy legislation have defined timelines that must be met so it will be important to know which legislation applies to common records. The disclosure of records through an informal process may be a preferable approach, although formal requests should be accommodated.

[35] See Appendix A - Specific Legislative References, Note 21, Professional Colleges.

Individuals also have a right to know who has access to, or has accessed their information. As such, organizations involved in a collaborative or integrated service approach should be prepared to provide that information, which, while it may have been provided at the point of giving Notice or consent, may need to be reiterated at any point a request is made.

7.9. User Information

User information includes information about specific staff who are involved in the collaborative approach. Identifying staff who are involved in providing services can be seen to further demonstrate transparency, and clients should be able to know who is working with them or on their behalf. Information that may be part of a credentialling process whereby the user gains access to information systems should be deemed sensitive; other sensitive information (complaints, potential need for restrictions such as due to identified conflicts of interest) will be managed in a secure, confidential manner. Access is to be limited to those who need to know, generally the user's supervisor within their organization, and potentially the Security/System Manager.

7.10. Electronic/paper records

In terms of privacy, there is no differentiation in the content of information whether stored in paper (hard copy) or electronic (soft copy) records. However, the way they are managed is likely to differ significantly, as does access to the information held in them. Paper records are much more difficult to provide broad access to in a confidential manner, and the implications of the type of information that is stored in them should be carefully considered. For example, if information about an individual indicates that they do not react well or perhaps even pose a risk to female staff, such that an alert has been identified that female staff are not to work alone with the individual, that information is pertinent to other areas or organizations involved in providing care. While capturing and placing that information on a case file may be appropriate, it also needs to be readily available and provided to any such organization. Storing it only on a paper file may not always be adequate.

On the other hand, information that is stored electronically can be much more easily provided, and even pushed out, to stakeholders and users. However, the risks of breaches and unauthorized access may differ, and in fact may increase. Adequate safeguards, including training staff on how to responsibly manage access to information systems and the information held within them, must be put in place.

Managing information electronically also provides numerous other benefits. It allows for relatively easy updates to information; the information can be readily accessed, and shared; and extracts of the information such as for reporting or evaluation purposes are more readily undertaken.

Where information is maintained in both paper and electronic versions, it should be clear which is to be deemed the source of truth, and which is a copy. Disposition of the records would need to be managed conjointly.

7.11. Coordinated Case Management Tools

Case management tools are increasingly available for organizations to improve their ability to capture and track the activities taken when supports and services are provided to their clients. They are often implemented through mobile applications, and can be made available to allow

multiple individuals and organizations to work on the same case. Organizations that decide to use case management tools as a means of increasing communications and efficiency when working collaboratively need to ensure that they are developed and implemented properly, with the appropriate mechanisms in place to track and monitor the individual user access and inputs. Safeguards will also be required to prevent unauthorized access.

7.12. Administrative Information

General Information about the collaborative approach, including marketing or communication materials, handbooks, forms, and other resource information that is deemed to be publicly available, is not required to be managed at the same level of security as client information, although it does need to be managed such that its integrity is maintained. It may also be necessary to protect some documentation regarding processes that deal with sensitive or security management.

Sensitivity of third-party information relating to the member organizations including proprietary information that might need to be shared to some degree between the partners, should be identified by the organization, and if deemed to be sensitive or requiring a level of protection, must be managed accordingly. It may be necessary or of value to implement a consistent approach.

Training materials are generally deemed to be administrative, and not required to be managed in a secure manner, although those dealing with steps required to access protected information, or the application of security measures may require secure management.

8. Electronic Information Management

Back

Technology plays a significant role in the management of personal and health information, and supporting the delivery of services in the social and health sectors. The use of electronic records and information has by and large replaced the more traditional hard copy records across many sectors and organizations. It has also facilitated making information and data increasingly available for a large number of uses, including evaluation, research and others. At the same time, with the increased use of and reliance on technology, there is also a substantially increased risk of unauthorized access and use. It is critical therefore, that organizations who rely on or who intend to use technology as a means to expand or enhance their collaboration or integration practices with others pay particular attention to doing so in a privacy conscious manner, and implementing the appropriate tools and safeguards.

Implementing an electronic information system requires careful planning – understanding current and future needs, including but not limited to: security, storage needs (documents and information), storage location, access management, scalability, and legal requirements, type of system (custom built system, off the shelf, Software as a Service), capacity for interface with other systems, vendor/system management. If a decision is made to use an existing system, other considerations may arise, including the ability to create a separate instance or to otherwise ensure there is no cross-over of data or access; ownership/responsibility; and retention beyond the life of the collaboration.

A number of areas within the Framework are related to the use of such a system or platform, and should be considered and applied from that perspective. The following sections touch on

some of the areas that should be considered, whether expanding the use of an existing system or implementing a new one.

Privacy Enhancing Technologies (PET) are tools or design enhancements that are meant to integrate the privacy by design principles. They minimize or reduce risk associated with the collection and management of personally identifying information or data, while enhancing the organization's ability to use it for authorized purposes. Examples include the use of VPNs, encryption, de-identification, anonymization, data-masking, the use of which would be driven in part by the intended users and mechanisms needed to support information flows.

The application of these processes is beyond the scope of this document, but should be an area that is discussed with any the organization's IT vendors, privacy and security professionals, and may need to be further described in a Privacy Impact Assessment (PIA).

8.1. Legal Requirements

Organizations need to ensure that any electronic systems used to manage information and documents meet any legal requirements the organization has. Some of these requirements may be set out in legislation, such as the need to:

- retain information for a set period of time, and the need to securely dispose of it once that has occurred,
- ensure that reasonable security measures are in place,
- maintain the integrity or accuracy of information,
- provide access to authorized individuals, including those to whom the information pertains.

8.2. System Access/Management

Electronic information systems can hold a significant amount of information to which access needs to be appropriately managed, allowing only those who require and are authorized to access the information. It has become an industry standard to manage such access with the use of credentials, using processes such as two-step authentication.

8.2.1. System Access/Credential Management

Managing access to the system or platform, should be delegated to a specific, central role, often linked to or part of the area responsible for security management, and includes credential management. Member Organizations should:

- Identify the lead person responsible to act as a liaison with the System Manager for the purposes of the initiative. That person will in turn identify the staff within their organization who will be users of the system, and interacting with or providing services to clients.
- Ensure that staff users have access to a secure means of connecting with the system, and in a confidential manner/setting, including when using mobile technology.
- Ensure that staff users are trained as required prior to their active engagement with the system.
- Ensure that any changes to staff users are identified, including reassignment, new users, and those who are no longer in the role.

Separate from the individual member organizations, there is a need to identify who is responsible to manage the electronic system on behalf of the members. On the System Management side there is a responsibility to:

- Liaise with the designated lead person for each member organization to identify their users.
- Provide the identified staff the credentials necessary to provide them with access according to their role and authorizations.
- Ensure that users have access to the training as required prior to their active engagement with the system or platform.

Review the lists of users on a periodic basis with the lead persons (e.g., every 3/6 months)

8.2.2. Role Based Access

The implementation of an electronic system for a collaborative approach must take into account the different roles that members may play, and provide or limit access to any personal and health information managed within that system accordingly. This includes but is not limited to the differing roles users may have, as identified or impacted by factors as described in Sections 2., 3., and 8. The different information requirements based on the differing roles should guide the system development and credential management. Access to information by groups who may have roles in specific information needs such as reporting, dashboards, evaluation, complaints, or other collections of information, must be considered from a 'Need to know' and authority-based perspective. Where identifying information is not required nor authorized, access must not be provided.

This may be a means to restrict access to information that needs to be maintained separately, such as health information, managed carefully through the use of heightened levels of permissions.

Not all systems can implement role-based access controls (RBAC), or it may not be possible to apply them to all data elements. As such, there may be a need to implement both the technical (RBAC, access trails) and administrative (e.g. training, access reviews and audits) safeguards.

8.3. Information/Document Management

An electronic information management system can be relatively simple, in that it only holds a minimal amount of information; or can be quite robust, not only having the capacity to hold significant amounts of information, being able to maintain electronic copies of paper or hard copy records, and to segregate the information in whatever manner is deemed appropriate, such that the data or information can be readily available for the specific uses. For example, segregation of the data could assist in the de-identification for use in evaluation and research. The data has to be appropriately managed in its entirety throughout its life cycle. Putting in place the appropriate electronic system can in effect act as an enhanced file room with efficient indexing processes.

Member organizations must determine what they require, based in part on their own systems, the degree of interaction, and the need to rely on shared information.

8.3.1. Information Access/Flows

Whatever level of system is developed or adopted, consideration must be given to how it is to be used, by whom, and for what purpose. Doing so can help inform the flow of information that is captured within the system:

- What information will be entered, and how?
- Will other systems feed into it, and how will that be managed?

- How will it be accessed, by whom?
- How will it be used, will/can it be copied?
- Will it be streamed into other systems?

Descriptions of this process should include any connections to other systems or information sources. Outlining this in a diagram can visually help in demonstrating and understanding the flows.

8.4. Storage

Information stored within an electronic information system is subject to the same rules as any other information or records. The member organizations must establish:

- Where the database or system is located. Are there requirements to maintaining it in the province, in the country? What are the implications for the use of cloud-based servers?
- How the information is backed up, and where the back-ups are stored. At a minimum any physical backups should be stored offsite. If the information is backed up electronically, how is it secured from any potential unauthorized access or loss?
- How the retention and disposition requirements will be applied to the information. Are there different retention requirements for de-identified data, and how will that be managed?

9. Security and Risk/Mitigation

Back

Privacy legislation generally requires that organizations take reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.[36] As technology continues to advance, the proliferation of risks also increases, as do the tools and measures that can be used to counteract those risks. Security of information should exist from the development of a system, through its use and maintenance, and through its eventual ceasing of operation. Responsibility for overseeing the implementation and management of secure processes for the collaborative approach should be identified. The process for reporting of issues, incidents, or breaches should be clearly outlined and provided to all staff involved in the collaborative.

9.1. Responsible Area

Identify the area responsible for security management on behalf of the collaborative approach along with the duties and responsibilities. It is preferable to ensure the person responsible reports at a high enough level to support accountability, and that they work in conjunction with the privacy officer or equivalent.

9.2. Review and Audit (Pre- and post-complaint)

Organizations that use electronic systems when providing support to individuals may not always be able to restrict user access on a data element level. Where technical safeguards are not always available, they can be bolstered by administrative ones. A process should be defined and in place to support the collaboratives' commitment to managing the personally identifying information in its control and custody in a secure manner. Electronic system logs

[36] See Appendix A - Specific Legislative References, Note 22, Security of Information.

showing who has accessed (Read/Write) the personally identifying information of individuals stored in that system should be subject to a review process.

A process involving ad hoc reviews should be undertaken on a regular basis to match access by a user against their authority for that access. Authority for access should be on a need-to-know basis, in keeping with their roles, and only for the clients they are providing services to.

In addition to the ad hoc process, when complaints are received that indicate that potential unauthorized access has occurred, the logs should be reviewed to determine if that has occurred.

9.3. User Environment

9.3.1. Mobile/Work from Home

Technology continues to support and advance the use of systems through remote and mobile methods, reducing the need to work strictly within an office environment. This has been exacerbated or enhanced significantly during the COVID epidemic, and many organizations have moved to a hybrid model where staff may work from both home and office. However, as a result, users may find themselves working in environments that are potentially less secure, and additional safeguards may be required as a result.

In addition, staff should ensure they:

- Use their device in a confidential manner (e.g., ensure the screen is not visible to others who may be in the same room;
- Sign off the system when away from the computer;
- Clear the cache after exiting sensitive applications;
- Do not store any personally identifying information of others (clients specifically) on their device;
- Do not send passwords in clear text (e.g., when sending a password to open a password protected document);
- If using password protection vaults, do not leave them on when away from the device;
- Do not open any emails they do not recognize or that may be from dubious sources;
- Report any breaches or potential breaches.

9.3.2. Bring Your Own Device (BYOD)

Member Organizations may need to rely on the use of mobile devices by their staff to access and manage information under the control of the collaborative. The use of mobile devices must be reviewed and authorized by the Governance to access information, or the system. If member organizations allow their staff to bring their own devices, their use must be managed in a manner that meets the security requirements.

Organizations that allow their staff to use their personal devices to access information should ensure that at a minimum the following are adhered to. Personal devices must have:

- Up-to-date anti-virus software, optimally with automatic updates enabled;
- Up-to-date application patches, optimally with automatic updates enabled;
- Firewalls enabled on laptops and computers;
- Sign-on requirements such as PIN technology or biometrics enabled to logon to the device;
- Secure wi-fi connections.

In addition, personal devices must not be authorized to store information under the control of the collaborative, nor where others may have access to the same devices (E.g., shared computers).

9.4. Breaches

A Breach of Privacy or Confidentiality occurs when there is unauthorized access to, or disclosure of, information that is in the control or custody of an organization. It may also include situations where there is the potential for unauthorized access due to information or records being managed inappropriately. An example of the latter can occur when information meant to be sent to one individual is sent to the wrong individual as the result of using the wrong email address, even when the email is retrieved unopened. Breaches can occur in a number of ways such as through a security breach, theft, unauthorized access by staff or users, and unauthorized disclosure.

All breaches of personally identifying information must be reported as required by the applicable legislation.[37] Breaches that are not addressed under legislation may also be reported, and must be investigated, whether reported to a Commissioner/Ombudsman or not. Breaches under PIPEDA are required to be reported to the federal Privacy Commissioner if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual (s.10.1).

Member Organizations of the collaborative approach are responsible for the appropriate management of identifying personal and health information, including taking the appropriate precautions in ensuring the security of that information, as enshrined in privacy legislation.

All breaches or potential breaches of information are to be reported immediately to the immediate supervisor and to the Security Lead, whether or not information has been accessed.

9.4.1. Preventing a Breach

As noted, legislation (and best practice where an organization might not be subject to legislative oversight) requires organizations to take reasonable safeguards to ensure that any information they control be properly protected from unauthorized access. While the term 'reasonable' provides some flexibility, as does the application of a security/data classification scheme, in situations where a breach occurs the onus would be on the organization to demonstrate that their security framework is appropriate to the type and sensitivity of the information they manage.

The breach prevention approach should include both the security infrastructure (system, access credentials, physical security, etc.) as well as a robust policy and practice approach, that ensures staff are trained on their roles and responsibilities vis-à-vis the management of the information. It includes the use of ongoing audits or reviews of usage by member organization staff (users) along with the infrastructure, processes in place, and access points.

9.4.2. Investigating a Breach

A breach may be surfaced in a number of ways, including a complaint by an individual or third party; an ad hoc or periodic audit/review, disclosure of an error made; the loss of a record, file, or device on which information is stored or accessed, such as a laptop, storage device, or smartphone; or as the result of a system or partial system failure. An investigation of the potential breach should be undertaken by whomever has been assigned that responsibility, and

[37] See Appendix A - Specific Legislative References, Note 23, Breaches.

may take place in parallel with other investigations such as a security investigation. Immediate steps should be taken to seal off the breach, and the review should address the following points:

- The nature of the breach (system, unauthorized access or disclosure…);
- The information that may have been accessed or is the subject of the breach, including the sensitivity of that information;
- How widespread the breach is (e.g., single individual or broad system access).

9.4.3. Assessing and Reporting a Breach

Once it is understood what information has been or may have the potential to be accessed, it will be reviewed to determine what if any implications may exist as a result of that access. The assessment will include determining if there is a need to:

- advise the individual(s) to whom the information relates of the breach;38
- provide any support to that individual to manage the implications of the breach (e.g., access to credit bureau protection in situations where there may be a financial implication, including identity theft)
- advise the Office of the Information and Privacy Commissioner/Ombudsman of the breach;
- implement any additional measures (policy/practice/system changes, additional training, etc.)

Organizations that are potentially impacted will be advised as needed during of the outcome. There should be a process put in place that includes how that is determined, and who is responsible for what steps. If a formal report to the Office of the Information and Privacy Commissioner/Ombudsman is required, that should be undertaken as soon as it is determined that it is required. Note that may take place prior to the internal investigation being completed if the breadth or impact indicates it is required.

Additional resources are available at: Privacy Breach Response, Reporting and Notification – Office of the Information and Privacy Commissioner of Alberta (oipc.ab.ca)

10. Evaluation and Research

Back

Measuring the progress of an initiative is critical to its success, and informs potential changes that might be required. As well, there is a need to understand and assess the potential success of any interventions undertaken by an organization as they work with the client. Both of these require the use of information for the purpose of evaluation, although it will not likely be the same information or data.

While it may be readily easy for an individual being provided support services to understand why certain information is required to meet their needs, that may not be the case when it comes to understanding the need to measure the effectiveness of the services themselves. Staff should be provided some messaging in this area as it's important to be as open and transparent as possible on how information will be used. A balance must be struck between the

[38] Organizations should make a conscious determination about advising individual(s) of a breach, taking into consideration the nature of the breach, and the potential impacts. The default should be to notify the individual(s) but there may be circumstances where that may create a greater risk to the individual, for example if there is potential due to their state of mental health that it may trigger a crisis situation. These are likely rare situations.

need to ensure the client is not deterred from seeking the necessary supports by the need to collect information that demonstrates the effectiveness of the supports.

As previously noted, the minimum amount of personal and health information should be used and disclosed in a way that is as anonymous as possible. That applies to the use of information or data for evaluation and research as well. Wherever possible aggregate, anonymous, or de-identified information should be used. Where it is necessary to use identifying information, it should be safeguarded in a manner commensurate with its sensitivity and value. Identifying information may require to be used for evaluating the success of an individual achieving their identified goals, and in some cases may be necessary to link information in order to allow for analysis of a larger set of data and outcomes, such as may be required in evaluating the effectiveness of an overall program, or for research purposes, but in those circumstances, the identifying information should be stripped as early as possible. Note that the removal of 'identifiers' may not be sufficient to reduce or eliminate the potential for the re-identification of an individual, and the greater the combination of datasets, the more that risk increases. Care must be taken therefore to take the necessary precautions to reduce that risk. Examples can include the elimination of direct identifiers (name, SIN, DoB, address), reduction of specific data (E.g., age instead of date of birth, DA (Distribution Area) instead of postal code, month of service in lieu of date of service…), using larger cell counts, or increasing the level being measured (e.g., going to a higher community level if numbers in a certain target population are too low to preclude re-identification.

Additional areas to be considered include the evaluation or research of First Nations at a population trend level, and the use of ethical considerations.

First Nations have asserted that they have established sovereignty over how their information can be used. In support of this a set of principles have been established – those of Ownership, Control, Access, and Possession, commonly known as OCAP® When information that falls within this sphere (i.e. identifies a First Nations culture and heritage) is being considered for collection, organizations need to ensure that they have a specific requirement for that information, what that requirement is, how it will be managed, and more importantly, they must seek out the guidance on working with First Nations to do so.

The First Nations Information Governance Centre (FNIGC)[39] provides additional resources, and is a good starting point for further support in understanding how to work with these principles.

Ethical Considerations:

Related to the above, disclosures of personally identifying information should not only be considered from the perspective of their legality, (i.e., they have been properly authorized) but they should also be considered from an ethical perspective – is it the right thing to do, with consideration of the impacts or implications at both an individual and a population or societal level. Guidance in this area can be found in a report completed by PolicyWise for Children and Families.[40]

10.1. **Evaluating Individual Outcomes** (E.g., of case plans or interventions)

As services and programs are provided to support individuals, the goals, outcomes, or objectives for that individual should be identified, and there needs to be an ability to measure

[39] https://fnigc.ca/ocap-training/

[40] Ethical Decision-Making Framework for Information Sharing: A Guide for the Homeless-Serving Sector by PolicyWise for Children & Families: Ethical Decision-Making Framework for Information Sharing

progress towards those goals. If there are dependencies on other factors, perhaps being addressed by others, those also need to be measured to an appropriate degree, and a coordinated case management may be required. If that is put in place, the sharing of information about the outcomes or goals of the agreed upon elements should be included. For example, a homeless individual who is seeking support for training and employment, and assistance to find appropriate housing, who is dealing with issues of addiction and mental health, may require support from a number of organizations. A requirement to enter into any training programs may be contingent on the individual obtaining support for the addiction or mental health issues, or may require accommodation in a shelter if not longer-term housing. The organization that is supporting the training may only need to know that the individual has contacted mental health supports, but the organization providing shelter or long-term housing may need more information regarding the mental health concerns, or vice versa.

Organizations that are collaboratively providing services to an individual are working at an identifying level, and any information that needs to be shared is likely also at an identifying level. As such, these organizations need to determine:

- What information is required from which organizations,
- How it will be shared, and
- How it will be managed? (E.g., how will an access request from the individual be managed?)

10.2. **Evaluating the overall approach** (i.e., collaborative approach)

The delivery of programs and services also needs to be evaluated at a broader level, beyond their effectiveness in addressing individual outcomes. Are they doing what they are intended to? Are they targeting the right demographics? Are there gaps that are not being addressed? Measuring this in a collaborative service delivery approach goes back to the identified purpose and objectives, and requires the member organizations to collectively determine how that will be measured. It will also require the sharing of certain information or data that is gleaned from the services that have been delivered, and the success rates of supporting achievement of individual outcomes. However, the analysis should be done at a population trend level, and not include any identifying information in either the analysis, or the reporting, as a general rule. If there is a need to link information at an identifying level, the identifiers should be removed at an early stage in the process, and prior to the analysis being done, with the appropriate safeguards put in place.

The appropriate authorities to share the information even for the purposes of evaluation must be identified, and there may be legislative implications, depending on the legislation that applies. As such, the disclosure of that information may need to be specified in the consent, or somehow be linked to the authorized reasons for disclosure. Where multiple organizations are involved, that becomes more difficult, and there may be a need to rely on a specific member organization to conduct any evaluations, depending on the legislative requirements.[41]

Given this, the following needs to be considered:

- What data is required to evaluate the overall program.
- What data is held by and required from which organizations.

[41] See Appendix A - Specific Legislative References, Note 24, Evaluation.

- What if any data needs to be linked at an identifying level.
- Can it be de-identified and used in that manner to conduct the evaluation?
- If so, the process should be outlined and reviewed to ensure the risk of re-identification is sufficiently negligible.

10.3. Using Data for Research

There is significant interest in accessing health and social data for research purposes. Organizations should determine in advance if they will be undertaking such use themselves, or entertaining external requests for data for research. If so, there are legislative provisions dealing with such use, and there may be additional procedures required.[42]

Organizations providing collaborative or integrated services that are willing to entertain the use of the information under their custody and control for research purposes should ensure they meet all legislative requirements, or where not subject to legislation, should address:

- How respondents (individuals whose information may be used) will be advised. Notice statements and consent forms should reflect such use.
- If identifying data used, how requirements for ethics board approvals will be managed.
- What the onus will be on the research body to obtain consents, and what role, if any, the member organizations will play in that process.
- What the expectations will be regarding the removal of identifiers at the earliest opportunity.
- What other conditions must be met and processes put in place if aggregate data will be used.

[42] See Appendix A - Specific Legislative References, Note 25, Research.

Alberta Specific Appendices

Appendix A: Applicable Legislation - Alberta

Back

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

Version Control

v.3	Updates Due to Changes in the Health Information Act.

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

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

Alberta Electronic Health Record Regulation
118/2010 *(Current to June 22, 2025)*

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

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

Compassionate Intervention Act
Chapter C-21.5 (Current to June 11, 2025)

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

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

***Health Information Act* (HIA)**
H-5 RSA 2000 *(Current to July 2, 2026)*

Health Information Regulation
70/2001 *(Current to July 2, 2026)*

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

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

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

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

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

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

The following legislation is available on the Justice (Canada) Laws Website:
Consolidated Acts (justice.gc.ca)

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

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

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

Notes Re: Specific Legislative References Found in the Framework

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

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

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

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

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

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

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

- With consent, [s.34]
- To avert the risk of harm to a minor, [s.35(1)(m)(i)]
- To avert the risk of significant harm to a person [s.35(1)(m)(ii)], or
- To a person responsible for continuing treatment and care, [s.35(1)(b)].

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

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

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

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

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

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

3. Health Organizations (Back)
   - In Alberta, health sector organizations and entities may be subject to the *Health Information Act* (HIA), which defines "custodians" to include among others:
     (i) a hospital operator of a health services sector in an approved hospital under the Provincial Health Agencies Act other than a hospital operator that is a provincial health agency, regional health authority or provincial health corporation under the Provincial Health Agencies Act;
     (ii) the operator of a continuing care home as defined in the Continuing Care Act other than a continuing care home owned and operated by a provincial health agency, regional health authority or provincial health corporation under the Provincial Health Agencies Act;
     (ii.1) an ambulance operator as defined in the Emergency Health Services Act;
     (iii) a health services delivery organization as defined in the Provincial Health Agencies Act;

(iv) a provincial health agency, regional health authority or provincial health corporation under the Provincial Health Agencies Act;
(vi) a subsidiary health corporation as defined in the Provincial Health Agencies Act;
(ix) a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause;
(ix.2) the Canadian Centre of Recovery Excellence;
(x) a licensed pharmacy as defined in the Pharmacy and Drug Act;
(xii) the Department;
(xii.1) the department administered by the Minister referred to in subclause (xiii.1);
(xii.2) the department administered by the Minister referred to in subclause (xiii.2);
(xii.3) the department administered by the Minister referred to in subclause (xiii.3);
(xiv) an individual or board, council, committee, commission, panel, agency, corporation or other entity designated in the regulations as a custodian,

- The HIA Health Information (Ministerial) Regulation designates a regulated member of each of the following regulatory colleges established under the Health Professions Act as a custodian:
  (a) Alberta College of Dental Hygienists;
  (b) Alberta College of Optometrists;
  (c) Alberta College of Pharmacy;
  (d) College of Alberta Denturists;
  (e) College of Chiropractors of Alberta;
  (f) College of Dental Surgeons of Alberta;
  (g) College of Dietitians of Alberta*;
  (h) College of Midwives of Alberta;
  (i) College of Opticians of Alberta;
  (j) College of Physicians and Surgeons of Alberta;
  (k) College of Physiotherapists of Alberta*;
  (l) College of Podiatric Physicians of Alberta;
  (m) College of Registered Nurses of Alberta.

* denotes new members

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

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

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

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

7. Organizations Not Generally Subject to Privacy Legislation (Back)
   - Where there is potential to involve organizations that are not subject to any oversight legislation as members of a collaborative partnership, a set of minimum standards should be established that mirror the expectations placed on other member organizations through their applicable legislation. Such organizations would be required to demonstrate how they meet those minimum requirements, and assistance to those who are not at the required level could be offered if their involvement is desired. A recommendation is to require the organizations to commit to aligning their policies and practices such that they would comply with private sector privacy legislation in their jurisdiction. In Alberta this would mean aligning with PIPA.

8. Common or Integrated Programs or Services (Back)
   - Both the POPA and HIA contain provisions supporting the collection, use, and disclosure of personal and health information for the purposes of planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service.
   - HIA s.1(1)(e.1) "common or integrated program or service" means a program or service
     (i) that is planned, administered, delivered or managed and, if applicable, monitored or evaluated by one or more public bodies and one or more custodians working collaboratively, and
     (ii) within which health services and any related well-being services are provided;
     (x) "well-being service" means a service relating to an individual's health and well-being that is provided within a common or integrated program or service for the purpose of supporting health services.

   - POPA s.1 (d) "common or integrated program or service", in relation to a public body, means a program or service planned, administered, delivered, managed, monitored or evaluated by

(i) the public body working collaboratively with one or more other public bodies, or
(ii) another public body working on behalf of
(A) the public body, or
(B) the public body and one or more other public bodies;

9. Collection (Back)

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

- PIPA s.11(1) An organization may collect personal information only for purposes that are reasonable.
(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.
- S.14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:
(a) a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
(b) the collection of the information is authorized or required by
(i) a statute of Alberta or of Canada,
(ii) a regulation of Alberta or a regulation of Canada,
(iii) a bylaw of a local government body, or
(iv) a legislative instrument of a professional regulatory organization;
(c) the collection of the information is from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the information to the organization;
(d) the collection of the information is reasonable for the purposes of an investigation or a legal proceeding;
(h) the information may be disclosed to the organization without the consent of the individual under section 20;

- POPA s.4 No personal information may be collected by or on behalf of a public body unless
(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,
(b) that information is collected for the purposes of law enforcement, or
(c) that information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program or service.

- PIPEDA s. 11(1) An organization may collect personal information only for purposes that are reasonable.
(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.

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

10. Notice (Back)

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

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

- PIPA s.7 (3) Notwithstanding section 7(1), an organization may collect, use or disclose personal information about an individual for particular purposes if
  (a) the organization
    (i) provides the individual with a notice, in a form that the individual can reasonably be expected to understand, that the organization intends to collect, use or disclose personal information about the individual for those purposes, and
    (ii) with respect to that notice, gives the individual a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for those purposes,
  ...
- s.13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally
  (a) as to the purposes for which the information is collected, and
  (b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

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

information from that individual for the same purpose and under the same specific legal authority as identified in the notice.

- PIPEDA s. 13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally
  (a) as to the purposes for which the information is collected, and
  (b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.
  (3) Before or at the time personal information about an individual is collected from another organization without the consent of the individual, the organization collecting the personal information must provide the organization that is disclosing the personal information with sufficient information regarding the purpose for which the personal information is being collected in order to allow the organization that is disclosing the personal information to make a determination as to whether that disclosure of the personal information would be in accordance with this Act.
  (4) Subsection (1) does not apply to the collection of personal information that is carried out pursuant to section 8(2).
- PIPEDA SCHEDULE 1 (Section 5) 4.2.3
  The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

- Privacy Act s. 5 (2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

11. Indirect Collection (Back)

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

- HIA s.22(1) A custodian must collect individually identifying health information directly from the individual who is the subject of the information unless subsection (2) applies.
  (2) A custodian may collect individually identifying health information from a person other than the individual who is the subject of the information in the following circumstances:
  (a) where the individual who is the subject of the information authorizes collection of the information from someone else;
  (b) where the individual who is the subject of the information is unable to provide the information and the custodian collects the information from a person referred to in section 104(1)(c) to (i) who is acting on behalf of that individual;
  (c) where the custodian believes, on reasonable grounds, that collection from the individual who is the subject of the information would prejudice
  (i) the interests of the individual,
  (ii) the purposes of collection, or
  (iii) the safety of any other individual,
  or would result in the collection of inaccurate information;
  (d) where collection from the individual who is the subject of the information is not reasonably practicable;
  (g) where disclosure of the information is authorized under Part 5;

(h) where disclosure of the information is authorized by an enactment of Alberta or Canada.
(3) When collecting individually identifying health information about an individual directly from the individual, the custodian must take reasonable steps to inform the individual
(a) of the purpose for which the information is collected,
(b) of the specific legal authority for the collection,
(c) of the title, business address and business telephone number of an affiliate of the custodian who can answer the individual's questions about the collection, and
(d) of the custodian's intention, if any, at that time to input the information into an automated system.

- PIPA s. 7 (1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,
(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,
- s.12 An organization may without the consent of the individual collect personal information about an individual from a source other than that individual if the information that is to be collected is information that may be collected without the consent of the individual under section 14, 14.1, 15 or 22.

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

(p) the information is necessary to plan, administer, deliver, manage, monitor or evaluate a common or integrated program or service.

- PIPEDA s. 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.

12. Use (Back)

- HIA s.27(1) Subject to sections 56.208 (Use of Shared Health Information by a Sharing Custodian) and 56.5 (Use of information accessible via the Alberta EHR), a custodian may use individually identifying health information in its custody or under its control only for the following purposes:
(a) providing health services;
(a.1) subject to the regulations, planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service;
(b) determining or verifying the eligibility of an individual to receive a health service;
(c) conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline;
(c.1) responding to complaints made or legal actions taken against the custodian;
(d) conducting research or performing data matching or other services to facilitate research if
    (i) the requirements in sections 49 to 52 and 53 to 56 have been met with respect to research described in section 49, or
    (ii) the requirements in sections 52.1 to 56 have been met with respect to research described in section 52.1;
(e) providing for health services provider education;
(f) carrying out any purpose authorized by an enactment of Alberta or Canada;
(g) for internal management purposes, including planning, resource allocation, policy development, quality assurance, quality improvement, monitoring, audit, evaluation,

reporting, obtaining or processing payment for health services and human resource management.

- PIPA s. 16(1) An organization may use personal information only for purposes that are reasonable.
  (2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.

- POPA s. 12(1) A public body may use personal information only
  (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
  (c) for a purpose for which that information may be disclosed under section 13, 15 or 16.

- PIPEDA s. 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).

13. Consistent Purpose (Back)

- The HIA is silent on the definition of consistent purpose. However, the Act does require that an individual from whom heath information is collected be advised of the purpose legal authority of the collection (s.22(3)), and is limited to only using it only in accordance with s.27.

- POPA s. 14 For the purposes of sections 12(1)(a) and 13(1)(b), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure
  (a) has a reasonable and direct connection to that purpose, and
  (b) is necessary for performing the statutory duties of, or for operating a legally authorized program or common or integrated program or service of, the public body that uses or discloses the information.

- Privacy Act s.9(4) Where personal information in a personal information bank under the control of a government institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not included in the statement of consistent uses set forth pursuant to subparagraph 11(1)(a)(iv) in the index referred to in section 11, the head of the government institution shall
  (a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and
  (b) ensure that the use is included in the next statement of consistent uses set forth in the index.

14. Health and Safety

(Back)

- HIA s. 35(1) A custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information
  (m) to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize
  (i) a risk of harm to the health or safety of a minor, or
  (ii) a significant risk of harm to the health or safety of any person,

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

- PIPA s. 20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:
  (a) a reasonable person would consider that the disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
  (g) the disclosure of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

- PIPEDA s.7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
  (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;
  (5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.1).

- Privacy Act s.8 (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
  (m) for any purpose where, in the opinion of the head of the institution,
  (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result
  from the disclosure, or
  (ii) disclosure would clearly benefit the individual to whom the information relates.

15. Disclosure
(Back)

- HIA s.31 No custodian shall disclose health information except in accordance with this Act.
- S.34 (1) Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure in accordance with this section.
- See also Note 19 – Consent Requirements, below.

- S.35(1) A custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information
(a) to another custodian for any or all of the purposes listed in section 27(1) or (2), as the case may be,
(a.2) to a regulated health services provider who is not a custodian and who is providing team-based health services to an individual,
(a.3) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for
    (i) planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service, and
    (ii) the performance of the duties of the officer, employee or member to whom the information is disclosed,
(b) to a person who is responsible for providing continuing treatment and care to the individual,
(c) to family members of the individual or to another person with whom the individual is believed to have a close personal relationship, if the information is given in general terms and concerns the presence, location, condition, diagnosis, progress and prognosis of the individual on the day on which the information is disclosed and the disclosure is not contrary to the express request of the individual,
(d) where an individual is injured, ill or deceased, so that family members of the individual or another person with whom the individual is believed to have a close personal relationship or a friend of the individual can be contacted, if the disclosure is not contrary to the express request of the individual,
(e) to an official of a penal or other custodial institution in which the individual is being lawfully detained if the purpose of the disclosure is to allow the provision of health services or continuing treatment and care to the individual,
(h) for the purpose of a court proceeding or a proceeding before a quasi-judicial body to which the custodian is a party,
(i) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information,
(l) to an officer of the Legislature if the information is necessary for the performance of the officer's duties,
(m) to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize
    (i) a risk of harm to the health or safety of a minor, or
    (ii) a significant risk of harm to the health or safety of any person,

(n) if that individual lacks the mental capacity to provide a consent and, in the opinion of the custodian, disclosure is in the best interests of the individual,
(p) if the disclosure is authorized or required by an enactment of Alberta or Canada,

- PIPA s.19(1) An organization may disclose personal information only for purposes that are reasonable.
(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.
- s.20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:
(a) a reasonable person would consider that the disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
(b) the disclosure of the information is authorized or required by
    (i) a statute of Alberta or of Canada,
    (ii) a regulation of Alberta or a regulation of Canada,
    (iii) a bylaw of a local government body, or
    (iv) a legislative instrument of a professional regulatory organization;
(c) the disclosure of the information is to a public body and that public body is authorized or required by an enactment of Alberta or Canada to collect the information from the organization;
(f) the disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation
    (i) undertaken with a view to a law enforcement proceeding, or
    (ii) from which a law enforcement proceeding is likely to result;
(g) the disclosure of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;
(h) the disclosure of the information is for the purposes of contacting the next of kin or a friend of an injured, ill or deceased individual;
(m) the disclosure of the information is reasonable for the purposes of an investigation or a legal proceeding;
(n) the disclosure of the information is for the purposes of protecting against, or for the prevention, detection or suppression of, fraud, and the information is disclosed to or by
    (i) an organization that is permitted or otherwise empowered or recognized to carry out any of those purposes under
        (A) a statute of Alberta or of Canada or of another province of Canada,

- POPA s.13(1) A public body may disclose personal information only
(a) if the disclosure would not be an unreasonable invasion of personal privacy under section 20 of the Access to Information Act,
(b) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
(c) if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure,
(d) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,
(e) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,

(f) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information,
(g) to an officer or employee of the public body or to a member of the Executive Council if the information is necessary for the performance of the duties of the officer, employee or member,
(h) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service and for the performance of the duties of the officer, employee or member to whom the information is disclosed,
(k) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,
(p) to a public body or a law enforcement agency in Canada to assist in an investigation
(i) undertaken with a view to a law enforcement proceeding, or
(ii) from which a law enforcement proceeding is likely to result,
(q) if the public body is a law enforcement agency and the information is disclosed
(i) to another law enforcement agency in Canada, or
(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,
(r) so that the spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted,
(s) to the surviving spouse or adult interdependent partner or a relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy,
(t) in accordance with section 15 (*research purposes)* or 16,
(y) to an officer of the Legislature if the information is necessary for the performance of the duties of that officer,
(z) for the purpose of supervising an individual under the control or supervision of a correctional authority,
(aa) to a lawyer or student at law acting for an inmate under the control or supervision of a correctional authority,
(cc) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize
(i) a risk of harm to the health or safety of a minor, or
(ii) an imminent danger to the health or safety of any person,
(ee) to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor, or
(ff) to another public body for the purpose of carrying out data matching to create data derived from personal information under section 17(1).
(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner.

- PIPEDA s. 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
    (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
    (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,
    (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.

16. Corrections (Back)

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

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

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

- PIPEDA 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.

17. Right of Access by Individuals (Back)

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

- HIA s. 7(1) Subject to section 56.61 (*Right of Access to Information accessible via the Alberta EHR*), an individual has a right of access to any record containing health information about the individual that is in the custody or under the control of a custodian.
  (2) The right of access to a record does not extend to information in respect of which a custodian is authorized or required to refuse access under section 11, but if that information can reasonably be severed from a record, an individual has a right of access to the remainder of the record.
  (3) The right of access to a record is subject to the payment of any fee required by the regulations.

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

- PIPEDA 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.

18. Retention (Back)

- HIA The Act does not address retention specifically, other than to indicate that the Lieutenant Governor in Council may make recommendations regarding the retention of records.
- Health Information Regulation s. 6 For the purpose of section 34(2)(e) of the Act (*Consent requirements*), each of the following is an additional requirement:
  (b) in the case of consent that is given orally,
  (iv) the custodian must record the consent in a manner that is
  (A) accessible to the custodian at a later time, and
  (B) capable of being retained by the custodian for a period of 10 years.

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

- POPA s. 6 If an individual's personal information will be used by a public body to make a decision that directly affects the individual, including a decision made using an automated system, the public body must
  (a) make every reasonable effort to ensure that the information is accurate and complete, and
  (b) retain the information for at least one year after using it so the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by
    (i) the individual,
    (ii) the public body, and
    (iii) if the body that approves the records retention and disposition schedule for the public body is different from the public body, that body.

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

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

19. Records (Back)

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

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

- POPA s.1 In this Act,
  (v) "record" means a record as defined in the Access to Information Act;
- ATIA s.1(u) "record" means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic,

electronic, digital, photographic, audio or other medium, but does not include any software or other mechanism used to store or produce the record;

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

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

20. Consent Requirements (Back)

- HIA s.34 (1) Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure in accordance with this section.
- (2) An individual's consent referred to in subsection (1) is valid only if
(a) the custodian provides the individual with the following information:
(i) the individually identifying health information that the custodian is authorized to disclose;
(ii) the purpose for which the individually identifying health information may be disclosed;
(iii) the identity of the person to whom the individually identifying health information may be disclosed;
(iv) the risks and benefits to the individual of consenting or refusing to consent;
(v) the date the consent is effective and the date, if any, on which the consent expires;
(vi) that the individual has the right to revoke the consent at any time,
(b) the individual, in writing, electronically or orally,
(i) authorizes the custodian to disclose the individually identifying health information, and
(ii) acknowledges that they have been informed of the risks and benefits referred to in clause (a)(iv),
(c) where consent is given in writing or electronically, the individual signs the consent,
(d) where consent is given orally, the custodian records, in writing or electronically, that
(i) the information referred to in clause (a) was provided to the individual, and
(ii) the individual gave the required authorization and acknowledgment under clause (b),
and
(e) any additional requirements set out in the regulations have been met. (See also Note 18 - Retention)
(3) A disclosure of individually identifying health information made under this section must be carried out in accordance with the terms of the consent.
(4) An individual may revoke a consent
(a) in writing, electronically or orally, regardless of the manner in which the consent was given, and
(b) only if the revocation complies with requirements set out in the regulations, if any.
- (5) A custodian must record, in writing or electronically, the revocation of a consent.

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

- POPA Regulation s.2(2) An individual's consent to a public body using or disclosing any of the individual's personal information under section 12(1)(b) or 13(1)(c) of the Act
  (a) must meet the requirements of subsection (3), (4) or (5),
  (b) must specify the personal information to which the consent relates,
  (c) must specify to whom the personal information may be disclosed and how the personal information may be used, and
  (d) must specify the date on which the consent is effective and, if applicable, the date on which the consent expires.
  (3) For the purposes of this section, a consent in writing is valid if it is signed by the individual who is giving the consent.
  (4) For the purposes of this section, an electronic consent is valid if
  (a) the head of the public body has established rules respecting the purposes for which electronic consent is acceptable,
  (b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),
  (c) the public body has explicitly communicated that it will accept electronic consent,
  (d) the electronic consent
    (i) is accessible by the public body so as to be usable for subsequent reference,
    (ii) is capable of being retained by the public body,
    (iii) can be authenticated in a manner that allows the individual giving the consent to be identified, and
    (iv) meets the information technology standards, if any, established by the public body,
  (e) the electronic consent includes the electronic signature of the individual giving the consent,
  (f) the electronic consent is provided in a manner consistent with the electronic signature requirements in section 16(2) of the Electronic Transactions Act, and
  (g) the association of the electronic signature with the consent is reliable for the purpose for which consent is given.
  (5) For the purposes of this section, a consent that is given orally is valid if
  (a) the head of the public body has established rules respecting the purposes for which consent that is given orally is acceptable,

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

- PIPEDA s.7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,
(a) collect that information unless the individual consents to the collection of that information,
(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,
(c) use that information unless the individual consents to the use of that information, or
(d) disclose that information unless the individual consents to the disclosure of that information.
(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

- Privacy Act s. 5 (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).
- s.7 Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

- s.8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.
- s.19 (2) The head of a government institution may disclose any personal information requested under subsection 12(1) that was obtained from any government, organization or institution described in subsection (1) if the government, organization or institution from which the information was obtained
  (a) consents to the disclosure;

21. Professional College (Back)
    - *Health Professions Act* (HPA) s.1(1) In this Act,
      (e) "college" means the college of a regulated profession;

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

    - The following Schedules list the health professions under the HPA. As such, a member of any of the professions is deemed to be a regulated health services provider under the HIA.

SCHEDULES

Green highlights *indicates designation as custodians under the HIA.*

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

The following provisions under the HIA may place some responsibilities and requirements on those members, even if they are not custodians under the Act, depending on the services they provide under specified relationships.

- s.1(1) (u.1) "*regulated health services provider*" means a health services provider regulated under the Health Professions Act;
- (v.4) "team-based health service" means a health service provided or carried out by 2 or more *regulated health services providers*, at least one of whom is not a custodian, working collaboratively;
- 35(1) Subject to sections 56.2091(a) and 56.63(a), a custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information
  (a.2) to a *regulated health services provider* who is not a custodian and who is providing team-based health services to an individual,

22. Security of Information (Back)

- HIA s.60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
  (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,
  (b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information,
  (c) protect against any reasonably anticipated
  (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or
  (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
  and
  (d) otherwise ensure compliance with this Act by the custodian and its affiliates.
  (2) The safeguards to be maintained under subsection (1) must include appropriate measures
  (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, and
  (b) for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.
  (3) In subsection (2)(a), "electronic health records" means records of health information in electronic form.

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

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

- PIPEDA 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).

23. Breaches (Back)

- HIA s.60.1(1) Subject to the regulations, an affiliate of a custodian must as soon as practicable notify the custodian in accordance with the regulations of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or under the control of the custodian.
  (2) Subject to the regulations, subsections (4) and (5) and section 85.1, a custodian must as soon as practicable give notice in accordance with the regulations and subsection (3) of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or under the control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.
  (3) The notice required by subsection (2) must be given to
  (a) the Commissioner,
  (b) the Minister, and
  (c) the individual who is the subject of the individually identifying health information.
  (4) A custodian must consider all relevant factors, including the factors prescribed by the regulations, in assessing for the purposes of subsection (2) whether there is a risk of harm to an individual.
  (5 If a custodian considers that giving notice under subsection (2) to an individual who is the subject of individually identifying health information could reasonably be expected to result in a risk of harm to the individual's mental or physical health, the custodian may decide not to give notice to the individual, in which case the custodian must immediately give notice to the Commissioner of the decision not to give notice to the individual, and the reasons for the decision, in accordance with the regulations.

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

- POPA s.10(2) If an incident occurs involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody or under the control of a public body where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, unauthorized access or unauthorized disclosure, the public body must give notice, without unreasonable delay, of the incident to the following:

(a) the individual to whom there exists a real risk of significant harm;
(b) the Commissioner;
(c) the Minister.
(3) A notice given under subsection (2) must comply with the prescribed requirements.

- PIPEDA s. 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.

24. Evaluation (Back)

Evaluating the effectiveness of a service or program should be deemed a use that is consistent with the initial purpose for which the personal information is collected and used. The ability to disclose personal and health information for purposes of evaluation should also be considered and conducted in compliance with legislation.

- HIA s.27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:
(a.1) subject to the regulations, planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service;
(g) for internal management purposes, including planning, resource allocation, policy development, quality assurance, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.
- HIA s.35(1) Subject to sections 56.2091(a) and 56.63(a), a custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information
(a) to another custodian for any or all of the purposes listed in section 27(1) or (2), as the case may be,
(a.3) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for
(i) planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service, and
(ii) the performance of the duties of the officer, employee or member to whom the information is disclosed,

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

25. Research (Back)

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

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

- PIPA s. 14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:
  (j) the organization collecting the information is an archival institution and the collection of the information is reasonable for archival purposes or research;
  (k) the collection of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about;
- Similar provisions exist for use [s.17(k),(l)] and disclosure [20(p),(q)] without consent.

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

- PIPEDA s.7(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if
  (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;
  (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
  (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

- Privacy Act see Note 14, section 8

Appendix B: Alberta Privacy Legislation Matrix

Back

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

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

Listed Legislation:

APPLICABLE PROVINCIAL LEGISLATION

Protection of Privacy Act (POPA)		Back

Collection:

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

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

Use:

Who (Organization)	Can Use What Information	Comments
Public Bodies under POPA, (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	A public body may use personal information only • for the purpose for which the information was collected or compiled or for a use consistent with that purpose, 12(1)(a)	• This section recognizes the legitimate use of information, and ties the use to the stated purpose(s). For this reason, the purpose should be well articulated and cover the intentions. Consistent use must be demonstrable. (E.g. evaluating the effectiveness of a service is consistent with the delivery of that service.)
	• if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, 12(1)(b) or	• Individuals can provide consent for a specific use of their information. Use of their information is restricted to the stated purpose(s). Consent may be written. Electronic, or verbal consent is also allowed, subject to certain conditions, and should be recorded.
	• for a purpose for which that information may be disclosed under section 13, 15 or 16. 12(1)(c)	• The listed sections outline when information may be disclosed to a public body. If the disclosure is for an authorized purpose under those sections, the public body is authorized to use that information.
	• A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner. 12(4)	• This section limits the public body to only use the information to the degree required.

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA, (Includes provincial, municipal and local government bodies, school authorities. This also includes those working on their behalf, defined as 'employees'.)	Public body may disclose Personal information only:		Note: "A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner. 13(4) Note: This section is permissive, not required (unless otherwise noted). The word 'only' means that one or more of the provisions listed must apply before disclosure can occur.
	• for the purpose for which the information was collected or compiled or for a use consistent with that purpose, [13(1)(b)]	• to any person responsible for fulfilling the stated purpose.	• Recognizes the legitimate use of information, and ties the use to the stated purpose(s). Consistent use must be demonstrable. (e.g. evaluating effectiveness of a service is consistent with the delivery of that service.)
	• if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure [13(1)(c)]	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given.	• Supports the individual having some control over who can access their information. Generally, the consent form should name an organization
	• for the purpose of complying with an enactment of Alberta or	• to any person responsible for or identified within the enactment.	

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada, [13(1)(d)]		rather than an employee within it.
	• for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure, [13(1)(e)]	• to any person responsible for or identified within the enactment.	• References the need to comply, i.e. “must do” with the obligations laid out in the enactment, or in accordance with a legislative instrument.
	• for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information, [13(1)(f)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Includes both a ‘can respond’ and ‘must respond’, depending on the enactment’s wording. • Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
	• to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member, [13(1)(g)]	• to any employee of the public body as required by their position and duties.	• May apply to staff beyond those delivering the specific program. (e.g. may include staff responsible for administrative support, data analysis, etc.)
	• to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for	• to any employee of a public body who is involved in the common or integrated program or service, as required by their position and duties.	

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service and for the performance of the duties of the officer, employee or member to whom the information is disclosed, [13(1)(h)]	• to any person who requires the information to determine suitability and eligibility.	• Limited to disclosure between public bodies involved in the administration and other activities related to common or integrated programs or services; it does not limit participation by other organizations under other provisions, but would not support disclosure to them unless they are acting on behalf of a public body as 'employees'[43]. See also the provision under the HIA outlined at the bottom of this table.
	• for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit, [13(1)(k)]	• to any public body, or an agency that meets the definition of law enforcement, and related to a law enforcement proceeding underway or likely to take place.	• Not limited to programs run by public bodies, e.g., when an individual applies for supports by an agency.
	• to a public body or a law enforcement agency in Canada to assist in an investigation • undertaken with a view to a law enforcement proceeding, or • from which a law enforcement proceeding is likely to result, [13(1)(p)]		• Authorizes disclosure to a public body that may require it for an investigation and proceeding under an act, as well as to a law enforcement agency. Evidence of a proceeding, including an investigation may be requested.
	• if the public body is a law enforcement agency and the information is disclosed (i) to another law enforcement agency in Canada, or	• to any law enforcement agency in Canada and outside of Canada	
Public Bodies under POPA			

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

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public Bodies under POPA	(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority, [13(1)(q)]		• Authorizes disclosure of information between a public body that is deemed law enforcement to other law enforcement agencies.
	• if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize a risk of harm to the health or safety of a minor, [13(1)(cc)(i)]	• to any person who may be involved in addressing risk of harm to a minor (under the age of 18)	
	• if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person, [13(1)(cc)(ii)] Note: POPA Regulation states: For the purposes of the Act, "imminent danger" includes a situation in which the head of a public body believes, on reasonable grounds, that (i) there is a significant risk of harm to the health or safety of a person, and (ii) disclosure of personal information is necessary to protect the health or safety of the person; [1(1)(b)]	• to any person who may be involved in addressing the risk of an imminent danger to any person	• Organizations using this should be prepared to provide rationale/argument of the potential for harm. There may be a need to provide the public body with information to assist in their decision making. • While the bar is somewhat higher, the definition of Imminent harm found in the regulations mirror the definition in the Health Information Act. Where there is imminent danger, action should be enabled early enough to prevent it. The use of a risk assessment tool may be of value. There may also be a need to provide the public body with information you have to assist in their decision making.

Who (Organization)	Can Disclose What Information	To Whom	Comments
	• to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor. [13(1)(dd)]	• to any organization meeting the criteria that is involved in services to minors, or has implications for the minor, if in the best interests of the minor.	• This somewhat mirrors the *Children First Act*, and authorizes disclosure of information about the minor or their parent or guardian if in the best interests of the minor. There may be a need to provide the public body with information to assist in their decision making. Note that there is no prescribed person or body.
Public bodies under POPA authorized under the HIA	• A public body may disclose personal information to a custodian or other public body for the purpose of providing a common or integrated program or service to or in respect of an individual. [38.1(1)] • Individually identifying health information disclosed by a custodian to a public body for the purpose of providing a common or integrated program or service must not be disclosed	• to a public body or custodian that is a participant in the common or integrated program or service. • limitations on any further disclosure	• This section is contained in the Health Information Act rather than the Protection of Privacy Act, and as such may not be readily apparent to any public bodies as they develop and implement a common or integrated program or service. • The limitations identified here outline that disclosure of health information obtained by a public body through a CIPS can only be further disclosed either with consent of the individual to

Who (Organization)	Can Disclose What Information	To Whom	Comments
	by the public body for any other purpose unless (a) the individual who is the subject of the health information has consented to the disclosure, or (b) the public body is required by this Act, the regulations or another enactment to disclose the information. [38.1(2)]		whom it pertains, or where other legislation requires the disclosure.

Access to Information Act (ATIA)
Back

Disclosure

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

Who (Organization)	Can Disclose What Information	To Whom	Comments
	person or of the applicant, or (b) information the disclosure of which is, for any other reason, clearly in the public interest. [37(1)]		

Health Information Act (HIA)	Back

Collection:

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

Who (Organization)	Can Collect What Information	Comments

Use:

Who (Organization)	Can Use What Information	Comments
Custodians as identified in the Act and Regulations (Includes those working on their behalf, defined as 'affiliates'.) Custodians as identified in the HIA and Regulations	One of the purposes of the Act is: to enable health information to be shared and accessed, where appropriate, to provide health services and well-being services and to manage the health system, 2(b) • A custodian may use non-identifying health information for any purpose. [26] • A custodian may use individually identifying health information in its custody or under its control for the following purposes: • providing health services; 27(1)(a)	Health services are defined to mean a service that is provided to an individual for any of the following purposes: (i) protecting, promoting or maintaining physical and mental health; (ii) preventing illness; (iii) diagnosing and treating illness; (iv) rehabilitation; (v) caring for the health needs of the ill, disabled, injured or dying, Well-being services are now included and defined to mean a service relating to an individual's health and well-being that is provided within a common or integrated program or service for the purpose of supporting health services. This outlines that a custodian is not bound by any restrictions in how they use information that is not personally identifying. The listed subsections are allowable uses by the custodian that could generally be relied on within the context of collaborative/integrated services. Others may also apply in specific situations. • Health services as defined in the Act. • Common or integrated program or service" means a program or service

Who (Organization)	Can Use What Information	Comments
Custodians as identified in the HIA and Regulations	• subject to the regulations, planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service; 27(1)(a.1)	(i) that is planned, administered, delivered or managed and, if applicable, monitored or evaluated by one or more public bodies and one or more custodians working collaboratively, and (ii) within which health services and any related well-being services are provided;
	• determining or verifying the eligibility of an individual to receive a health service; 27(1)(b)	• Information that may be required in the assessment of what health services are required.
	• conducting research or performing data matching or other services to facilitate research if (i) the requirements in sections 49 to 52 and 53 to 56 have been met with respect to research described in section 49, or (ii) the requirements in sections 52.1 to 56 have been met with respect to research described in section 52.1;27(1)(d)	• Information that may be used for research or data-matching by the custodian, where the outputs are required by another person (not necessarily a custodian) in research they are managing.
	• carrying out any purpose authorized by an enactment of Alberta or Canada; 27(1)(f)	• Where the purpose is authorized by other legislation, provincial or federal.
	• for internal management purposes, including planning, resource allocation, policy development, quality assurance, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management. 27(1)(g)	• Where necessary for administrative purposes as outlined.
	• An affiliate of a custodian must not use health information in any manner that is not in	• This section restricts the affiliate to only use information to carry out their responsibilities outlined by the custodian.

Who (Organization)	Can Use What Information	Comments
	accordance with the affiliate's duties to the custodian. 28	

Disclosure:

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the Act and Regulations (Includes those working on their behalf, defined as 'affiliates'.)	Health information may be disclosed in the following circumstances: • Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure in accordance with this section. [34(1)] Disclosure without consent: • to another custodian for any or all of the purposes listed in section	• to any person or staff of an organization identified in the consent responsible for the purposes for which consent was given. • a custodian that discloses individually identifying diagnostic, treatment and care information must inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is made (with some exceptions). [42(1)] • to another custodian	The HIA requires that any collection, use and disclosure "be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances". 2(c) • Consent must be in writing, provided electronically, or oral, and must meet HIA requirements. See the rest of this section (34), along with the regulations. • Exceptions include disclosures to another custodian (s.35(1)(a),s.47), to a police service or Justice Minister (s.37.1,37.2, or 37.3).

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the HIA and Regulations	27(1) or (2), as the case may be, [35(1)(a)] • to a regulated health services provider who is not a custodian and who is providing team-based health services to an individual, [35(1)(a.2)] • (a.3) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for (i) planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service, and (ii) the performance of the duties of the officer, employee or member to whom the information is disclosed, [35(1)(a.3)] • to a person who is responsible for providing continuing treatment and care to the individual, [35(1)(b)]	• to a regulated health services provider such as a psychologist or social worker who is neither a custodian nor an affiliate to a custodian, • to any employee of a public body that is involved in the common or integrated program or service, as required by their position and duties. • to any person responsible for providing continuing treatment and care. • to the person(s) identified with the responsibility of obtaining the information	• For the purposes outlined in s.27, which focus primarily (but not exclusively) on providing health care, and include common or integrated programs or services • This section recognizes the roles that other professions may play in the provision of team based health services, including those that are ancillary to health care per se. • Limited to disclosure between public bodies involved in the administration and other activities related to common or integrated programs or services; it does not limit participation by other organizations under other provisions, but would not support disclosure to them unless they are acting on behalf of a public body as 'employees' • Not limited to health care providers, so applies to entities outside of the formal health system. E.g., schools, social workers, support agencies. Providing the custodian with

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the HIA and Regulations	• for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information, [35(1)(i)] • to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize a risk of harm to the health or safety of a minor, [35(1)(m)(i)] • to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize a significant risk of harm to the health or safety of any person, [35(1)(m)(ii)] • if that individual lacks the mental capacity to provide a consent and, in the opinion of the custodian, disclosure is in the best interests of the individual, [35(1)(n)]	(generally identified within the document issued). • to any person who may be involved in addressing risk of harm to a minor (under the age of 18) • to any person who may be involved in addressing the risk of significant harm to any person • to any person who can address the issue who requires the information and acts in the best interests of the individual	information to assist in their decision may be necessary. • 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. • Organizations using this should be prepared to provide rationale/ argument of the potential for harm. Providing the custodian with information to assist in their decision may be necessary. • While the bar is somewhat higher, where there is a significant risk, action should be enabled. The use of a risk assessment tool may be of value. Providing the custodian with information to assist in their decision may be necessary. • Requires the custodian to determine the lack of mental capacity, and that the

Who (Organization)	Can Disclose What Information	To Whom	Comments
Custodians as identified in the HIA and Regulations	• if the disclosure is authorized or required by an enactment of Alberta or Canada, [35(1)(p)]	• to any person responsible for or identified within the enactment.	disclosure is in the best interests, which while not defined, allows for the custodian to make determination based on the individual and the circumstances. Providing the custodian with information to assist in their decision may be necessary. • Includes both a 'can respond' and 'must respond', depending on the enactment's wording.
	• A custodian may disclose individually identifying health information referred to in subsection (2) without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Solicitor General where the custodian reasonably believes (a) that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and (b) that the disclosure will protect the health and safety of Albertans. [37.3(1)]	• To a police service or the Minister of Justice and Solicitor General	• Authorizes disclosure of demographic and other to police services where there is potential for risk to the health and safety of an individual or group of Albertans, through the possible commission of an offence. There may be situations where the potential offence needs to be identified to assist in the decision making.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Public bodies under POPA authorized under the HIA	• A public body may disclose personal information to a custodian or other public body for the purpose of providing a common or integrated program or service to or in respect of an individual. [38.1(1)]	• to a public body or custodian that is a participant in the common or integrated program or service.	• This section is contained in the Health Information Act rather than the Protection of Privacy Act, and as such may not be readily apparent to any public bodies as they develop and implement a common or integrated program or service.
	• (2) Individually identifying health information disclosed by a custodian to a public body for the purpose of providing a common or integrated program or service must not be disclosed by the public body for any other purpose unless (a) the individual who is the subject of the health information has consented to the disclosure, or (b) the public body is required by this Act, the regulations or another enactment to disclose the information. [38.1(2)]	• limitations on any further disclosure	• The limitations identified here outline that disclosure of health information obtained by a public body through a CIPS can only be further disclosed either with consent of the individual to whom it pertains, or where other legislation requires the disclosure.

Personal Information Protection Act (PIPA)	Back

Collection:

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

Use:

Who (Organization)	Can Use What Information	Comments
Private and non-profit organizations (The act does not apply to non-profit organizations [as defined] but does apply to personal information they manage in connection to commercial activities.)	An organization may use personal information only for purposes that are reasonable. 16(1) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used. [16(2)] An organization may use personal information about an individual without the consent of the individual but only if one or more of the following are applicable: • a reasonable person would consider that the use of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way	The test for 'reasonable' is what a reasonable person would consider appropriate in the circumstances. There must be other conditions present, including notice, etc.. The following listed subsections are allowable uses by the organization that could generally be relied on within the context of collaborative/integrated services. Others may also apply in specific situations. • This addresses situations where consent cannot be obtained but would not likely have been

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

Disclosure:

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

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

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

Children First Act	Back

Collection and Use:

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

Who (Organization)	Can Collect and Use What Information	Comments
		for enabling or planning for the provision of services to the child.

Disclosure:

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

Who (Organization)	Can Disclose What Information	To Whom	Comments
			disclosure additional information, to assist in their decision making.

Canadian Centre of Recovery Excellence Act Back	

Outlines the authority for the Centre of Recovery Excellence (CORE), a crown corporation in the Government of Alberta for the collection, use, and disclosure of personal and health information (PHI) for the purposes outlined. The collection, use, and disclosure, (as outlined in section 13 of the Act) may be in aggregate form, non-identifying if aggregate is not adequate, and identifying only if necessary for its stated mandate. Both the mandate and activities are outlined in section 3.
The mandate is to support an improved approach to mental health and addiction issues by:
• conducting and supporting research, evaluations and innovations related to mental health and addiction issues,
• providing advice, information, reports and the results of research and evaluations to the Minister ..., and
• supporting the provision of services to individuals in Alberta with mental health and addiction issues, and providing provincial, national and international leadership on
  ○ addressing mental health and addiction issues, and
  ○ recovery-oriented systems for providing services to individuals with mental health and addiction issues. [3(1)]
 	
The Centre shall collect, use or disclose
• aggregate information if it is adequate for the intended purpose, and
• non-identifying health information and non-identifying personal information if it is adequate for the intended purpose and the collection, use or disclosure of aggregate information is inadequate for the intended purpose,
• and may only collect, use or disclose personal information and individually identifying health information when necessary for purposes that the Centre is authorized, under this or any other enactment, to collect, use or disclose that information for. [13(3)]
	This Act has provided the Centre with significant authority to collect, use, and disclose personal and health information in order to achieve its mandate.
	
	This requires the Centre to collect information in an aggregate form, or in a non-identifying manner if aggregate is not sufficient for the purposes, or
	
	in an identifying form if neither aggregate or non-identifying is not sufficient.
	
	This section broadly outlines the authority of the Centre.

Canadian Centre of Recovery Excellence Act	Back
The Centre may collect, directly or indirectly, use and disclose information, including personal information and individually identifying health information, for the purposes of fulfilling the Centre's mandate, undertaking the Centre's activities, exercising the Centre's powers and performing the Centre's duties and functions under this Act, and for any other purposes prescribed in the regulations. [13(4)] Personal and health information may be collected from any of the following: • custodian as defined in the Health Information Act, • Minister or department, • public body prescribed in the regulations, • public agency prescribed in the regulations, • organization prescribed in the regulations, • mental health and addiction service provider prescribed in the regulations, or • other persons or entities prescribed in the regulations [13(5)] Personal information and individually identifying health information may be disclosed under this section without the consent of the individual who is the subject of the information. [13(7)]	Note that at this time Regulations have not been enacted, which limits the Centre to the information held by the first two types of entities. This outlines the authority of the Centre to collect the information they require without the consent of the individuals to whom it pertains.

Compassionate Intervention Act	Back
The Compassionate Intervention Act authorizes the issuance of an apprehension order, assessment order, or care plan order when it is determined that an individual is at risk of substantial harm to themselves as a minor or an adult, or to others as a result of the individual's substance use or addiction.	

Collection, Use, and Disclosure:

Who (Organization)	Can Collect and Use What Information	Comments
The Commission may require any person, organization as defined in the *Personal Information Protection Act*, public body as defined in the *Protection of Privacy Act* or custodian as defined in the *Health Information Act* to (a) provide information or answer any questions the Commission considers necessary for the determination of a matter before the Commission, and (b) attend a hearing and provide evidence at a hearing if the Commission considers it necessary for the determination of a matter before the Commission. [8(3)] Collection of records 32(1) If an assessment order has been granted, the Commission may order any person, organization as defined in the Personal Information Protection Act, public body as defined in the Protection of Privacy Act or custodian as defined in the Health Information Act to produce any records to the Commission prescribed by the regulations if, based on an application for an assessment order and the materials before the Commission, the Commission has reasonable grounds to believe that the records would disclose information necessary for the Commission to determine whether a care plan order should be issued. (2) The Commission may order any person, organization as defined in the Personal Information Protection Act, public body as defined in the Protection of Privacy Act or custodian as defined in the Health Information Act to produce to the statutory director any record that the Commission may order to be produced to the Commission under subsection (1) for the purposes of the statutory director's powers, duties and functions under this Act. 2025 cC-21.5 s32;AR 141/2025		• The legislation authorizes members of various organizations who may have been involved with the individual to request an assessment; and directs members of various organizations whether subject to PIPA, POPA, or the HIA, to provide any personal and health information as directed by the Commission for the purposes of informing the assessment and or treatment of the individual.

Emergency Health Services Act	Back

Disclosure:

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

APPLICABLE FEDERAL LEGISLATION

Privacy Act	Back

Collection:

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

Use under the federal Privacy Act:

Who (Organization)	Can Use What Information	Comments
Federal institutions (E.g. RCMP and Health Canada)	Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except • for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; [7(a)] or • for a purpose for which the information may be disclosed to the institution under subsection 8(2) [7(b)].	• This provision outlines that the consent of the individual to whom the information pertains is required for any use of their information with the following exceptions: • This allows the institution to use the information they have collected for the purpose(s) for which it was collected, • This allows the institution to use the information they have collected for the purpose(s) for which it was disclosed to them.

Disclosure:

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

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

Personal Information Protection and Electronic Documents Act (PIPEDA) Back

Collection:

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

Use under the Personal Information and Protection of Privacy Act:

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

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

Disclosure:

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

Who (Organization)	Can Disclose What Information	To Whom	Comments
jurisdiction such as credit card payments.)	• required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; [7(3)(c)]	• to the person(s) identified with the responsibility of obtaining the information (generally identified within the document issued).	• Supports a formal request made by (e.g.) law enforcement, and requires a response. Any challenge (e.g., through the courts) should be based on legal advice.
Federally Regulated Organizations and Private Sector Organizations	• made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, [7(3)(c.1)(ii)]	• to any government institution or part thereof and related to law enforcement, or carrying out an investigation related to law enforcement, of Canada or a province.	• "Government Institution" is not defined in PIPEDA, but given that this section applies to provincial legislation as well, an argument can be made that provincial government departments could make the request.
	• made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that	• 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

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	the disclosure is requested for the purpose of administering any law of Canada or a province, [7(3)(c.1)(iii)] • made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual; [7(3)(c.1)(iv)] • 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 administering a legislation of Canada or a province. • to any government institution or part thereof and related to a potential or current contravention of a law (legislation). • to any organization that has the capacity and	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. • "Government Institution" is not defined in PIPEDA, but given that this section applies to provincial legislation as well, an argument can be made that provincial government departments could make the request. The legislation cited should include the authority to disclose information to a next of kin or authorized representative for the outlined purposes. (E.g., HIA s. 35(1)(d)). • The institution would presumably need the authority to collect such information, including having the legislative responsibility to deal with the contravention.

Who (Organization)	Can Disclose What Information	To Whom	Comments
Federally Regulated Organizations and Private Sector Organizations	• 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)] • made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud; [7(3)(d.2)] • 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	mandate to investigate a breach of an agreement or contravention of the laws of Canada or a province. • to any organization that has the capacity and mandate to investigate or prevent fraud. • 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. • 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. • 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

Who (Organization)	Can Disclose What Information	To Whom	Comments
	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 to identify the individual.	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 person who may be involved in responding to the emergency	• Organizations or persons should be prepared to provide evidence of their authority. The individual whose information is being disclosed should be notified about the disclosure, if they are alive.
	• made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the		• 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

Who (Organization)	Can Disclose What Information	To Whom	Comments
	organization informs that individual in writing without delay of the disclosure; [7(3)(e)]		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, the collecting organization should have authority to collect the information, and the other sources should be advised of 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 B Addendum:
Common or Integrated Programs and Services (CIPS), Care Teams, and Other Back

1. Introduction:

The Government of Alberta, as is true in other jurisdictions, recognizes the provision of care and support services to individuals and families in need often requires collaborative and integrated services from organizations in different sectors, that may fall under different privacy legislation. Recent changes to the *Health Information Act* (HIA) support this trend with the introduction of provisions dealing with:

- Common or integrated programs and services (CIPS),
- Regulated health services provider,
- Team-based health service, and
- Well-being service

2. Legislation supporting CIPS

2.1. The *Health Information Act* defines the following terms:

"common or integrated programs and services" to mean *"a program or service*
(i) that is planned, administered, delivered or managed and, if applicable, monitored or evaluated by one or more public bodies and one or more custodians working collaboratively, and
(ii) within which health services and any related well-being services are provided;

"health service" means a service that is provided to an individual for any of the following purposes:
(i) protecting, promoting or maintaining physical and mental health;
(ii) preventing illness;
(iii) diagnosing and treating illness;
(iv) rehabilitation;
(v) caring for the health needs of the ill, disabled, injured or dying,
but does not include a service excluded by the regulations;

"well-being service" means a service relating to an individual's health and well-being that is provided within a common or integrated program or service for the purpose of supporting health services.

The manner in which health information can be used and shared for the purposes of CIPS is supported be the following provisions, including sections 27 (Use), and 38.1 (Disclosure).

27(1) Subject to sections 56.208 and 56.5, a custodian may use individually identifying health information in its custody or under its control only for the following purposes:
(a) providing health services;
(a.1) subject to the regulations, planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service;

35(1) Subject to sections 56.2091(a) and 56.63(a), a custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information

(a) to another custodian for any or all of the purposes listed in section 27(1) or (2), as the case may be,
(a.2) to a regulated health services provider who is not a custodian and who is providing team-based health services to an individual,
(a.3) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for
(i) planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service, and
(ii) the performance of the duties of the officer, employee or member to whom the information is disclosed,

The act also addresses an element that does not appear in the *Protection of Privacy Act* (POPA), the authority for disclosure by a public body when involved in a common or integrated program or service with custodians.

38.1(1) A public body may disclose personal information to a custodian or other public body for the purpose of providing a common or integrated program or service to or in respect of an individual.
(2) Individually identifying health information disclosed by a custodian to a public body for the purpose of providing a common or integrated program or service must not be disclosed by the public body for any other purpose unless
(a) the individual who is the subject of the health information has consented to the disclosure, or
(b) the public body is required by this Act, the regulations or another enactment to disclose the information.

2.2. The Protection *of Privacy Act* states:

"common or integrated programs and services", in relation to a public body, means a program or service planned, administered, delivered, managed, monitored or evaluated by
(i) the public body working collaboratively with one or more other public bodies, or
(ii) another public body working on behalf of
(A) the public body, or
(B) the public body and one or more other public bodies;

The Act also recognizes in section 4 one of the purposes for the collection of information is:

"No personal information may be collected by or on behalf of a public body unless (c) that information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program or service.

Recognizing the need for member organizations to work together in a relatively seamless manner, the Act goes on to provide authority under sections 5 (indirect collection), 13 (Disclosure), and 14 (Consistent Use), for those members to share the information necessary for the stated services.

5(1) Subject to subsection (3), a public body must collect personal information directly from the individual the information is about unless (p) the information is necessary to plan, administer, deliver, manage, monitor or evaluate a common or integrated program or service.

13(1) A public body may disclose personal information only (h) to an officer or employee of a public body or to a member of the Executive Council if the disclosure is necessary for planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service and for the performance of the duties of the officer, employee or member to whom the information is disclosed,

14 For the purposes of sections 12(1)(a) (Use) *and 13(1)(b)* (Disclosure)*, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure*
(a) has a reasonable and direct connection to that purpose, and
(b) is necessary for performing the statutory duties of, or for operating a legally authorized program or common or integrated program or service of, the public body that uses or discloses the information.

These provisions outline the authority for public bodies and custodians to work together in a collaborative or integrated manner to provide supports and services to individuals and families who would benefit from that ability to work closely together. The personal and health information that is required to deliver those services can be shared between the member organizations without consent, provided that it is necessary for the delivery of those services. The Information Sharing Framework for Alberta aligns well with this approach, and provides guidance on the manner in which member organizations can enable the necessary elements of the collaboration.

3. Private and Nonprofit Member Participation

While the above areas move in the right direction, they do not address the private and nonprofit sectors, other than as noted below, and there are as well a number of points that need to be taken into consideration.

3.1. Public Bodies and Other Organizations

The POPA itself is still limited to only enabling public bodies to participate in CIPS, as the provision does not contemplate the inclusion of other organizations. That said, a public body either on its own, or as part of a group, can enter into agreements with other organizations to provide services on its/their behalf, thereby 'pulling' those organizations under their umbrella. The agreements would need to clearly outline what their roles and responsibilities are, and demonstrate appropriate accountability of the public bodies. These relationships would result in the organizations being deemed 'employees' for the purposes of POPA.

As noted, the HIA does expand the authority for public bodies to disclose information, enabling them to work with custodians and share information through a CIPS.

3.2. Custodians and Other Organizations

The HIA goes somewhat further, not only in recognizing the ability to enter into a CIPS with public bodies, but also in the ability for others to play a role. The Act defines additional terms that are relevant to collaborative services:

"authorized user" means a person, other than a custodian, authorized under Part 5.1 to use shared health information or to use health information accessible via the Alberta EHR;

"health services provider" means an individual who provides health services;

"team-based health service" means a health service provided or carried out by 2 or more regulated health services providers, at least one of whom is not a custodian, working collaboratively;

"*Regulated health services provider"* means *"a health services provider regulated under the Health Professions Act;*

The HIA identifies that a "well-being service" is one that is delivered within a CIPS, and is meant to support the delivery of heath services. An argument can be made that would include addressing deficits in the social determinants of health. Providers of these services may include members of a health profession, as defined above.

While specific regulated health professions are also identified as custodians, there are several who are not, yet may be involved in the delivery of a team-based health service, including psychologists and social workers. Team-based health services may involve a custodian, but that is not a requirement. As noted previously, the HIA authorizes the disclosure of personal health information to these regulated professionals when they are delivering team-based health services.

Given the above, team-based health services may include non-custodians, who include regulated health services providers, and who may be staff of various organizations.
Note there are additional requirements that may need to be met, including the development of a privacy impact assessment when contemplating a CIPS.

Appendix C: Disclosure Tool (Alberta)

Back

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

Use of the Tool:

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

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

Version Control

v.3	Updates Due to Changes in the Health Information Act.

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

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

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

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

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

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

Back

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

Purpose

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

Policy

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

Legislation

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

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

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

- What information it pertains to (e.g., personal information, health information)
- Who is subject to the legislation (e.g., government organizations, health service providers, non-government organizations)
- What authority exists to collect, use, and disclose the information (e.g., legislated, with consent, for specific purposes)

- How the information should be managed (i.e., in a secure manner, conducting Privacy Impact Assessments)
- What oversight and accountability measures exist (e.g., Office of the Information and Privacy Commissioner, Privacy Breach Reporting)

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

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

Non-Profit Organizations

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

Contracted and Other Service Relationships

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

This is important from a couple of perspectives:

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

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

The relationships are recognized by legislation as follows:

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

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

Privacy Training

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

Health and Safety

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

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

Roles

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

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

Policy/Practice

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

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

What Staff Need to Know

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

Area	Item	Notes
	Other members Other Areas	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 Liaisons	*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.* *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 (if applicable)	The staff and individuals may have an expectation, or the collaborative approach may have identified that the services will be delivered within a safe and healthy environment.	One of the goals may be to ensure the supports and services are provided in a manner that creates a safe place for individuals and staff. That means if any risks to someone's health or safety emerge, steps will be taken to minimize that risk, working with others if necessary. That might require the sharing of some information about the individuals involved or impacted by the risk, to deal with the situation. Such a disclosure or sharing will take place notwithstanding consent, as the best interests of all individuals must be top of mind. Staff who interact directly with individuals need to explain this to the individuals being served in a manner they can understand.
2. Legislation		
2.1 Privacy Legislation in Alberta	*Protection of Privacy Act* (POPA)	POPA applies to public bodies (government entities in Alberta), including provincial municipal and others. The act sets out the rights of access and of privacy, and the expectations on how the public bodies are to manage their obligations regarding

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

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

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

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

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

Area	Item	Notes
	Child Youth and Family Enhancement Act	The Act also authorizes the disclosure of health information about the child by a custodian to a service provider when necessary for the purposes of enabling or delivering services when it is in the best interest of the child. The *Child Youth and Family Enhancement Act* provides authority for the department of Children's Services to assess and determine if there is a need to provide services to a child that is in need of intervention. The act also places a requirement on any person who has reasonable and probable grounds to believe that a child is in need of intervention, to report that to a director (under the Act) or a police officer. The Act also contains a number of provisions providing authority for the collection and disclosure of personal and health information when conducting an assessment or investigation or providing services under the Act.
	Health Professions Act	The *Health Professions Act* sets out the authorities for the establishment of professional Colleges under the Act, and to manage information relative to the regulated members. Colleges are authorized to set Standards of Practice and Codes of Conduct for its members. These standards may impose additional requirements on its members regarding the management of personal and health information. A number of the colleges have been identified in the HIA Regulations as custodians, which then requires the members of those colleges who provide a health service to comply with the HIA. In addition, Regulated Health Service Providers, who would include the members of other Colleges, are defined under the HIA, and enabled to participate in the use of health information, depending on the work they are providing. They are not deemed to be custodians,however, although if working on behalf of a custodian ould be deemed an affiliate.
2.6 Contracts and Agreements	Employees and Affiliates	As noted above, privacy legislation defines employees (POPA, PIPA) and affiliates (HIA) as individuals (and others) working on behalf of the organization, and may include volunteers, and those working under a contract or agreement. The

Area	Item	Notes
		legislation authorizes the disclosure to and use of information by these entities where it is required for the purposes of providing the services that is expected of them. Contracts or agreements should ensure the entity manages the information in such a manner that the host organization remains accountable for the information in compliance with the legislation. This may have implications on the entity in how they can use or disclose the information, which should be a consideration when they are involved in collaborative or integrated service delivery approaches.
3. Working with Individuals		
3.1 Authentication / Verification *(If applicable)*	Need to authenticate or verify identity	When determining the eligibility of individuals for services, there may be a need to know who the individual is. The member organizations will have determined if such a need exists, and the methods for doing so.
	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.

Area	Item	Notes
	Notice Revisiting Notice	Notice or notification is a requirement under privacy legislation whenever personal and health information is being collected directly from the individual, which is also the default (but not the only) manner of collection. providing notice means advising the individual what information is required to be collected, under what authority, and used for what purpose. It should also indicate to whom the information may be disclosed, and the name or title of someone who can answer their questions about the collection must be provided, along with their business phone number and address. Beyond the formal requirements, it is important for staff working with the individual to explain what 'Notice' means in a way the individual can understand. (See also Deemed Consent, 7.1 below) 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 Required Information	*Authority to collect information is driven by the purpose. Legislation authorizes the collection of personal and health information for specific purposes, which generally have as their foundation the reason why services are being assessed for and delivered. Staff need to be clear about the purpose for working together, and how the collection of information relates to that purpose.* *When the member organizations work through their intentions for working collaboratively, and what they hope to achieve, they should 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.

Area	Item	Notes
	POPA	POPA defines allowable purpose for the collection of personal information to be limited to • Where authorized by an enactment of Alberta or Canada, • Where required for law enforcement purposes, • Where directly related to and necessary for an operating program or activity of the public body. (see POPA s.4) Many programs and services delivered by government are based on legislation or some form of legislative instrument. However, there are also many programs and services that have been implemented under the authority/approval of the 'Head' of the public body.
	HIA	HIA outlines that health information can be collected for specific purposes primarily focused on the determination of need for and delivery of health services. (See HIA s.20, 27) or where authorized under legislation.
	PIPA	PIPA limits the collection of personal information to purposes that are 'reasonable', which is further determined to mean 'what a reasonable person would consider appropriate in the circumstances'.
	Consent	Consent in and of itself should not be seen as the authority to collect information, but rather the means by which permission is granted by the individual for the collection of their information for the stated purpose. In other words, once an organization has determined they have authority to collect information, that it will be collected from the individual, and have provided notice to that individual, consent 'opens the door'. If consent is not provided, the organization has to rely on some other provision to collect the information, if available. (See also Deemed Consent, 7.1 below).
4.3 Limiting Collection	Limiting collection when working on behalf of an integrated service	It's important to have a good understanding of what information is likely to be required, including for when the information is collected on behalf of the member agencies participating in a collaborative or integrated service delivery approach. This may have been identified by listing questions that need to be answered, or completion of forms as part of screening and assessment

Area	Item	Notes
		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 Obtaining additional information	If the individual is not able to provide what is missing, and has indicated involvement with other organizations, it may be feasible to see if they have the required information. This may be especially true in urgent or risk situations where there is limited time or capacity to obtain what is required. The authority to approach them and request that information must be in place. 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.

Area	Item	Notes
4.6 Direct or Indirect collection	Direct collection on behalf of the member organizations	Legislation requires that information be collected directly from the individual it pertains to as a default, unless authorized exceptions are met. Information that is collected on behalf of the collaborative/integrated service delivery partners is deemed to be a direct collection for use by the members, with the intent (and consent) for it to be shared with the members who require it.
	Authorized representative	Instances may arise where an authorized representative is acting on behalf of the individual, and provided they meet the defined legislative parameters and are authorized to exercise the individual's rights and powers (HIA s.104(1), POPA s.54, PIPA s.61), then the representative is acting as the individual, and the collection is deemed to be a direct collection.
	Indirect Collection	Exceptions to collecting the information directly do exist, and the collaborative partnership may have identified what is permissible, or the circumstances should clearly meet the legislated provisions, being vetted as required. (POPA s.5, HIA s.22(2), PIPA s.7(b)). An example of an exception is collection with the consent of the individual.
4.7 Contact Information	Collecting information about contact persons	Collecting contact information is an acceptable part of the process as long as the following criteria are met: • There has to be a reason for having contact information. This can include being able to reach the individual to set up appointments if they are not easily reached (e.g. no phone, couch-surfing,...), or in case of emergency situations. • The contact information is limited to the minimum required, and only for the purposes of connecting with the individual. In other words, it is collected for one purpose, and cannot be used for any other purpose. It may be sufficient in some circumstances to only collect a phone number. It is up to the client to advise their contacts that their information has been provided as a contact, and they should be advised to do so.
4.8 Consent	Requiring consent	The consent of the contact(s) is not required to collect their information. However, if contacted and additional information is requested of them,

Area	Item	Notes
		consent likely would be required, unless other provisions authorize the collection.
5. Use		
5.1 Use	Authorized use	The information about the individual is collected to: *(E.g.)* • *Screening / conducting an initial needs assessment,* • *Providing/facilitating accurate, appropriate referrals,* • *Delivering services meant to address their identified needs.*
5.2 Other Uses	Other authorized uses	There will likely be some consistent or related uses of the information, such as for evaluative purposes. That may include a service evaluation on an individual basis, to ensure the individual is receiving services appropriate to their needs; and on a broader organizational basis to assess the success of the initiative or of the impacts on individual member organizations. Other uses may be appropriate, but may need to be determined on a case-by-case basis. Examples could include dealing with urgent or risk situations, or where required by law, such as the need to report a child in need of intervention. Additional or other uses such as these should likely be discussed with your management team if clear direction has not been provided.
5.3 Risks *(If applicable)*	Risk of harm (to health and safety) Safe and healthy environment	Privacy legislation contains a 'safety valve' that authorizes the disclosure of personal and health information where necessary to prevent or minimize harm. (POPA s.13(1)(CC), HIA s.35(1)(m), PIPA s.20(g)) The language differs, but the underlying intent of the provisions is to allow for actions to be taken to minimize that risk. Where there is an immediate risk to life, requiring an urgent response, police services should be contacted. Where there is an emerging risk, the degree of risk and the response required may shift, and there may be a need to discuss the situation with management. Where the members have identified as part of the purpose for the collaboration that the services are to be delivered in a safe and healthy environment, and a risk to the health or safety of an individual

Area	Item	Notes
		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.
	POPA	POPA identifies a number of circumstances where, if met, disclosure is authorized. These may include: • for the purpose for which it was collected, or a consistent purpose, • if the individual has provided an informed consent, • to comply with an enactment of Alberta or Canada, • to comply with a subpoena, warrant or order issued by someone with authority to compel the production, • to an employee of a public body if the information is necessary for a common or integrated program or service, • to determine or verify someone's suitability or eligibility for a program or service, • to a public body or law enforcement agency to assist with an investigation,

Area	Item	Notes
Authority to Disclose		• to minimize the risk of harm to the health and safety a minor, or an imminent danger to the health and safety of any person. **See** POPA **s.13 for more information, and the exact wording.**
	HIA	HIA identifies the circumstances under which health information can be disclosed. They include: • to another custodian for purposes outlined in s.27, which primarily deal with the provision of health services, • for purposes related to planning, administering, and evaluating a common or integrated program or service (CIPS), • to a person responsible for continuing treatment and care, (this may include non-health care providers) • to any person to avert or minimize the risk of harm to the health and safety of a minor, or a significant risk of harm to the health and safety of any person, • if a person lacks the mental capacity to provide consent and it is in their best interest, • if authorized or required under an enactment of Alberta or Canada, • with the consent of the individual, • where the information relates to the possible commission of an offence, and the disclosure will protect the health and safety of Albertans. (There are limitations on what can be disclosed under this section (HIA s.37.3) **See HIA ss. 27, 34, 35, 37.3 for more information, and the exact wording.**
	PIPA	PIPA limits the disclosure of personal information, identifying a number of circumstances under which it may occur. These include: • with consent of the individual, • where a reasonable person would think if in the best interests of the individual, and consent cannot be obtained in a timely way, • where authorized or required by a statute of Alberta or Canada, or some other regulation, bylaw, or legislative instrument, • to a public body or law enforcement agency to assist with an investigation,

Area	Item	Notes
	Consent	• where necessary to respond to an emergency that threatens the life, health or security of an individual or the public. **See PIPA ss.7, 20 for more information, and the exact wording.** Consent 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	Access through electronic systems Email	*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 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 to provide supports and services to the individuals they are working with. Information may be provided through some other means, if sanctioned by the member organizations, such as by email. However, given that email is inherently not secure, any personal information sent that way should be within an encrypted (preferred) or password-protected attachment. Personal information, including the name or other identifiers of individuals, should not be included in

Area	Item	Notes
		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.
7.3 Understanding	Assist the individual to understand the implications of providing or not	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

Area	Item	Notes
	providing their consent	upon partners to assess and provide them with services needed, - Not consenting to collection means they may still receive the services they need, but not in an efficient or as effective a manner; - Not consenting to sharing means approaching other agencies individually and repeating their story.
7.4 Capacity	The individual providing consent must have the capacity to understand what is required	The individual should be able to understand what they're told. Wording may need to change or be reframed or paraphrased to help them better understand; or there may be a need for interpreter if language is an issue. If the individual is under the influence of drugs or alcohol, consent may not be valid and may have to be revisited/confirmed at a point in the future. If the individual is too young to understand the implications of what consent means, or if they suffer some form of condition that impacts their capacity to understand, there may be a need to determine if someone can legally act on their behalf, or if there is some other provision that authorizes the collection or disclosure of their information.
7.5 Signature	Individuals must sign the consent form	There needs to be some form of verification that the person has actually consented. The normal way is for the consent form to be signed. The *Health Information Act* requires written consent, which includes electronic consent, but the level of authentication must be sufficient to identify the person signing the consent is who they say they are. The HIA, POPA and the *Personal Information Protection Act* allow for oral or verbal consent, negating the need for a signature in those circumstances. Written consent includes electronic consent, but there is a need to authenticate that the person signing the consent is who they say they are, and under POPA the Head of the public body will need to approve a set of rules regarding the use and process for oral or electronic consent. Verbal consent must be properly documented.

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

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

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

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

Area	Item	Notes
		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. (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*

Area	Item	Notes
		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 annotation should be made, indicating what the individual is requesting, but the opinion should not be changed.
9. **Access**		
9.1 Information Access	Accessing required information	Users (staff) of organizations should be provided credentials that allow their access to the appropriate electronic information management system. Authorized users are permitted to access the system and the information they require of the

Area	Item	Notes
		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 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.

Area	Item	Notes
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 Formal requests for access	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. 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

Area	Item	Notes
		in managing the personal information of others has an obligation to help protect the information, including: - Protecting the credentials provided as a user to access the electronic information system, not sharing them or storing them where they may be accessible to others; - 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;

Area	Item	Notes
		- 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 Agreement[44]

Back

Appendix E: Sample Commitment Agreement

Collaborative Approach Participation Agreement

This Agreement is between:

and

and

and

and

and

[44] This version (v.3) has been amended to reflect the changes in the Health Information Act.

Preamble

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

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

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

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

Therefore the parties agree as follows:

1.0 Definitions

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

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

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

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

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

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

2.0 Purpose

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

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

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

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

3.0 Collection, Use and Disclosure of Information

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

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

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

(b) personal and health information which is collected will be used solely for the purposes for which it was collected under this Agreement and for no other purpose unless:

(i) if the party is subject to, and such use is specifically authorized under, the *Protection of Privacy Act*; or

(ii) if the party is subject to, and such use is specifically authorized under, the *Health Information Act; or*

(iii) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection Act; or*

(iv) if the party is subject to, and such use is specifically authorized under the federal *Privacy Act; or*

(v) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection and Electronic Documents Act; or*

(vi) the individual to whom the information pertains has consented to the use;

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

(d) a party agrees to keep personal and health information disclosed to it confidential and will not further disclose it except as required to fulfill the purpose of this Agreement and for no other purpose unless:

(i) if the party is subject to, and such use is specifically authorized under, the *Protection of Privacy Act*; or

(ii) if the party is subject to, and such use is specifically authorized under, the *Health Information Act*; or

(iii) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection Act*; or
(iv) if the party is subject to, and such use is specifically authorized under the federal *Privacy Act*; or
(v) if the party is subject to, and such use is specifically authorized under, the *Personal Information Protection and Electronic Documents Act*; or
(vi) the individual to whom the information pertains has consented to the disclosure;

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

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

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

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

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

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

4.2 The purpose of the Case Management Meetings is to provide a forum where participating parties can jointly assess and provide direction regarding the needs of an individual, and develop a coordinated case management plan. A meeting will occur:
(a) when an individual has been assessed by one of the parties as being in need of supports in a number of areas; and
(b) where the individual consents to, or where it may be in their best interests to participate in the collaborative or integrated service delivery approach to address their needs; and
(c) when a Coordinated Case Management Plan may be required.

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

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

4.5 The Coordinated Case Management Plan referred to in 4.2(c) shall contain the following information:
(a) name, contact information of the subject individual;
(b) date of birth;
(c) gender;
(d) information regarding the subject individual that has led to the determination they are in need of supports, including issues, supports, and factors that may place the individual at risk;
(e) the party that referred the situation to the Case Management Meeting;
(f) the services that are to be provided;
(g) the party that will be responsible for leading service delivery and the parties involved in service delivery; and

(h) whether consent of the subject individual has been obtained for collection, use and disclosure of personal information.

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

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

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

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

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

(ii) to be used in an aggregate form;

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) jointly assess and provide direction regarding the delivery of the collaborative services by the parties;
(b) provide guidance on issues brought forward by the Case Management Committee;
(c) review and evaluate progress of the initiative; and
(d) recommend *(or decide on)* changes to the collaborative approach as required, based on the reviews and evaluations vis-à-vis stated objectives.

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

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

6.0 Responsibilities, Dispute Resolution and Costs

6.1 Responsibilities

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

6.2 Dispute Resolution

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

6.3 Costs

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

7.0 Administrative, Technical and Physical Safeguards

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

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

7.3 The administrative, technical and physical safeguards mentioned in subsection (1) must:
(a) Protect the integrity, accuracy and confidentiality of the Information;
(b) Protect against any reasonably anticipated:
(i) Threat or hazard to the security or integrity of the Information;
(ii) Loss of the Information; and
(iii) Unauthorized access to or use, disclosure, modification or deletion of the Information.

7.4 Where personally identifying information is maintained in a central repository or system for access and use by participating parties, the repository will be managed by *<Identify responsible party>* in such manner that:
(a) the repository meets all of the technical safeguards required as noted in 7.3 above;
(b) only those parties authorized to access it are able to.

8.0 Incident Management

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

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

8.3 In the event of accidental or unauthorized access, use, disclosure, modification or deletion of information, including de-identified or aggregate information, the party responsible shall promptly:
(a) notify all of the other parties of the event;
(b) take all reasonable steps to contain the disclosure; and
(c) take all reasonable steps to prevent a recurrence of the event.

8.4 Where personally identifying information is maintained in a central repository for access and use by participating parties, incident management will also apply in like manner to the information stored therein, with the following requirements:
(a) steps will be taken as required to prevent any further unauthorized access, as required;
(b) the incident will be reported to all members of the (*ACM)* Committee;
(c) a determination will be jointly made by the (*ACM)* Committee on the steps to be taken regarding reporting of the incident.

9.0 Retention and Disposition

9.1 Retention
(a) Each party shall retain the Information according to its policies, procedures or guidelines regarding retention periods.

(b) If a party does not have policies, procedures or guidelines mentioned in subsection (a), that party shall exercise due diligence in adopting or creating policies, procedures or guidelines, in keeping with the standards outlined in the adopted framework.
(c) The policies, procedures or guidelines mentioned in subsection (a) must ensure the Information stored in any format is retrievable, readable and useable for the full retention period.
(d) Where personally identifying information is maintained in a central repository for access and use by participating parties, retention of records will be managed in accordance with (c), with the following provisions:
    (i) Personally identifying information will be kept for a period of *<Identify the agreed upon/legislated time frame>* years;
    (ii) Non-identifying information will be maintained for an additional *<Identify the agreed upon/legislated time frame>* years to enable ongoing trend analysis. *<If required>*

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

10.0 Access Requests

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

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

10.3 Where personally identifying personal information is maintained in a central repository for access and use by participating parties, access requests will be managed by *<Identify the responsible party/area>* as per the following:
(a) Consultation will take place with the parties responsible for the provision (disclosure) of the individual's information. If the providing party is of the view the information should not be disclosed, they should identify the (legal) rationale, and be prepared to assist in defending that decision, should there be a challenge.
(b) Alternatively, the individual may be directed to contact the providing organization for access to specific information/records.

11.0 Accuracy

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

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

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

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

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

12.0 Indemnification <Delete if not required>

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

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

13.0 Review of Agreement

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

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

14.0 Amendments

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

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

15.0 Application / Assignability

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

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

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

16.0 Withdrawal

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

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

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

17.0 Termination

17.1 The parties may agree to terminate this Agreement.

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

18.0 Coming into force

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

19.0 General

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

Division [if applicable]
Organization
Address

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

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

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

20.0 Signatures, Signing Dates and Appendices

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

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

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

_____ _____
(Witness Signature) (Signature)

_____ _____
(print name) (print title)

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

...

Appendix F- Sample Consent Forms[45]

Back

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

Requirements under the HIA[46]:

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

(2) An individual's consent referred to in subsection (1) is valid only if

(a) the custodian provides the individual with the following information:

(i) the individually identifying health information that the custodian is authorized to disclose;

(ii) the purpose for which the individually identifying health information may be disclosed;

(iii) the identity of the person to whom the individually identifying health information may be disclosed;

(iv) the risks and benefits to the individual of consenting or refusing to consent;

(v) the date the consent is effective and the date, if any, on which the consent expires;

(vi) that the individual has the right to revoke the consent at any time,

(b) the individual, in writing, electronically or orally,

(i) authorizes the custodian to disclose the individually identifying health information, and

(ii) acknowledges that they have been informed of the risks and benefits referred to in clause (a)(iv),

(c) where consent is given in writing or electronically, the individual signs the consent,

(d) where consent is given orally, the custodian records, in writing or electronically, that

(i) the information referred to in clause (a) was provided to the individual, and

(ii) the individual gave the required authorization and acknowledgment under clause (b), and

(e) any additional requirements set out in the regulations have been met.

(3) A disclosure of individually identifying health information made under this section must be carried out in accordance with the terms of the consent.

(4) An individual may revoke a consent

(a) in writing, electronically or orally, regardless of the manner in which the consent was given, and

(b) only if the revocation complies with requirements set out in the regulations, if any.

(5) A custodian must record, in writing or electronically, the revocation of a consent.

HIA Regulation[47]:

6 For the purpose of section 34(2)(e) of the Act, each of the following is an additional requirement:

[45] This Appendix (v.3) has been updated due to changes in the HIA.

[46] *Health Information Act* Revised Statutes of Alberta 2000 Chapter H-5 Current as of July 2, 2026

[47] *Health Information Regulation* Chapter/Regulation: 70/2001

(a) in the case of consent that is given electronically, the custodian must ensure that the level of authentication of the consent is sufficient to identify the individual who gives the consent;

(b) in the case of consent that is given orally,

(i) the custodian must set out in their privacy management program the purposes for which the custodian will accept consent that is given orally,

(ii) the purpose for which the custodian seeks consent is a purpose referred to in subclause (i),

(iii) the custodian must authenticate the identity of the individual who gives the consent orally in a manner that is reliable for the purpose of

(A) verifying the identity of the individual, and

(B) associating the consent with the individual,

and

(iv) the custodian must record the consent in a manner that is

(A) accessible to the custodian at a later time, and

(B) capable of being retained by the custodian for a period of 10 years.

HIA Fact Sheet: Consent for disclosures[48]:

Under the HIA, a person can consent to the disclosure of their health information to a third party when there is no authority to disclose without consent. Section 34 authorizes a custodian to disclose identifying health information if the individual has provided consent. The disclosure must follow the terms of that consent. Consent may be obtained in writing, electronically or orally. To be valid, a custodian must inform the individual:

- what health information will be disclosed
- why the information will be disclosed
- who will receive the information
- the risks and benefits of consenting or refusing to consent
- when the consent takes effect and, if applicable, when it ends
- that they can withdraw consent at any time

For written and electronic consent, this information may be included on the consent form. To be valid, the individual must authorize the disclosure and confirm they understand the risks and benefits of consenting or refusing to consent.

For oral consent, the custodian must document, in writing or electronically, that:

- the required information was provided
- the individual authorized the disclosure
- the individual understood the risks and benefits

Electronic or Oral Consent

Privacy legislation deals with electronic and oral consent differently.

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

[48]HIA Fact Sheet: Consent for disclosures Online

authenticated, and records must be maintained and available. Details of the above are in the POPA Regulations.

The HIA also authorizes the use of electronic and oral consent, provided that the means of authentication is sufficient to identify the individual providing consent. If consent is collected electronically or orally, the individual must have been advised of the authority, rationale and other elements listed above.

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

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

Sample Forms:

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

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

Sample 1: Simple consent

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

Sample 2:

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

Sample 3:

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

Sample 4:

Consent for the disclosure of information to organizations working together to provide seamless, integrated services. Disclosure is deemed to be to all of the organizations, provided that the organizations have enabled an integrated service delivery process. This form could be used in a Common or Integrated Program or Service (CIPS) involving public bodies and custodians.

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

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

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

This Consent Form can be adapted by the following steps.

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

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

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

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

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

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

This Consent Form can be adapted by the following steps.

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

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

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

Sample 3:

CONSENT TO DISCLOSE INDIVIDUALLY IDENTIFYING PERSONAL AND/OR HEALTH INFORMATION

Authorized by and in accordance with:

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

Client Information:	Full Legal Name:
	Also Known As:

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

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

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

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

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

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

Name: _____

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

_____

Relationship to client if confirming to be the nearest relative:

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

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

	Type of Service	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*	*Type of Service*
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															
Name of Organization															

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

Name of Organization															
Name of Organization															

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

This Consent Form can be adapted by the following steps.

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

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

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

Sample 4:

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

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[49]. You may choose to indicate that should any new organizations be added as partners, that will only occur once they have gone through a rigorous onboarding process such that they are able to also operate as a seamless member of the integrated approach.
3. If a legally authorized representative is signing on behalf of the client, ask them to provide evidence of the authority they indicate they are acting under, and indicate what that authority is.
4. If the legally authorized representative indicates they are the client's nearest relative as per the *Personal Directives Act* or the *Mental Health Act*, indicate what their relationship is with the client.
5. If any new organizations are added as partners in the collaborative approach, their names should be added and the client or representative should be asked to initial their consent to disclosure.

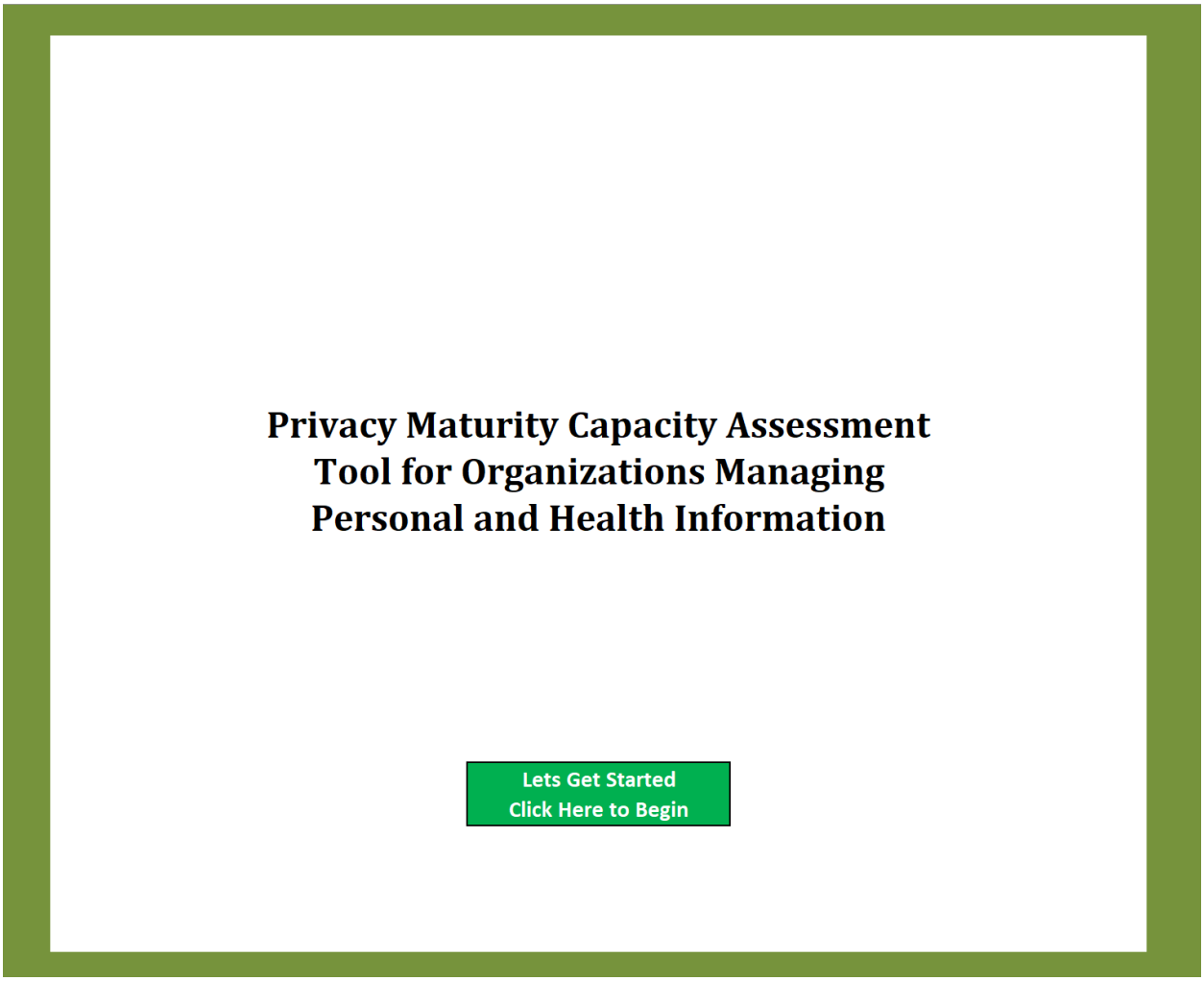
[49] This should only be available if the integrated service delivery partners have gone through a rigorous formalization such as by adopting the Information Sharing Framework, and ensuring they are fully committed to the agreed upon purpose, processes and governance structure.

Generally Applicable Appendices

Appendix G: Capacity Assessment Tool and Companion Guide

The intended purpose for the Privacy Maturity Capacity Assessment Tool (the Tool) is to assist organizations to determine their level of maturity in the way they manage personal and health information in their control or custody. By using the Tool, the organization should be able to determine what areas, if any, they may need to enhance or address, so as to ensure they are managing such information appropriately.

The following are screen prints of the tool, provided for informational purposes. To access and use the tool, go to: https://www.convergementalhealth.org/our-work?tab=resources#tabs. The tables on pages following the Slides provide additional notes for each of the elements under each section, meant to assist the user understand what is expected. The 'Description' mirrors the description in the Tool, and the 'Notes' in combination with the information on the levels is meant to assist the organization determine what they require.



User Guide

NEXT

DESCRIPTION

Please see "Background Information" Tab for additional information regarding what the Privacy Maturity/Capacity Assessment Tool is, and additional information to consider while filling out the tool. Note that for the purposes of expediency, personal information is deemed to include health information.

A Quick Start Guide to using this tool:

- Determine who will complete the assessment. This should be an individual (or multiple individuals) with knowledge of the organization and privacy in general. They may need to consult with other employees in the area.
- Identify project completion timelines and who the results will be shared with.
- Gather all necessary materials for reference (privacy policies, information sharing agreements, consent forms, etc.)
- Decide how often this tool will be revisited. This could be based on time (such as every two or three years) or on need (such as if a new project starts) or as often as the organization wishes.
- Review results on the tool with management/executive and make plans to address deficiencies.

How to use the tool:

- Using the slider at the bottom right of the Excel screen, adjust your zoom level so that the entire tool and the pop-up boxes in Maturity Level 5 are viewable. 80% zoom is the recommended starting point.
- You can move between sections by scrolling down or by clicking the green menu on the left.
- Hover your mouse over the criteria for a description. Hover over the empty dots for descriptions of each maturity level.
- Select the dot for the "current" maturity level which best describes your organization. Then choose the "target" maturity level for what your organization aspires to achieve. (See Companion Guide)
  - If you click the wrong dot you can just choose the correct one. If you need to deselect a dot, right click it, select Format Control, select the Control tab and change the Value from Checked to Unchecked. There is a button to reset all entries at cell GQ108.
- To print only a specific area (for instance, the Dashboard Summary section), click the "Page Layout" tab from the top menu, highlight the section you want to print, select the "Print Area" icon and then the "set print area" option.
- The "All Tables" tab at the bottom displays the results from each of the ten sections on one page for ease of reference and printing.

Things to Consider while filling out the tool:

- **Approximate timeframe:** This will vary depending on the organization and their familiarity with privacy practices.
- The tool is comprised of ten different sections with an average of four different questions to consider per section.
- **Choosing Targets**:
- Discussing your targets with senior management may clarify the long- and short-term goals of your organization and ensure that the privacy officer and management are on the same page.
- A Level 5 maturity rating is an optimized state, but this is not always reasonable or achievable depending on individual factors.
- Use the comment box found below each section to state more detail about your chosen target level. Flag any targets that you are not sure of for further discussion.
- **Flagging, Highlighting and Commenting**:
- Click on the section or title that you want to flag for later.
- In the Excel "Home" menu, choose the "fill colour" (paint can) option and choose a highlighting colour.
- Use the comment box provided below each Principle to identify any comments or concerns that are specific to that section.
- Use the "additional comments" box at the end of the assessment to put any final thoughts/comments that may not be specific to any certain section.

Please see "Background Information" Tab for additional information regarding what a Privacy Maturity Assessment (PMA) is, and additional information to consider while filling out the PMA.

MENU

- User Guide
- 1: Privacy Management
- 2: Purpose for Collecting Information
- 3: Collection
- 4: Use and Disclosure of Information
- 5: Notice / Consent
- 6: Information Management
- 7: Safeguards / Security of Information
- 8: Providing Access
- 9: Managing Compliance
- 10: Evaluation and Research
- Dashboard Summary

1: Privacy Management

BACK NEXT

Organizations that manage personal information are responsible for how it is managed, and should ensure they are structured in a manner that reflects that responsibility throughout the organization, including identifying how it is accountable for compliance with the applicable privacy legislation. If the organization is not subject to privacy legislation, a best practice is to demonstrate alignment between its policies and the *Personal Information Protection Act* (PIPA).

		Maturity Level				
		1	2	3	4	5
Privacy Framework	Current	○	○	○	○	○
	Target	○	○	○	○	○
Complete Understandable Policies	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Governance	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Officer / Duties	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Culture	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Training	Current	○	○	○	○	○
	Target	○	○	○	○	○
Contractor Privacy Awareness	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Breaches	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

MENU

- User Guide
- 1: Privacy Management
- 2: Purpose for Collecting Information
- 3: Collection
- 4: Use and Disclosure of Information
- 5: Notice / Consent
- 6: Information Management

Back

2: Purpose for Collecting Information

NEXT

Personal information is only to be collected for a purpose that relates to an existing or proposed program or activity of the organization. When considering what information is to be collected or required, organizations should identify the purposes for which it is collected along with the roles and impacts of such collection.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

4: Use and Disclosure of

		Maturity Level				
		1	2	3	4	5
Purpose for Collection	Current	○	○	○	○	○
	Target	○	○	○	○	○
Roles and Responsibilities	Current	○	○	○	○	○
	Target	○	○	○	○	○
Relevancy of Information	Current	○	○	○	○	○
	Target	○	○	○	○	○
Privacy Impact Assessments (PIA)	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

3: Collection

NEXT

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization, and in accordance with the applicable legislation. Information should be collected directly from the individual to whom it pertains, unless otherwise authorized.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

		Maturity Level				
		1	2	3	4	5
Limiting Collection	Current	○	○	○	○	○
	Target	○	○	○	○	○
Manner of Collection: Direct	Current	○	○	○	○	○
	Target	○	○	○	○	○
Manner of Collection: Indirect	Current	○	○	○	○	○
	Target	○	○	○	○	○
Accuracy of Personal Information	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

4: Use and Disclosure of Information

NEXT

The use of personal information shall be limited to the purposes identified by the organization, and in accordance with the applicable legislation. The disclosure of information must be with the consent of the individual to whom it pertains, or in accordance with applicable legislation. Where the organization is not subject to any privacy legislation, a best practice is to follow PIPA.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

		Maturity Level				
		1	2	3	4	5
Use	Current	○	○	○	○	○
	Target	○	○	○	○	○
Use: Other Uses	Current	○	○	○	○	○
	Target	○	○	○	○	○
Disclosure: with Consent	Current	○	○	○	○	○
	Target	○	○	○	○	○
Disclosure: without Consent	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

5: Notice / Consent

NEXT

Organizations must be transparent in the collection, use, and disclosure of personal information. This includes the provision of notice where required and obtaining informed consent of the individual to whom the information pertains, unless otherwise authorized. Informed consent means the individual understands what they are consenting to, and has been advised of the consequences of their decision regarding consent.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

		Maturity Level				
		1	2	3	4	5
Notice	Current	○	○	○	○	○
	Target	○	○	○	○	○
Consent	Current	○	○	○	○	○
	Target	○	○	○	○	○
Informed Consent	Current	○	○	○	○	○
	Target	○	○	○	○	○
Consequences of Refusal	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

6: Information Management

NEXT

Personal information that is used to make decisions, along with any such decisions and actions taken, must be appropriately documented, maintained, and disposed of in a secure manner, in accordance with any applicable legislation and legal requirements. Organizations should ensure they maintain records of any holdings of personal information such that they can be readily accessed where required, such as in response to requests by authorized persons.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

4: Use and Disclosure of

		Maturity Level				
		1	2	3	4	5
Documentation	Current	○	○	○	○	○
	Target	○	○	○	○	○
Retaining Personal Information	Current	○	○	○	○	○
	Target	○	○	○	○	○
Disposal of Personal Information	Current	○	○	○	○	○
	Target	○	○	○	○	○
Personal Information Banks/Holdings	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

7: Safeguards / Security of Information

NEXT

Personal information shall be protected by security safeguards that include physical, administrative and technical safeguards. The safeguards in place should coincide with the level of sensitivity of the specific personal information.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

4: Use and Disclosure of Information

		Maturity Level				
		1	2	3	4	5
Information Security Program	Current	○	○	○	○	○
	Target	○	○	○	○	○
Types of Safeguards	Current	○	○	○	○	○
	Target	○	○	○	○	○
Access Controls	Current	○	○	○	○	○
	Target	○	○	○	○	○
Safeguarding Portable Devices	Current	○	○	○	○	○
	Target	○	○	○	○	○
Safeguards Effectiveness Test	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

8: Providing Access

NEXT

An organization shall be open with individuals about the existence, use, and disclosure of the individual's personal information, and provide access as appropriate when requested. Access requests must be processed in accordance with applicable legislation, or where the organization is not subject to legislation, it must have and follow a policy in keeping with the principles of openness. An individual can challenge the accuracy and completeness of the information and ask that it be amended as appropriate.

MENU

User Guide

1: Privacy Management

2: Purpose for Collecting Information

3: Collection

4: Use and Disclosure of

		Maturity Level				
		1	2	3	4	5
Access to Personal Information	Current	○	○	○	○	○
	Target	○	○	○	○	○
Procedures for Requests	Current	○	○	○	○	○
	Target	○	○	○	○	○
Establishing Identity	Current	○	○	○	○	○
	Target	○	○	○	○	○
Challenging Accuracy/Corrections	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

9: Managing Compliance

NEXT

Individuals can challenge the compliance of an organization with applicable privacy legislation or its own privacy policies. The organization will advise individuals where to send their concerns; complaints will be investigated; and changes will be made to practice or policy when warranted.

MENU
User Guide
1: Privacy Management
2: Purpose for Collecting Information

		Maturity Level				
		1	2	3	4	5
Complaints Procedures	Current	○	○	○	○	○
	Target	○	○	○	○	○
Investigating Complaints	Current	○	○	○	○	○
	Target	○	○	○	○	○
Modifying Actions	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.

BACK

10: Evaluation and Research

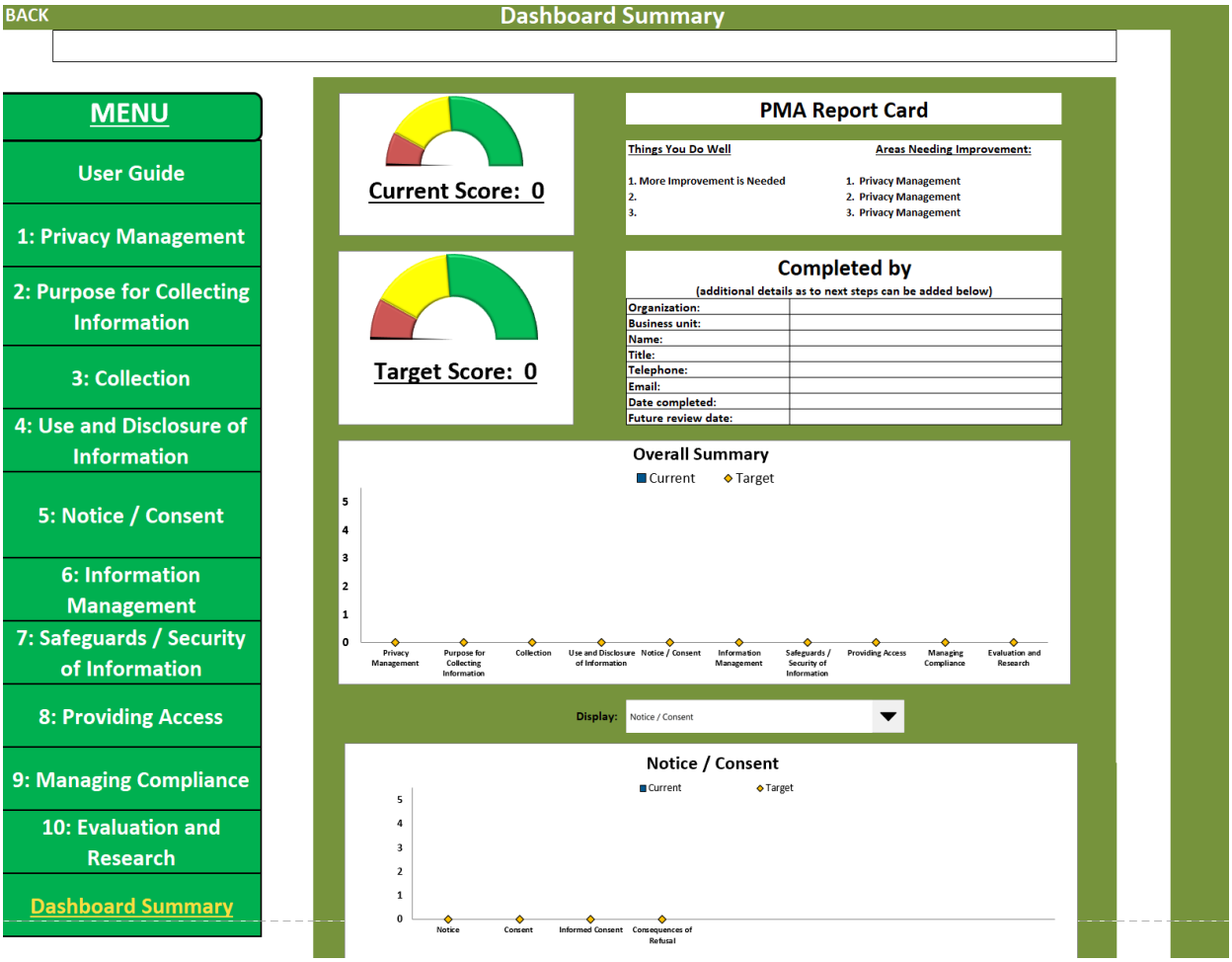
NEXT

The appropriate use of personal information must be in accordance with applicable legislation. Where information is required for evaluation and research purposes, organizations must use it in as anonymous a manner as possible, and ensure that any such research or evaluation is undertaken in such a way that is ethical, and that the confidentiality and privacy of individuals are maintained.

MENU
User Guide
1: Privacy Management
2: Purpose for Collecting Information
3: Collection

		Maturity Level				
		1	2	3	4	5
Using Data to Evaluate Objectives	Current	○	○	○	○	○
	Target	○	○	○	○	○
Managing Data	Current	○	○	○	○	○
	Target	○	○	○	○	○
Using Data for Research	Current	○	○	○	○	○
	Target	○	○	○	○	○
Obtaining Data for Research	Current	○	○	○	○	○
	Target	○	○	○	○	○

Add links to policies or procedures that are currently used in relation to in the above section. Identify any actions that should occur to increase maturity in this area.


BACK
Dashboard Summary
MENU
User Guide
1: Privacy Management
2: Purpose for Collecting Information
3: Collection
4: Use and Disclosure of Information
5: Notice / Consent
6: Information Management
7: Safeguards / Security of Information
8: Providing Access
9: Managing Compliance
10: Evaluation and Research
Dashboard Summary
Current Score: 0
Target Score: 0
PMA Report Card
Things You Do Well
1. More Improvement is Needed
2.
3.
Areas Needing Improvement:
1. Privacy Management
2. Privacy Management
3. Privacy Management
Completed by
(additional details as to next steps can be added below)
Organization:
Business unit:
Name:
Title:
Telephone:
Email:
Date completed:
Future review date:
Overall Summary
Current
Target
Privacy Management
Purpose for Collecting Information
Collection
Use and Disclosure of Information
Notice / Consent
Information Management
Safeguards / Security of Information
Providing Access
Managing Compliance
Evaluation and Research
Display:
Notice / Consent
Notice / Consent
Current
Target
Notice
Consent
Informed Consent
Consequences of Refusal

Background Information

What is the Privacy Maturity/Capacity Assessment Tool?

- The Privacy Maturity/Capacity Assessment Tool is a tool which will allow organizations to determine what specific portions of their privacy plan are working well, and help organizations identify and address particular aspects of their privacy plan which need improvement.

- Developed for use by organizations that manage personal information based on existing national and international standards, the tool is an adaptation of a Privacy Maturity Assessment tool developed by the Government of Saskatchewan, permission for use graciously provided by Aaron Orban, Executive Director, Chief Access and Privacy Officer, Integrated Justice Services, Saskatchewan.

- A section was included in this tool (*Section: 10 Evaluation and Research*) that addresses the heightened interest and need for the use of data in both of those domains. While information can and should be used for the purposes of evaluating progress, and while there are legitimate interests and purposes for using data for research, both areas require the application of a privacy lens as decisions are made on how to evaluate, and what data can be used for what research.

- The tool is an interactive spreadsheet that allows users to select the option which best represents their organization's current level of privacy maturity on a five point scale. The maturity levels can vary and be subjective, but generally can be described as:

  1) Informal. Incomplete. Usually inadequate
  2) Partial or occasional compliance. Policies may be incomplete.
  3) Clearly communicated and documented policies and procedures. Consistency in application.
  4) Fully implemented policies, procedures and practices. Well educated staff. Well managed.
  5) Regularly monitored and improved based on feedback and data. Proactive.

The end results are displayed as graphs which easily identify which areas are strong and which areas may need improvement. There is also space at the end of the tool to outline your organization's plan to improve on certain areas (adding notes for improvement into the comment boxes as you fill out the tool may be useful points of reference once you reach this stage), and set future goals based on your targeted state of compliance.

Nothing in this tool should be considered legal advice or a replacement for fully documented privacy policies and procedures or privacy impact assessments.

Why Should an assessment be done?

- To provide an overview of current privacy compliance,
- To help measure targets and goals, chart progress, and identify areas of improvement,
- To improve the privacy practices of an organization,
- To demonstrate the state of privacy compliance when collaborating/integrating with other organizations,
- Upon completion of the tool, the user is provided with a score that assesses the organization's current state, provides a target score, and graphs the movement towards overall growth and maturity.

All organizations that manage personal information have a duty to protect personal and health information (PHI) in keeping with both federal and provincial legislation, as well as to uphold the privacy rights of individuals with respect to the collection, use, retention, disclosure, and disposal of personal information. Organizations working with other organizations in collaborative or integrated service delivery approaches should all be held to common standards. The tool will help these organizations assess their current levels of privacy compliance.

Who Should complete the tool?

- Any organization who wants to measure their privacy practices and identify areas for improvement.
- An individual (or multiple individuals) with knowledge of the organization and privacy in general.
- The Privacy Officer or employee responsible for privacy protection within the organization, with assistance from subject matter experts as required.

When Should an assessment be done?

- At any point of time, as it is intended to evaluate the current and future state of privacy compliance within a organization.
- Scheduling a time to revisit the assessment in the future ensures that progress can measured and new goals can be outlined.

Companion Guide

The following Guide provides a sense of what the levels mean, and how to assess where and what your organization should be doing in each of the areas. Additional resources may also be useful, and a list of more notable ones can be found in the Information Sharing Framework - Appendix J: Additional Resources.

The Maturity Levels (1-5) generally follow similar criteria. Organizations do not necessarily need to be at the same level across all areas. Factors that may influence where they need to be include the:

- size of the organization,
- number of staff,
- type and sensitivity of the information they manage,
- reliance on technology to manage information,
- any requirements they may have through contracts or agreements.

As any of these factors increase, so does their impact, as does the degree of complexity, and as a result, the higher the level that might be required. As well, organizations working in a collaborative or integrated approach may rely on the Tool to determine if a potential member meets what they feel are minimum expectations. They may set the levels as they deem appropriate for the information required given the type of services they provide.

Level 1: There may be some rudimentary efforts of addressing or demonstrating the area, but they often exist informally, and are not necessarily well known by all staff who should. An organization that is working at this level should not be managing personally identifying information that has any level of sensitivity. It may be acceptable if the organization only deals with publicly available information, although the management of even that level of information would likely not be efficient.

Level 2: At this level, there may be the start in the development of policies and practices, but they have not been necessarily well thought through, and may be incomplete. Staff may not be aware of their existence nor have been trained on their use, or of their responsibilities under them. Organizations working at this level should not be managing sensitive personally identifying information, or if they do, should make a concerted effort to upgrade their policies. Note that depending on the area and its specific implications on the management of personally identifying information, this level may be sufficient for a smaller or less complex organization.

Level 3: At this level, an organization will typically have a basic understanding of the requirements for the area, and has put in place policies and practices that are likely sufficient for most of the personally identifying information they manage. The policies may not always be framed in the most understandable language as they may reflect a re-iteration of legalese and legislation, but they exist. Staff have been trained at a basic level, and there are resources they can go to if necessary. This is likely the minimum operating level for an organization that manages personally identifying information.

Level 4: At this level, the policies are mostly comprehensive and complete, and framed in language that is easily understood by staff such that they can readily explain them to the

individuals they provide services to. Management pays more attention to the level of detail required, and the organization is achieving a relatively higher level of maturity in the way it demonstrates its responsibility in the area.

Level 5: At this level, policies are complete, reviewed periodically to ensure they still meet the requirements, and practices are in alignment with the expectations and responsibilities laid out in the policies. The organization acts in a seamless manner, and compliance is monitored on a regular basis, with adjustments and interventions taken as required. Staff receive training on a regular basis, updated and refreshed as required.

Section	Description	Notes
1. Privacy Management: Organizations that manage personal information are responsible for how it is managed and should ensure they are structured in a manner that reflects that responsibility throughout the organization, including identifying how it is accountable for compliance with the applicable privacy legislation. If the organization is not subject to privacy legislation, a best practice is to demonstrate alignment between its policies and the private sector privacy legislation that applies to the jurisdiction the organization resides in. (E.g. *Personal Information Protection Act* – PIPA; *Personal Information Protection and Electronic Documents Act* - PIPEDA).		
1.1. Privacy Framework	A privacy framework is in place that addresses how the organization manages its accountability in compliance with its applicable legislation. If the organization is not subject to any legislative oversight, the privacy framework sets out its accountability to the individuals whose information it manages.	A privacy framework is a set of policies and procedures that comprehensively provide guidance and expectations on the organization's management of personal and health information. It should include policies and processes regarding the areas, roles, and responsibilities regarding decisions made on the management of; the collection, use, and disclosure of; and the security regarding; personally identifying information that the organization requires to provide the services and programs it has a responsibility for. The overall framework should set out and support the development of a privacy management culture that permeates all areas where personally identifying information is in use.
1.2. Complete Understand-able Policies	Privacy policies are complete and easy to understand. They cover notice, consent, collection, use, disclosure, retention,	Policies should exist for and include all areas, including but not necessarily limited to: • Clarity of purpose and objectives, including the organization's services, as well as the purpose and objectives for the collection and use of personally identifying information, • Governance or decision-making regarding all aspects on the collection, use, and disclosure of personally identifying information,

Section	Description	Notes
	disposal, access, security, quality/accuracy, monitoring and enforcement broadly, and any other specific privacy issues that are relevant to the program. They consider the specific types of personal and health information that might be collected, used, or disclosed.	• Providing appropriate 'Notice' where applicable, • The appropriate use of Consent, including when it is or isn't required, • Retention and disposition of personally identifying information in all its formats, • Managing appropriate and authorized access by staff, external users, and the individuals to whom it pertains, • Corrections and other areas related to quality control, • Security of the information, • Compliance and training of staff.
1.3. Privacy Governance	Management supports privacy management and requirements, and the need for demonstrated accountability in how obligations and issues are adequately addressed.	Privacy management must start with and be visibly endorsed by the organization's management, and cascade through all levels. This should include clear decision-making processes on the development of policies and practices, as well as the allocation of resources to specific roles and responsibilities, training, and other areas as required.
1.4. Privacy Officer / Duties	The organization has identified a Privacy Officer/Duties, responsible for ensuring privacy obligations under the legislation are met. The role/duties of the Privacy Officer are well defined and there is a strong leadership structure in the area of privacy.	By identifying a person responsible for the privacy portfolio, the organization demonstrates its commitment to the appropriate management of personally identifying information in a privacy conscious manner. The position should report at a high enough level in the organization that it has the visibility and support necessary to achieve its objectives. It should also work closely with the Security Officer Role/Duties.
1.5. Privacy Culture	Privacy is a part of the organization's culture and is	Privacy should not be seen as a one-off area of focus, but rather should be woven throughout the structure, policies and processes of the organization.

Section	Description	Notes
	detailed in written policies and procedures. Employees are trained in and demonstrate the importance of privacy.	In addition, the staff dealing with or responsible for services that involve the use of personally identifying information should be fully trained.
1.6. Privacy Training	New employees receive privacy training appropriate to their job duties shortly after they start their employment. Existing employees receive refresher privacy training. Privacy training is reviewed on a regular basis to ensure it is up-to-date and current. Employees are reminded of the importance of privacy throughout the year through emails, posters, staff meetings and training.	Privacy training should be both broad and specific. Employees should be conversant enough with applicable privacy legislation and the organization's commitment to the appropriate management of personally identifying information to the point they are able to pass that on to their clients in a manner they can understand. At the same time, any policies and processes that are relevant to their roles and responsibilities, especially in how they make decisions on the collection, use, and disclosure of information should be well understood. Up to date resources should be available to staff who have questions or require input.
1.7. Contractor Privacy Awareness	Communication regarding the obligation to protect personal information is provided to all contractors that handle personal and health information to ensure they are aware of their	Organizations that manage personally identifying information are accountable for how that information is used, even where the organization contracts out any services that involves the collection, use, or disclosure of personally identifying information. It cannot contract away any such responsibility, so should ensure the contracts or agreements contain requirements to ensure the contractor manages such information in an appropriate manner, as an extension of the organization itself. The organization should ensure the contractor has processes in place, including training their own staff, to support on their

Section	Description	Notes
	privacy obligations. Contracts are in place that outline their privacy and information management obligations.	responsibilities vis-à-vis the management of the information, given the ongoing accountability of the organization.
1.8. Privacy Breaches	The organization has a process in place to respond to privacy breaches. The process would include identifying, managing, and resolving privacy breaches. The process would include preventing similar privacy breaches, who should be notified of the privacy breach, and when. The organization should assign duties for managing privacy breaches to a particular individual.	Organizations that collect and use personally identifying information have a responsibility to not only ensure that appropriate security mechanisms are in place to protect and prevent any unauthorized access, use of the personal information they manage; they must also have processes in place to deal with privacy breaches. Such processes must include the investigation of any breaches whether actual or potential; the appropriate reporting of the breach, including to the individual(s) whose information may have been breached, along with the Office of the Information and Privacy Commissioner/Ombudsman if required; and steps taken to prevent the breach from occurring again. There may also be some responsibility to assist individuals who are impacted by the breach. The organization should identify an individual or area that has responsibility for oversight in managing privacy breaches, in conjunction with the security team if appropriate, and staff should be trained on the prevention and reporting of breaches.
Additional Resources: See Appendix J: Additional Resources for • Privacy Management: • Privacy Breach Response, Reporting and Notification:		
2. Purpose: Intended / Consistent Personal information is only to be collected for a purpose that relates to an existing or proposed program or activity of the organization. When considering what information is to be collected or required, organizations should identify the purposes for which it is collected along with the roles and impacts of such collection.		
2.1. Identify Purpose of Collection	The organization identifies what information it requires for what purpose(s), including	Understanding the purpose for which information is collected is a critical step in establishing the authority to collect and use it. Organizations should determine what is the minimum information they will require in the delivery of its programs and services. To assist in that determination, the organization

Section	Description	Notes
	consistent purposes, how the information will be used, and if and to whom it might be disclosed. The organization has documentation regarding the purpose(s) for collecting personal information.	should be clear about its purpose for each program/service area, what its intended objectives or outcomes are, and what information they would then require to fulfill those objectives. When considering the purpose and objectives there are additional considerations to assess: • How will the program/service be evaluated? It should be recognized that to be successful, programs and services need to be evaluated, and the information required to conduct those evaluations would be deemed a use consistent to the original purpose. However, the use of identifying information should be limited and not part of the broader program level evaluation. • What is the environment in which the services will be delivered? For example, if the intent is to deliver services in a healthy, safe environment, especially given that the individuals being served may be dealing with unsafe situations, it would be worth determining if that should be stated as part of the purpose or mandate of the organization. By doing so, the organization is establishing that where necessary, it will address risks that emerge to individuals working or being supported in that healthy safe environment. This then supports the authority to use information for that purpose, notwithstanding consent being provided. If this is an intended approach, the organization should be transparent, and it would be appropriate to include that in the notice provided to individuals at the outset. Transparency in how information is needed and used to achieve a purpose is important. As such, staff must not only understand the purpose and objectives, but they must also be able to explain it in a manner that the individuals they support can understand. As well, the organization should be transparent about what information is collected, and for what purpose. That may mean providing an explanation on its website, or in pamphlets, or in whichever approach is best able to reach its clients, in addition to providing notice.
2.2. Roles and Responsibili-ties	The organization has determined what areas or roles are responsible for	The roles and responsibilities of staff also have a part in determining what information needs to be accessed or used, and by whom. For example, a staff who is doing initial booking and assessment will not likely require access to the more in-depth case file

Section	Description	Notes
	what aspects of services, whether client facing or internal, and what information those roles require to conduct their functions.	information of someone who is receiving counselling services. Similarly, individuals who manage data analysis likely do not require access to identifying information, nor should staff supporting IT infrastructure development (use dummy data if required for testing), and so forth. When using electronic systems to manage data, the preferable approach is to limit access by role, such as RBAC - role based access controls, or more advanced control processes.
2.3. Relevancy of Information	Procedures are in place to ensure personal information is sufficiently relevant to the purposes for which it will be used. There is minimal possibility that inappropriate information is used to make business decisions about the individual.	Once the purpose and roles have been defined and understood, and the determination of what information is necessary to be collected and used, care must also be taken to ensure that only the information that is relevant to decision-making in support of the objectives and outcomes is used. For example, a service that is provided to the public generally should not be influenced by demographic factors such as age, culture, language, unless such factors are a focus of the service. Services to seniors would not include individuals under the age of 55, or 65, or whatever the age of eligibility is set at; while eligibility for services to someone who is dealing with addiction should not generally be limited by the fact they are homeless or from a specific cultural background. Those factors may be important in other ways, but not in determining initial eligibility.
2.4. Privacy Impact Assessments	The organization has a process to consider the privacy impacts of any new use of personal information which includes notification and consent. This should also include other change initiatives such as personal information being used for a	When a program or service is being developed, the organization should conduct a Privacy Impact Assessment (PIA), a due diligence exercise by which the intended collection, use, and disclosure of information is carefully assessed from a privacy management perspective. Similarly, as services and programs evolve, there is the potential for additional information to be required. This may also be true if it is determined that the initial collection of information is insufficient to achieve the stated objectives and outcomes. That additional collection, or a potential new use of information, should also be carefully assessed from a privacy management perspective, (and may be added to an existing PIA as an amendment):

Section	Description	Notes
	different purpose than when it was originally collected, and for reorganizations where information is being used, disclosed, or stored differently.	• Is there authority to collect and use that information? • Is there a need to advise the individual of the (initial or new) use or collection, or to obtain their consent in advance of such use or collection? • How will that additional information be collected? • Who will have access to it, and to whom might it be disclosed, and with what authority? • How will it be safeguarded? • How long will it be retained, and will it be disposed of in a secure manner? While conducting a PIA may only be required under some privacy legislation, it is a useful tool to ensure the appropriate management of personally identifying information by any organization, and should be part of the organization's toolbox in assessing and managing privacy risks. Additional information on conducting a PIA is available through government and Privacy Commissioner/ Ombudsman sites.
Additional Resources: See Appendix J: Additional Resources for Privacy Impact Assessments		
3. Collection The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization, and in accordance with the applicable legislation. Information should be collected directly from the individual to whom it pertains, unless otherwise authorized.		
3.1. Limiting Collection	The organization limits the amount and type of personal information collected to what is necessary for the identified purpose.	Privacy legislation generally limits the collection of personally identifying information to the minimum required by the organization (e.g., to determine eligibility or provide a service). It is therefore important that organizations be clear as to what those minimum requirements are.
3.2. Manner of Collection: Direct Collection	Personal information is collected directly from the individual to whom it pertains unless there are specific and approved reasons for not doing so. The	When determining what information is required to provide a service, consideration should also be given to the manner of collection. The personal information of an individual should be collected directly from the individual to whom it pertains. This requirement is in keeping with an underlying tenet of privacy legislation – recognition that the individual should be in control of their own information, including decisions on who can access it. Direct collection is

Section	Description	Notes
	manner of collecting personal information is reviewed to confirm that personal information is obtained fairly and lawfully.	the expectation in legislation unless an exception is identified and met.
3.3. Manner of Collection: Indirect Collection	Indirect collection occurs when personal information is collected from someone other than the individual to whom it relates. Any indirect collection is documented.	Exceptions to the (above noted) direct collection do exist, including with the informed consent of the individual, or when dealing with health and safety situations. Those circumstances should be determined in advance wherever possible, and staff should be trained and aware of when they can collect information indirectly, and how to go about doing so.
3.4. Accuracy of Personal Information	The organization takes reasonable measures to ensure that personal information is accurate, complete, relevant, and up to date prior to using the information to make decisions.	The use of personal information can have significant implications for purposes including assessing or providing programs or services. It is important therefore, to ensure that the information being collected and used is up to date, accurate, and as complete as necessary for the identified purpose(s). It is also important to ensure that electronic systems properly maintain the integrity of the information, and that processes are in place to allow for the correction of information if not accurate, or if incomplete.
4. Use and Disclosure of Information The use of personal information shall be limited to the purposes identified by the organization, and in accordance with the applicable legislation. The disclosure of information must be with the consent of the individual to whom it pertains, or in accordance with applicable legislation. Where the organization is not subject to any privacy legislation, a best practice is to follow the private sector privacy legislation that applies to the jurisdiction the organization resides in. (E.g. *Personal Information Protection Act* – PIPA; *Personal Information Protection and Electronic Documents Act* - PIPEDA).		
4.1. Use	The organization has policies and/or procedures in place to ensure that information is	As noted above in Section 2: Purpose, the organization must identify what information is required for the programs and services it provides. The information it collects must only be used for those programs/services, or for a use consistent with

Section	Description	Notes
	used for the specified purpose(s). Procedures are in place to ensure personal information is sufficiently relevant to the purposes for which it will be used. There is minimal possibility that inappropriate information is used to make business decisions about the individual. Where it is determined that additional uses are required, processes are in place to determine the authority, and to inform individuals to whom the information pertains of that new use, if required.	that purpose. Examples of what might be considered a consistent use includes: • Information that is collected to assess/identify the services required by an individual is subsequently used to provide those services, • when information that has been collected is used to determine if the provided service is benefiting the individual, or • where the information that reflects achievement of the anticipated outcomes is used to assess the overall program or service – I.e., is the service providing what it is intended to.
4.2. Use – Other Uses	A use different from the initial (or consistent) purpose for which the information was initially collected. Where it is determined that additional uses are required, processes are in place to determine the authority (including obtaining consent	When an organization determines that it may be beneficial to use the information it manages for a purpose different than what it was originally collected for, it is obligated to undertake the process(es) necessary to obtain the requisite authority to use it for that purpose. That may include advising individuals of the new use and providing them the opportunity to respond, obtaining their consent for the new use, and completion of a privacy impact assessment. For example, it may be determined that in order to more holistically meet the needs of certain individuals, the organization will enter into a collaborative or integrated relationship with other organizations. However, the use of the previously

Section	Description	Notes
	if not otherwise authorized), and to inform individuals to whom the information pertains of that new use, if required.	collected information within the context of an integrated service approach could be considered a new use, and the organization should obtain the consent of the individual before including them in the integrated service. Note that there may be authority to disclose the information that should also be considered.
4.3. Disclosure with Consent	The organization has policies and procedures in place to ensure that information is disclosed for authorized purposes. Information is disclosed with the informed consent of the individual to whom it pertains, unless otherwise authorized. All disclosures are documented.	An organization has limitations on the disclosure of the personal information that it manages. The informed consent of the individual to whom it pertains is generally required before it can be disclosed, unless other authority exists. Consent is further described in section 5: Notice and Consent, below. Legislation also requires that any disclosures are limited to the minimum amount required for the purpose, and that it be disclosed in as anonymous a way as possible. Organizations should determine what that means for the specific circumstances. For example, in situations where a staff attends an interagency conference and is trying to determine what services might be appropriate for a certain condition or need, it may not be necessary to identify the individual who is in need of that service. However, if the staff is coordinating with staff from another organization to provide holistic services, and there may be dependency by one service on the outcomes of another service, it may well be appropriate to discuss the individual in an identifying manner, and consent of the individual for that disclosure (and discussion) may be required.
4.4. Disclosure without Consent	Where the consent of the individual is not required for the disclosure of their information, processes exist to ensure that any such disclosure is duly authorized, and any follow-up actions are taken, if necessary. All disclosures are documented.	There is recognition in privacy legislation that there will be circumstances in which there is a need for the disclosure of an individual's personal information without their consent. The organization has an obligation to ensure that any disclosures without consent are duly authorized by legislation. As such, it is important to understand what circumstances might arise, given the demographics of the clients served, the types of services provided, and the potential for disclosures without consent that might emerge. It would behoove an organization to carefully consider the use of consent when not required, as there may be unintended consequences in doing so. Examples could include disclosures when an individual lacks the capacity to provide consent, yet the disclosure is

Section	Description	Notes
		in their best interests; situations where there may be a risk to health and safety; and circumstances where legislation authorizes the collection of information without the individual's consent, or where otherwise required by law. Such situations may require clarity that "notwithstanding consent" information may be disclosed in those circumstances. As noted previously, it is a best practice for organizations to be transparent about how they manage personal information, including the potential noted disclosures ("where authorized or required by law" is a commonly used phrase, but further clarity may be appropriate).
5. Notice / Consent Organizations must be transparent in the collection, use, and disclosure of personal information. This includes the provision of notice where required and obtaining informed consent of the individual to whom the information pertains, unless otherwise authorized. Informed consent means the individual understands what they are consenting to and has been advised of the consequences of their decision regarding consent.		
5.1. Notice	The organization provides proper notice including: the purpose for the collection of personal information, how it will be used, to whom it will be disclosed, and the name and contact information of someone who can answer questions regarding the collection. Notice is provided at or before the time of direct collection (from the individual to whom it pertains). The organization should have documentation regarding the purpose(s) for collecting	When an organization collects information directly from the individual to whom it pertains, there is an obligation to provide 'Notice' to the individual. Legislation varies somewhat on the elements required, but the following elements will meet all requirements: • What information is being collected, • For what purpose, (how it will be used), • The specific legal authority for the collection, • To whom it might be disclosed, • The title, business address and business phone number of someone (affiliate, officer, person) who can answer any questions the individual may have about the collection. Organizations should be familiar with the nature of the circumstances that drive individuals to require their services. Individuals who are in crisis may not always focus on or retain what they are being told, or they may respond to requests by providing what they feel they need to say to obtain the services. It may therefore be important to provide additional information, whether in hard copy such as a brochure or print-out of some sort, or by checking with them if they have any questions regarding the information provided in the notice in a future interaction once the crisis has been addressed.

Section	Description	Notes
	personal information.	
5.2. Consent	The organization obtains consent for the collection of information from an individual at the time of, or before, any collection, or use, of personal information – unless otherwise authorized. Individuals are advised of the consequences of providing or not providing consent. Consent for disclosure may occur simultaneously, or at a later point, dependent on the circumstances.	While some privacy legislation does not require the consent of the individual prior to the collection of their information, (although Notice would generally apply) there are circumstances where consent is required, such as when the individual consents to the collection of their information from someone else. Organizations not subject to privacy legislation, and who do not work on behalf of an organization that is, should generally obtain the consent of the individual prior to the collection of their personal information. See above (4.2 and 4.3) for discussion on the disclosure of information with and without consent.
5.3. Informed Consent	Informed consent means the individual understands what they are consenting to. They are informed about the requirement for consent and the choices available to them with respect to the collection, use and disclosure of their personal information, and are made aware of the risks and benefits of consenting or not. This includes why	Consent should not be seen as checking off a box, or someone waiving their rights to confidentiality. Privacy legislation is predicated on the notion that an individual should have control over their information, including to whom it might be disclosed. As such, it is important that organizations seeking consent ensure it is informed. That means they take the time to ensure the individual understands what they are being asked to provide permission for, to whom their information might be provided, and the implications of providing or not providing consent. Note that there may be additional expectations regarding 'informed consent' placed on health care professionals by their colleges identified through their Standards of Practice or similar instruments under the applicable health professions legislation. Organizations should be familiar with the nature of the circumstances that drive individuals to require their services. As with when providing Notice, individuals who are in crisis may not always focus on or retain what they are being told, or they may

Section	Description	Notes
	their personal information is being collected, how it will be used, and to whom it will be disclosed.	respond to requests by providing what they feel they need to say to obtain the services, including consent. It may therefore be important to offer or provide additional information, whether a copy of the consent, or by checking with them if they have any questions regarding the consent in a future interaction once the crisis has been addressed.
5.4. Consequences of Refusal	Individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use or disclose personal information.	Individuals should not generally be denied a service on the basis of not providing consent. However, there may be impacts on what and how the service can be provided. For example, an individual who does not consent to the disclosure of their information by the agency they are working with to other agencies that might be of benefit, can still be referred to them, but the individual may then have to repeat their story, outlining their circumstances and so forth. Similarly, if an individual chooses to withdraw their consent, they should be advised of the consequences of doing so. That may include advising them of the need to repeat their circumstances to any new organizations being referred to; as well as letting them know that while any further disclosure will not occur, decisions and actions taken up to that point on the basis of the previously provided consent cannot be undone. As noted previously, there may still be circumstances where disclosure can occur without the consent of the individual, and they should be made aware of that wherever possible and appropriate.
6. Information Management Personal information that is used to make decisions, along with any such decisions and actions taken, must be appropriately documented, maintained, and disposed of in a secure manner, in accordance with any applicable legislation and legal requirements. Organizations should ensure they maintain records of any holdings of personal information such that they can be readily accessed where required, such as in response to requests by authorized persons.		
6.1. Documenta-tion	The organization has documentation practices that includes recording information that is collected and used to make decisions that	Individuals have a right of access to their information, that which is used to make decisions that impact them, as well as who may have accessed it. It is important then, that such information is available for access, which in turn means that organizations must record such information, and do so in a manner that it can be accessed by authorized users. Information can be recorded in hard copy (e.g., paper records) or soft copy (e.g., electronically); must be stored in a

Section	Description	Notes
	impact the individual(s) to whom it pertains. The collection, use, and disclosure of information is duly recorded in the appropriate manner.	secure manner such that it is properly protected from unauthorized access; and must be disposed of when no longer required in keeping with retention and disposition requirements.
6.2. Retaining Personal Information	The organization only retains personal information as long as necessary to allow for the fulfillment of identified purposes, or where and as required by law. Retention schedules have been developed and implemented, ensuring that electronic and paper records are retained and disposed of appropriately.	There may be a number of implications related to the requirement to retain information. Information must be kept in accordance with any legislative, contractual, and reasonable use requirements. Some privacy legislation requires identifying information about an individual used to make a decision that impacts on that individual, to be kept for a minimum of one year, and retention periods often run a minimum of 10 years or longer, depending on other legislative requirements and policies. If the organization is not bound by any legislative, contractual or other retention requirements, it should make a determination as to what is reasonable, be transparent, and abide by that. Note that there may be a need to retain aggregate or non-identifying information for periods longer than what would be reasonable for identifying information, such as to monitor trends at a population level. Organizations working on behalf of another should ensure that they understand what is required of them regarding the retention and disposition of records once the contract or agreement they operate under ends. Being aware of the impacts of contractual provisions is critical, especially where information used to fulfill a contract may also be used for other programs or in the delivery of collaborative services.
6.3. Disposal of Personal Information	The organization has complete policies and practices regarding the disposal of records containing personal information in a secure manner -	Information that is no longer required to be retained under a retention period must be disposed of in a secure manner. That includes information that is stored in hard copy or electronically. As such, any electronic systems that store personally identifying information, including back-ups, must have the ability to purge or dispose of records. Equipment used to manage information must also be handled in a way that ensures the appropriate disposal of information. For example, the disposal of hard drives on

Section	Description	Notes
	once they are no longer required, and once the identified retention period has passed. Logs that are kept identifying when records were disposed of must not include personally identifying information.	computers or printers, USB drives and other storage media must occur in a secure manner such that the information stored or backed up on them cannot be accessed.
6.4. Personal Information Banks/ Holdings	The organization has identified and classified the types of personal information, and their uses, that are collected and retained by the organization. A clear understanding of how the personal information is stored, used, and disclosed exists, and all data flows have been documented.	Organizations must be transparent about what information they control or have custody of, and how they manage it. One of the ways they can demonstrate transparency is to identify what type of information they typically manage, and for what purpose. (These information holdings are often referred to as Personal Information Banks (PIB) under privacy legislation.) While some of that can be publicly identified, a more detailed inventory should be maintained internally, including clear understanding and documentation regarding what information is used for what purpose, by whom, and where it is disclosed or shared, and to whom. Creating such inventories and information flows will be critical to its management and the implementation of the appropriate safeguards and practices.
7. Safeguards/ Security Personal information shall be protected by security safeguards that include physical, administrative, and technical safeguards. The safeguards in place should coincide with the level of sensitivity of the specific personal information.		
7.1. Information Security Program	The organization has adopted and documented an information security program to protect personal information against loss or theft, unauthorized access, disclosure,	Organizations that use or access personal and health information have a responsibility to ensure that it is managed in a secure manner, and that steps are taken to prevent unauthorized access or use. Implementing a security program that considers and addresses any areas of risk is critical. Staff should be trained and aware of what is required of them should any issues or risks emerge, and with or to whom they should connect or bring the issue to be addressed.

Section	Description	Notes
	copying, use or, modification, which includes physical, technical, and administrative safeguards. Include a link to any policies that are used to safeguard personal information in the comment box below.	
7.2. Types of Safeguards	The organization's information security program includes reasonable physical, administrative, and technical safeguards. Physical safeguards monitor and control the work environment. Examples include having records stored in a locked filing cabinet and having controlled access systems. Administrative safeguards provide the organizational framework for safeguarding personal information and should be formalized in written policies	The security program should address all areas. For example, while technical safeguards such as role-based access controls can be built into an electronic system that limit access to certain types of information, it may not be feasible to restrict access at a data element level, as it may not always be clear who will require access to what specific information. However, by ensuring that there are logs maintained of who accesses (both read and write) what information, in conjunction with both pre- and post-complaint audits (of the logs) can minimize the risk of unauthorized access. This combination of technical (logs) and administrative (audits) tools, along with the training of staff on their use would be an important element of a security program where information is stored electronically. Examples of physical safeguards include ensuring file cabinets, server and records rooms are locked, with access only available to authorized persons; and ensuring that computer screens are positioned such that they are not viewable by unauthorized persons.

Section	Description	Notes
	and procedures. Examples of this would include having an appropriate training program available for staff, and audit/review processes for system access. Technical safeguards monitor and control access to information and computer systems. They should include strong password protection, access (read/write) logs, secure off-site data back-up protocols, and data encryption, as required based in part on the sensitivity and value of the data. The application of software updates is also critical to minimizing identified risks.	
7.3. Access Controls	The organization has controls and procedures in place which restrict access to information based on roles and responsibilities. Access to information is granted on a need-to-know basis, supported	Organizations should ensure they not only understand and outline what information is required by whom for what purpose, but that their security framework supports address and manage access based on those aspects. Staff who do not provide any services to individuals should not have access to personally identifying information, and staff who do should be limited to only accessing and using the information they require to support the individuals they have responsibility for. Credential management is a critical part of controlling that access, and staff must not only be duly authorized, they must also be trained on the need to

Section	Description	Notes
	with credential management.	properly secure their credentials to prevent use by other parties. Sharing credentials or passwords cannot be condoned, and staff must understand their accountability for their use.
7.4. Safeguarding Portable Devices	The organization has procedures in place to protect personal information when it is transmitted, transported, or temporarily stored by any means and in various technologies.	Organizations are increasingly reliant on staff who work remotely, whether in the field delivering services, or working from home. This has led to a significant increase in the use of mobile devices, including laptops, tablets, smart phones, and various storage devices such as USBs. This places additional pressures and requirements for the proper deployment and management of those devices. Organizations should consider if and how they will support the use of any devices, if they will allow staff to use their own devices, and how they will ensure their use in a secure manner. Policies and practices should be in place that apply not only to the devices themselves, but to the use of software, including social media, as well.
7.5. Safeguards Effectiveness Test	The organization regularly tests the effectiveness of all safeguards.	Having a security program in place is only a starting point. Ensuring that it is regularly reviewed and updated as necessary is a critical component, and that applies to all policies and processes contained within it. The ability to manage that means there should be staff dedicated to administering the program, with access to the necessary resources, including senior management responsible for their allocation. Training of all staff should include training to their roles, with periodic updates, whether scheduled or ad hoc in response to required changes.
Additional Resources: See Appendix J: Additional Resources for Securing personal information		
8. Providing Access An organization shall be open and transparent with individuals about the existence, use, and disclosure of the individual's personal information, and provide access as appropriate when requested. Access requests must be processed in accordance with applicable legislation, or where the organization is not subject to legislation, it must have and follow a policy in keeping with the principles of openness. An individual can challenge the accuracy and completeness of the information and ask that it be amended as appropriate.		
8.1. Access to Personal Information	The organization informs individuals about how they	At some point early in the process of staff connecting with individuals approaching the organization for services, they should also advise

Section	Description	Notes
	may obtain access to their personal information, to review, update, and correct that information, as required.	them about their right of access to the information the organization holds, and how they can obtain access or request corrections. This can be built into the discussions around notice and consent.
8.2. Procedures for Requests	The organization has policies and procedures for responding to requests for personal information, both informally and formally under applicable legislation. Employees know the appropriate Privacy Officer or staff who deals with these requests.	An underlying tenet of privacy legislation is the right an individual has to their own information. Wherever possible, such access can be managed in a proactive or informal manner, such as by providing them with copies of forms they complete. There should also be clarity provided about the process for responding to formal requests that are made under legislation. There may be some exceptions regarding what information may be provided, and organizations should be familiar with those and when they may be applied. For example, information about others may be included within a record about the individual seeking their own information. The individual may not have a right of access to that other information, and there should be a process for dealing with such situations.
8.3. Establishing Identity	The organization has procedures in place to verify the identity of individuals, whether accessing services or requesting access to their personal information. Include a link to any policies you use to establish the identity of an individual in the comment box below.	Establishing identity is a critical component in addressing privacy management. Organizations should have processes in place to confirm they are dealing with who the person presents to be, if that is a requirement. This may apply • When approached by an individual seeking services, whether in person or by phone or online, • When contacting someone to obtain additional information or verification, whether an individual or an organization, • When communicating with someone by electronic means, such as by phone or email, • When providing information or access to information to someone, whether in person or electronically, • Similar to the above, when dealing with someone who is alleging to be acting on behalf of another. The use of identification is an important component in these processes, but consideration must also be given to how that is managed. Is there a need to only view ID, or note the identifiers, or to keep a copy of it, and how will that be managed securely?

Section	Description	Notes
		As noted, there may not always be a need to establish identity, as some services may be delivered anonymously.
8.4. Challenging Accuracy / Corrections	The organization has a process through which individuals can challenge the accuracy of the personal information that has been collected about them.	It is important that information managed by an organization is accurate. As noted, individuals have a right to access their information, and request it to be corrected if it is not accurate. This applies to factual information, such as birthdate, age and so forth. Information that is provided as an opinion, such as that provided by a health professional on the basis of tests and assessments, may not be factual, but the individual may have the right to request an addendum be linked to that opinion. Organizations should ensure they have a process by which an individual can access and make a request for a correction. The process may be relatively straight-forward, or may require the submission of documentation to support the request being made.
9. Managing Compliance Individuals can challenge the compliance of an organization with applicable privacy legislation or its own privacy policies. The organization will advise individuals where to send their concerns; complaints will be investigated; and changes will be made to practice or policy when warranted.		
9.1. Complaints Procedures	The organization has policies and procedures in place to advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to the appropriate Information and Privacy Commissioner/ Ombudsman, if applicable.	Privacy legislation includes provisions that deal with oversight by a third party, that being an Information and Privacy Commissioner or Ombudsman, whether provincial or federal. This is in recognition that organizations have a significant responsibility and accountability in how they manage the information of others. Individuals whose information is being managed must have someone they can turn to if they have concerns about how that information is managed, and the organization has a responsibility to be open to dealing with concerns or complaints. When complaints can be dealt with informally in an open and transparent manner, it is quite possible that the relationship between the parties will continue to be one of trust. Where a complaint cannot be dealt with by the organization, the process for bringing the complaint to an oversight body should be outlined and provided, if the organization is subject to such oversight.

Section	Description	Notes
		Other areas that may provide some degree of oversight includes the ability to bring complaints to a professional body, such as exist under health professions legislation.
9.2. Investigating Complaints	The organization investigates complaints from individuals who challenge compliance with privacy policies. Policies and procedures are in place to guide the investigations.	Complaints must be dealt with openly and effectively. There may situations where the individual misunderstood or was not provided information about a process, and doing so clears up any issues. There may as well be situations where policy was not followed, or where it does not sufficiently deal with a situation, or where the complaint may not have merit. In any case, there needs to be a process by which complaints are investigated and reviewed, likely by someone who is not the focus of the complaint. The organization should consider how it would deal with complaints, identify an area of responsibility, and ensure there is adequate training for staff.
9.3. Modifying Actions	The organization modifies its actions and processes if a complaint is substantiated and takes steps to minimize the likelihood that the issue will occur again in the future.	Where complaints have been found to be legitimate, and the result of some inaction or lack of appropriate policies or practices, the organization must have a means of responding and addressing any required changes. That may include enhanced or focused training, monitoring adherence to policy, or changes and updates to policies and practices.
10. Evaluation and Research The appropriate use of personal information must be in accordance with applicable legislation. Where information is required for evaluation and research purposes, organizations must use it in as anonymous a manner as possible, and ensure that any such research or evaluation is undertaken in such a way that is ethical, and that the confidentiality and privacy of individuals are maintained.		
10.1. Using Data to Evaluate Objectives	The organization has processes in placed to evaluate achievement of outcomes for individuals being provided services (micro level evaluation), as well as of the service or system	Services cannot be seen as being provided successfully without some way of measuring their effectiveness. The use of personal information for such evaluation is deemed to be consistent with the purpose for which the information was collected. When the services are provided directly to an individual, it is often important to determine if the goals or objectives outlined in the case plan were achieved, and if not, are there other factors or issues that were missed, or other interventions or supports

Section	Description	Notes
	in use (macro level evaluation). Processes include determining what data is required for either type of evaluation.	required. It is therefore important to identify and understand how the goals will be measured, and what information will be required to conduct that measurement. Such information is likely to be at an identifying level, as the goals are specific to the individual. The overall service or program also needs to be evaluated to determine if it is doing what was intended. For example, are there gaps that were not considered, are there enhancements that might lead to greater effectiveness, are there efficiencies that can be obtained? While the ability to measure the effectiveness in how the service or program is delivered or operates is consistent with the actual delivery, measuring it may not require the same information as is required for the achievement of an individual's goals. It is likely that analysis is completed at a population trend level, in contemplation of multiple outcomes and factors. It is important therefore to clearly outline what needs to be measured, what indicators are required to conduct the measurement, and what information is required in that process.
10.2. Managing Data	The organization has policies and processes in place to manage the data required for conducting analyses (evaluation) at both the micro and macro levels.	Organizations should consider how they can sort the information required for either form of evaluation, and how it will be managed, including who may have access to it. At the individual level, it is likely that the staff involved in the delivery of supports to the individual need to understand if the supports are effective, as may their supervisors and managers, in order to make adjustments in the supports as required. However, that identifying information would not be generally accessible to staff not involved in the direct service delivery, including senior management who may only need to know generally how things are progressing. At the broader program level evaluation, there may be a need for some of the dame data to be used across all individuals, but not at an identifying level. Given that, there should be some means of separating the identifying information where possible, and at a minimum, only reporting at a population trend level. Note that while the information may be provided at in an aggregate or de-identified manner, the potential for re-

Section	Description	Notes
		identification may exist, and it needs to be protected accordingly.
10.3. Using Data for Research	The organization has policies in place to respond to requests to conduct research, whether internal or from external sources.	Data has a significant role to play in the identification of new processes such as in response to societal issues. The use of data through research for purposes such as these, while acceptable, needs to be managed in a manner that addresses the necessary protection of privacy for any information used. Organizations should determine if they will entertain any requests for the use of the data they manage for research purposes; and if so, outline the process by which they manage such requests. This applies to research that is driven internally as well as from external entities. The process should include what expectations will be placed on any research(er) that must be met prior to the release of any data, and how it must be managed going forward.
10.4. Obtaining Data for Research	The organization has policies and processes to support the use of relevant data in an appropriate manner for research, whether driven by internal or external interests.	There organization should determine how data may be disclosed in a privacy managed approach, which could include restrictions on the disclosure of any identifying information. Where the research may require access to identifying information/data, requirements under privacy legislation may include that: researchers be required to go through a research ethics board approval; obtain consent for access to identifying information; de-identify information at the earliest point if they do require and access such information; and submit a PIA if there is any information being combined or matched. Data-matching may need to be performed by the custodian that holds the health information. Other processes to protect the privacy of research subjects might focus on means to minimize the potential for re-identification of individuals.
Additional Resources: See Appendix J: Additional Resources		

Appendix H: Guide to Using the Information Sharing Framework

The Information Sharing Framework is meant to provide guidance on what should be put in place to support enhanced collaborative or integrated service delivery. Depending on the type of collaboration, some or all of the Framework may apply. While the Framework addresses the need to, and manner in which it is possible to, share information, it is more about facilitating the delivery of collaborative and integrated services to better support individuals and families achieve their desired outcomes and goals. Organizations need to not only provide the specific services under their mandates, but where appropriate they should recognize how that potentially plays a role in meeting the individual's long-term needs and goals, and in addressing underlying issues.

This Guide will assist organizations who have an interest in working together in determining what elements of the Framework would be the most pertinent. Decisions regarding the application of the Framework should be made jointly by the member organizations.

The Framework can be adopted in its entirety, but it is critical that partnering organizations go through it, ensuring the circumstances under which they work are reflected in it, such as by identifying the governance model that will apply, the specific legislation provisions that apply, and the adaptation of their own processes where necessary.

The tables that are included in the Framework and Appendices should be reviewed to determine which specific areas apply to the services and organizations being considered for inclusion by the member organizations. For example, not all legislative provisions listed will necessarily apply in all situations (such as outlined in the Matrix), nor will all service types or types of information (such as outlined in the Disclosure Tool). As such they should be reviewed for applicability and accuracy and adjusted as required.

The following identifies the areas that should likely be considered and if applicable, adopted by the organizations that intend to collaborate. However, there may be value in adopting other areas beyond the ones identified, so it is recommended that the entire framework be reviewed and considered.

The Framework – Initial Steps:

1. Determine the potential partner organizations.
2. Determine what privacy legislation applies, if any.
3. Determine the purpose for the collaborative approach, and what is hoped to be achieved.
4. Determine the type of collaborative process (E.g., Referrals, Coordination, Collaboration, Integration) that will best support achieving those goals.

Referrals - Applicable Elements:

Member organizations may decide that they simply want to know *who provides what services* so they can make appropriate referrals. If so, no personally identifying information is being shared, and the use of the Framework is not needed.

Alternatively, the members may want to ensure the *referrals are appropriate*, and some feedback may be desired. This can be done without naming the individuals but may not be comprehensive or accurate.

Going one step further, the members may want to engage in '*warm hand-offs*', where the referring member provides some information to the receiving member, thereby opening the door, and eliminating the need for the individual to repeat their story. In this case, some information is exchanged, and the following sections may be applicable.

- 3. Roles and Responsibilities (p.17)
- 5. Applicable Legislation (p.25; see also Appendix A: Applicable Legislation, Appendix B: Legislative Matrix)
- 8.5 Consent (p.45; see also Appendix F: Consent Forms)

Coordination - Applicable Elements:

Member organizations may determine that there is a need for some level of coordination between them when supporting an individual or family. The level of coordination may require some sharing of information, possibly limited to identifying and contact information, but at times may require some collecting and sharing of initial assessment of needs. The following sections may be applicable:

- 2. Membership (p.15) – may be limited to simply registering who is involved
- 3. Roles & Responsibilities (p.17)
- 5. Accountability (p.17)
- 5. Applicable Legislation (p.26, see also Appendix A: Applicable Legislation, Appendix B: Legislative Matrix, and, Appendix C: Disclosure Tool)
- 7. Elements of Policies, Practices, Procedures (p.31)
- 8.5 Consent (p.45; see also Appendix F: Consent Forms)

Collaboration / Integration - Applicable Elements:

Member organizations may determine that in order to meet the needs of the individuals being supported, they need to do more than provide a level of coordination and move into a more enhanced collaborative or integrated service delivery process. In either situation, most of or all the Framework would likely be applicable. The level of detail and some of the approaches (E.g., Notice) may differ.

To support the use of the full Framework, the *Framework Template* can be used. The Framework itself provides the areas/ to be considered as the template is completed. The following steps will assist the use of the template:

- Using the Framework as a guide, respond to the questions and complete the applicable areas.
- Some areas are highlighted in the Framework that require the insertion of the names of the collaborative membership group, applicable committees, leads, etc. These should be determined by the members as the structure is developed.
- Review and identify the following specific areas that apply:
    - Legislation – which legislation applies based on the member organizations.
    - Services – what services are to be provided, by whom.
    - Information – what personal and health information will be required for the provision of the identified services.
    - Roles – what are the roles of the various staff, members, committees, etc.

- Legislation – which provisions will apply in what circumstances, based on the services being provided, and the roles of the members. Note that the specific legislative provisions should be reviewed to ensure their applicability.

Appendix B: Privacy Legislation Disclosure Matrix

The Matrix outlines the provisions under the various privacy legislations that might apply in various circumstances where services are being provided by organizations supporting individuals and families with mental health concerns. **Not all provisions will apply.** As such, the provisions should be reviewed, and the determination of which ones might apply be made. This can occur in consultation with privacy and legal staff. The tables can then be adjusted accordingly, to serve as a reference for staff involved in the collaborative approach.

Appendix C: Disclosure Tool

The Disclosure Tool takes the information in the Matrix further, outlining at a high level the type of information that can be disclosed by which type of organization (under what legislation) in what type of circumstance (type of services). While being at a relatively high level provides an indication of whether disclosure can occur, a more in-depth review of the specifics should be completed by the members once the collaborative services, member organizations and purpose are identified. The references to the legislative provisions or sections are abbreviated and should be reviewed in their entirety.

The collaborative members may choose to recreate the tables, using the above sets, and based on the specific circumstances they are dealing with and addressing.

Appendix D: Capacity Assessment

The Capacity Assessment is meant to help organizations determine if and what areas they may need to improve on in the management of personal and health information. The tool and Companion Guide can be used by the agency for their own purposes, or it can be used by the collaborating members as a means to determine if a particular agency is ready to be onboarded, given the way it manages information. To be used for that purpose, the members would need to determine what levels a potential participating agency would need to minimally meet.

Appendix E: Sample Commitment Agreement

The Sample Commitment Agreement is a template drafted for the use of partnering organizations when they determine they will be committing to working together. It differs somewhat from what may be perceived as more traditional in that it addresses the components that any organization would need to meet irrespective of what legislation they come under. While certain provisions within the agreement may only apply to certain organizations, including them all is meant to demonstrate to the partners what will authorize their partners to participate. As well, organizations that are not subject to any legislation do not generally have external oversight, and the agreement is meant to provide for that.

There are of course, other instruments that can be used. However, where organizations have agreed to work together there should be some documentation that identifies how they will do so in a collaborative manner, and that holds them accountable to some degree. Agreements do not replace or override legislation, but can serve to build on what the legislation entails.

Appendix F: Sample Consent Forms

The sample consent forms are designed for various circumstances, and should be reviewed by the partnering organizations to ensure they meet their requirements. They are all designed to meet the highest legislative requirements for the jurisdiction, thereby satisfying any legislative requirements.

Appendix G: Sample Training Resource

The training resources are meant to support the staff from any organizations when they work together in a collaborative or integrated manner. While they address a number of areas they should be reviewed and adjusted to reflect the circumstances of the partnering organizations. For example, staff need to understand and be able to explain to their clients the rationale that is the driver behind the member organizations working together, in a manner that the clients can understand. The actual purpose or rationale would need to be identified as part of the training.

Additional resources have also been identified in the Training Guide, and in Appendix J: Additional Resources.

Appendix I: Security Measures

The security measures, while not comprehensive, identify a number of areas and practices for consideration and use by the partnering organizations. As noted, legislation places an onus on organizations that manage personal and health information to ensure they protect that information, taking the necessary steps to prevent unauthorized access, and to minimize any potential harm that may come with such access. Partnering organizations should review the expectations and the manner in which they and their staff collectively manage information with their privacy, security, and IT, resources to ensure they have implemented practices that are commensurate with the sensitivity of the information they have responsibility for.

Appendix J: Additional Resources

There are a myriad of resources available to guide organizations in all of the areas the Framework touches on. This appendix identifies some of the key ones that should be attended to, along with others that have been deemed to be worthwhile exploring.

Appendix I: Security Measures

Privacy legislation requires that subject organizations ensure the appropriate level of security is in place, commensurate with the sensitivity of the information, against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction of the information they manage.

Technology continues to evolve at a rapid pace, leading to significant benefits including the ability to more efficiently manage information through electronic means. While most organizations are taking advantage of these benefits, and have moved to the use of technology as the default approach to managing information, the proliferation also means there are increasing risks that must be guarded against. In addition to the areas identified in the Framework under sections 8 and 9, organizations should consider and discuss addressing the following with their IT, HR, and building management staff.

Given the rapid evolution and introduction of new technologies, organizations should ensure that they employ and rely on the advice of IT staff or contractors who are up-to-date. The following describes some of the more foundational measures that should be considered for implementation to protect information from administrative, physical, and technical perspectives. They are not comprehensive, and resources are listed at the end that can provide further guidance.

The Environment

Administrative safeguards include ensuring:

- Lead responsibility for the management of security measures has been assigned, positioned sufficiently high in the organization to obtain necessary resources,
- Conducting a security assessment on the environment,
- Staff are trained:
    - to only access information they are authorized for, and require for the role and of the individuals they are providing services to,
    - on the consequences of inappropriate/unauthorized access or use of information,
    - on the relationships between their roles and those of others in the organization in the management of privacy and security,
    - to report any unauthorized access or breach of information or potential breach,
    - to never share or disclose their password,
    - to not open suspicious emails, texts,
    - on other necessary aspects of security management, both general and specific to their roles,
    - to display any assigned identification cards when on site in the workplace,
    - to request identification from persons in the work environment that are not familiar to them and not accompanied by other staff,
    - on any other necessary aspects of security management, both general and specific to their roles,
- Staff take oaths of confidentiality, sign non-disclosure agreements, or some other means of demonstrating accountability in managing information appropriately.

Physical safeguards include ensuring:

- File and server rooms are secure, with locked doors, accessed only by authorized staff, using card reader systems if appropriate,
- Doors close and lock automatically,
- Doors are checked and locked during off-hours, or when the building/site closes for the day,
- Alarm systems are in place if appropriate,
- Computer monitors oriented so to only be visible to the staff users,
- Files and documents are not in plain view of the public,
- Physical files are locked when not in use, desks are cleared every night.

Technical safeguards include ensuring:

- Card reader access logs are maintained for a period of time sufficient to manage identified risk or breach situations,
- Logs are reviewed on a proactive as well as post-complaint basis.

Technology:

Administrative safeguards include ensuring:

- An overarching security policy has been developed and implemented, supported by management,
- Staff are:
    - trained to deal appropriately with phishing attacks, dealing with unrequested/ unfamiliar email/text messages, and other forms of information security attacks,
    - provided credentials for access to electronic information management systems in accordance with their roles and need for access to information, role-based access is a preferred approach,
    - trained on the proper management of assigned credentials, passwords, use of technology, and access to information being restricted to that which they are authorized and require for their roles and the individuals they are responsible for,
    - trained to immediately report any loss of equipment or devices, any breaches or potential breaches of privacy or security to the designated individual,
    - trained to not use social media for communicating with or about the individuals or services provided to them unless approved by the organization.
- Policy and practice include reviewing read/write access logs to electronic systems on both a proactive and post-complaint basis.

Physical safeguards include ensuring:

- Access to electronic information system servers is restricted to authorized staff only
- Laptops and other portable devices are:
    - approved for use, with policies in place to provide oversight,
    - assigned to, and recorded when used by, staff,
    - secured when not in use,
    - transported securely when used out of the office,

- Physical hard drives are removed and securely wiped/destroyed when equipment is being refreshed/replaced/disposed of,
- Physical back up tapes are stored off site in secure locations.

Technical safeguards include ensuring:

- Electronic information management systems:
    - are protected with intrusion detection software, and tested periodically,
    - are accessed by authorized users using two- or multi-factor authentication,
    - credentials are managed and updated as staff change roles or leave their positions,
    - implement role-based access or other means of limiting access to authorized users,
    - are backed up on a scheduled basis, using physical or cloud based technology,
    - if using cloud-based technology ensure it meets standards (secure and appropriate for the data being managed and stored), be aware of cloud location, preferably in-country, and understand implications of laws applicable in that country if not,
- Networks are not accessible by non-authorized users,
- Virtual Privacy Networks (VPN) are implemented and used where appropriate,
- Change default passwords on devices, networks
- Computers, laptops, tablets, smartphones and other devices:
    - are outfitted with the appropriate security software including firewalls, antivirus, and other data protection software,
    - have software updates installed as updates become available,
    - use password protected screensavers, with short shut-down intervals,
    - use of Bluetooth technology is secure, with updates installed as they become available,
- Laptops and other portable devices:
    - Are outfitted and enabled for remote tracking and data deletion in case of loss,
- The use of Encryption:
    - for data stored outside of organization, including backed up data,
    - for transfer of information e.g., via email.

<u>Information/Records Inventories:</u>

Administrative safeguards include ensuring:

- An inventory of information holdings exists that is:
    - complete with archived/historical records maintained for the appropriate retention period,
    - properly backed up,
    - up-dated on a regular basis, when changes occur.
- Policies and procedures have been developed that include:
    - managing access, by users, and individuals to whom the information pertains to,
    - managing requests for access by researchers,
    - staff training requirements.

Physical safeguards include ensuring:

- Files and records are secure at all times, including:
    - storage of active and non-active records in secure controlled locations,

- files and records are locked up when not in use, including when staff using them are away from their desks/offices,
- inventoried as required under the retention/disposition policy.

Resources:

Securing Personal Information: A Self-Assessment Tool for Public Bodies and Organizations
Security-Self-Assessment-2020.pdf (oipc.ab.ca)

Small Business Tools to Protect Privacy
For businesses - Office of the Privacy Commissioner of Canada

Protecting Personal Information: A Guide for Business[50]
Protecting Personal Information: A Guide for Business | Federal Trade Commission (ftc.gov)

[50] While this guide was developed by the US Federal Trade Commission, it does provide some useful information.

Appendix J: Additional Resources

GENERAL

First Nations Sovereignty:
OCAP® Community Resources
Alberta First Nations Information Governance Centre | Resources (afnigc.ca)
Tri-Agency Research Data Management Policy
Tri-Agency Research Data Management Policy
National Inuit Strategy on Research
National Inuit Strategy on Research

Information Sharing:
Infographic: 6 Principles for Getting Information Sharing Right
Information-Sharing-2017.pdf (oipc.ab.ca)
Report on Findings and Implications for an Ethical Decision-Making Framework for Information Sharing:
CHH Report on Findings and Implications for an Ethical Decision-Making Framework for Information Sharing – PolicyWise for Children & Families
Information Sharing Education and Resources
Information sharing education and resources | Alberta.ca

Privacy Commissioners/Ombudsman
Canada (Federal)
Office of the Privacy Commissioner of Canada - Office of the Privacy Commissioner of Canada
Alberta Information and Privacy Commissioner
Office of the Information and Privacy Commissioner of Alberta (oipc.ab.ca)
British Columbia Information and Privacy Commissioner
Office of the Information and Privacy Commissioner for B.C. | Home
Manitoba Ombudsman
https://www.ombudsman.mb.ca/
New Brunswick Ombudsman
Ombud NB
Newfoundland and Labrador Information and Privacy Commissioner
https://www.oipc.nl.ca/
Northwest Territories Information and Privacy Commissioner
http://atipp-nt.ca/
Nova Scotia Information and Privacy Commissioner
https://oipc.novascotia.ca/
Nunavut
http://www.info-privacy.nu.ca/
Ontario Information and Privacy Commissioner
https://www.ipc.on.ca/
Prince Edward Island Information and Privacy Commissioner
https://www.assembly.pe.ca/offices/information-and-privacy-commissioner
Quebec Commission d'accès à l'information du Québec
http://www.cai.gouv.qc.ca/english/

Saskatchewan Information and Privacy Commissioner
https://oipc.sk.ca/
Yukon Information and Privacy Commissioner
https://yukonaccountability.ca/ipc

Privacy Management:

Privacy Breach Response, Reporting and Notification:
Privacy Breach Response, Reporting and Notification – Office of the Information and Privacy Commissioner of Alberta (oipc.ab.ca)
Health Information Act Guideline and Practices Manual, Chapter 14 (alberta.ca)
Managing breaches | Information and Privacy Commissioner of Ontario

Privacy Management Program - At A Glance
https://oipc.ab.ca/wp-content/uploads/2022/02/Accountability-Fact-Sheet-2012.pdf
Getting Accountability Right with a Privacy Management Program
Privacy Management Programs – Office of the Information and Privacy Commissioner of Alberta (oipc.ab.ca)

Privacy Impact Assessments
Privacy Impact Assessments – Office of the Information and Privacy Commissioner of Alberta (oipc.ab.ca)
Completing a privacy impact assessment : annotated template - Open Government (alberta.ca)

Research Privacy Tip Sheet:
PHSA Research Privacy Tip Sheet and Data Terms_2017Nov29.pdf

Security:

Bring Your Own Device
Bring-Your-Own-Device-2015.pdf (oipc.ab.ca)
https://oipc.ab.ca/wp-content/uploads/2022/02/Bring-Your-Own-Device-Tips-2015.pdf

HIA Guidelines and Practices: Chapter 11 – Records and Information Management, Privacy, and Security
Health Information Act Guidelines and Practices Manual, 2011 (alberta.ca)
See sections 11.3.3, 11.3.4

Protecting Personal Information: A Guide for Business[51]
Protecting Personal Information: A Guide for Business | Federal Trade Commission (ftc.gov)

Securing personal information: A self-assessment for public bodies and organizations:
Security-Self-Assessment-2020.pdf (oipc.ab.ca)

Small Business Tools to Protect Privacy
For businesses - Office of the Privacy Commissioner of Canada

[51] While this guide was developed by the US Federal Trade Commission, it does provide some useful information.

BY JURISDICTION

Canada

Legislation:
Justice Laws Website

Alberta

Legislation:
FOIP(POPA) Guidelines and Practices
https://open.alberta.ca/publications/9780778585633
FOIP Support
http://www.servicealberta.gov.ab.ca/foip/

HIA Guidelines and Practices Manual
Health Information Act Guidelines and Practices Manual, 2011 (alberta.ca)
health-hia-guidelines-practices-manual-chapter-15-2020-amendments-2021-04.pdf (alberta.ca)
Health Information Act Guideline and Practices Manual, Chapter 14 (alberta.ca)
HIA Support
Health Information Act | Alberta.ca

Personal Information Protection Act
Personal Information Protection Act – Overview | Alberta.ca
PIPA-Guide-2008.pdf (oipc.ab.ca)
PIPA
Personal Information Protection Act | Alberta.ca

Health Professions:
Alberta College of Social Workers (ACSW)
Practice Resources - ACSW
College of Alberta Psychologists
The College of Alberta Psychologists > Resources & Regulatory Information > Practice Guidelines (cap.ab.ca)
Legislation that may impact on Psychologists Practice
JURISPRUDENCE: LEGISLATION NAMING OR AFFECTING PSYCHOLOGISTS IN ALBERTA (March 2016) (cap.ab.ca)

British Columbia

Legislation:
Laws Publications - Government

Manitoba

Legislation:
Manitoba Laws

New Brunswick

Legislation:
Acts and Regulations - Attorney General

Newfoundland and Labrador

Legislation:
House of Assembly - NL - Consolidation

Northwest Territories

Legislation:
Bills & Legislation | Legislative Assembly of The Northwest Territories

Nova Scotia

Legislation:
Nova Scotia Legislature - Nova Scotia Statutes on the Internet - statute list

Nunavut

Legislation:
Welcome to the Nunavut Legislation website | Legislation

Ontario

Legislation:
e-Laws | Ontario.ca

Prince Edward Island

Legislation:
Statutes and Regulations | Government of Prince Edward Island

Quebec

Legislation:
https://www.legisquebec.gouv.qc.ca/en/

Saskatchewan

Legislation:
Law and legislation

Yukon

Legislation:
Statutes of Yukon | CanLII

Appendix K: Sample Integrated Cluster - Information Stored in IEIM or Central Repository

The following table outlines the collection, use, and disclosure of personal and health information between organizations that are involved in an integrated service delivery collaboration. Agencies A, B are core members, PS is a support on crisis calls, some agencies are external to the collaboration and receive referrals either as an ad hoc member, (provide expertise that requires access to personally identifying information – E.g. government agency or health custodian) or an extended member (does not require personally identifying information – E.g. Food Bank). The legislative authority provisions are generally stated, and would need to have the jurisdictionally appropriate provisions specified if to be relied on.

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
Agency A – Nonprofit with medical and social service staff		**Agency itself not subject to privacy legislation but aligns with provincial or federal private sector privacy legislation, medical staff subject to health privacy legislation.**				
Outreach	• Initial discussion, Notice provided, identifies individual, obtains contact information.	• Notice requirements	• Contact Information	• Authorized members requiring information, if involved	• Contact Information	• Authorized agency staff requiring information, if involved
	• Obtains consent to both access and enter information into IEIMS and Other.	• Collection with consent, • Disclosure with consent	• Consent Form	• Authorized members requiring information, if involved		
	• Conducts preliminary needs assessment.	• Use with consent,	• Preliminary Needs Assessment	• Authorized members requiring	• Preliminary Needs Assessment	• Authorized agency staff requiring

[52] (Cluster uses an Electronic Information Management System (IEIMS) to support the delivery of integrated case management; an Electronic Health Record (EHR) may also be used by custodians.
[53] Subject to consent or other provisions.
[54] Subject to consent or other provisions.

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	• Sets up internal service appointments.	• Use with consent,	• Referrals made	information, if involved • Authorized members requiring information, if involved	• Referrals made	information, if involved • Authorized agency staff requiring information, if involved
Case Workers (may be the same staff as on Outreach Team)	• Follows up from Outreach, collects some additional information to determine what other referrals would be relevant. • Provides referrals to other programs and services.	• Collection with consent, • Use with consent, • Disclosure with consent	• Expanded Needs Assessment • Referrals made	• Authorized members requiring information, if involved • Authorized members requiring information, if involved	• Expanded Needs Assessment • Referrals made	• Authorized agency staff requiring information, if involved • Authorized agency staff requiring information, if involved
Social Workers (SW)	• Provides counselling and support services. • Conducts more in-depth assessment, collecting additional information as required.	• Use with consent, • Collection with consent, Reviews consent[55]	• Case plan • In-depth needs assessment	• Authorized members requiring information, if involved • Authorized members requiring information, if involved in case planning		

[55] E.g., College of Social Workers, in keeping with Standards of Practice

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	• Refers to other programs as needed.	• Use with consent, • Disclosure with consent	• Referrals made	• Authorized members requiring information, if involved	• Referrals made	• Authorized agency staff requiring information, if involved
Psychologists	• Provides counselling and support services. • Conducts more in-depth assessment, collecting additional information as required • Refers to other programs as needed.	• Use with consent, • Collection with consent, Reviews consent[56] • Use with consent, • Disclosure with consent	• Case plan • In-depth needs assessment • Referrals made	• Authorized members requiring information, if involved • Authorized members requiring information, if involved in case planning • Authorized members requiring information, if involved	• Referrals made	• Authorized agency staff requiring information, if involved
Physician (Custodian under health privacy legislation)	• Provides medical services and supports. • Collects health information as required. • Makes referrals to other custodians (health professionals) as	• Collection • Disclosure to custodian	• Prescribed contact and health information	• Other custodians receiving referral for/or otherwise providing services.	• None	• None

[56] E.g., College of Psychologists, in keeping with Standards of Practice

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	deemed necessary. • Provides case plan input to other support services as deemed necessary. • Enters health information in electronic system(s) as appropriate.	• Disclosure with consent • Disclosure	*(Stored in EMR/EHR, not IEIMS)* • Case plan • Prescribed contact& health information *(Stored in EHR, Not IEIMS)*	• Authorized members requiring information, if involved in case planning • Other custodians receiving referral for/or otherwise providing services.		
Nurses (Affiliates to Custodian under the legislation)	• Supports physician in providing health services. • Accesses internal systems (referral and health information records), Other, and EMR/EHR (Connect Care) as needed. • Makes and follows up on case plan input, referrals made, as required.	• Deemed staff/employee/agent of custodian • Use, • Disclosure to custodian • Use • Disclosure with consent • Disclosure	• Prescribed contact and health information *(Stored in EMR, Not IEIMS)* • Case plan	• Custodians providing health services. • Authorized members requiring information, if involved in case planning	• Referrals made	• Authorized agency staff requiring information, if involved

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	• Updates health records as required.		• Prescribed contact and health information *(Stored in EHR, Not IEIMS)*	• Custodians providing health services.		
Agency B – social service staff		**Agency not subject to privacy legislation but aligns with provincial or federal private sector privacy legislation.**				
Case Workers	• Follows up from Outreach referrals, collects some additional information to determine if other referrals would be needed. • Provides referrals to other programs and services.	• Collection with consent, • Use with consent • Disclosure with consent	• Expanded Needs Assessment • Referrals made	• Members requiring information, if involved • Authorized members requiring information, if involved	• Expanded Needs Assessment • Referrals made	• Authorized agency staff requiring information, if involved • Authorized agency staff requiring information, if involved
Social Workers	• Provides counselling and support services. • Conducts more in-depth assessment, collecting additional information as required.	• Use with consent • Collection with consent, Reviews consent (see footnote 4) • Use with consent	• Case plan • In-depth needs assessment • Referrals made	• Authorized members requiring information, if involved in case planning • Authorized members requiring information, if involved in case planning	• Referrals made	

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	• Refers to other programs as needed.	• Disclosure with consent		• Authorized members requiring information, if involved		• Authorized agency staff requiring information, if involved
Psychologists	• Provides counselling and support services. • Conducts more in-depth assessment, collecting additional information as required. • Refers to other programs as needed.	• Use with consent • Collection with consent, Reviews consent (See Footnote 5) • Use with consent, • Disclosure with consent	• Case plan • In-depth needs assessment • Referrals made	• Members requiring information, if involved in case planning • Members requiring information, if involved in case planning • Authorized members requiring information, if involved	• Referrals made	• Authorized agency staff requiring information, if involved
Agency PS (Police Service) working in conjunction with Agency A on crisis support calls		**Public Sector Privacy Legislation**				
Outreach Team	• Provides support, including information regarding any potential risks they are aware of, in response to call for outreach services	• Collection • Use		• Agency B accesses contact information and referrals. Other information restricted on need-to-know basis, e.g., involved in case planning.	• None	• None

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	• Documents interactions with individuals involved	• Disclosure for health and safety reasons. An argument may be made that the information compiled in police databases is also to inform police for situations when they become involved with the individual, and the involvement in an outreach team approach has expanded that involvement. Outreach team members who are not police services should likely sign a non-disclosure agreement, and not use the information for any other purpose.	• Notes regarding involvement, for case planning as needed	• Members requiring information, if involved in case planning		
	• Intervenes if there are risks or as needed for outstanding warrants.	• Collection for law enforcement purposes	• None			
Provincial Government Social Service Department (Peripheral involvement)[57]		**Public Sector Privacy Legislation**				

[57] Determination regarding the access to the Other Repository by any of the Peripheral Agencies needs to be made, including whether it is read only or write access as well, and for what information. Restrictions may be to only allow access to referrals and referral status, and based on consent.

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
Intake staff receiving referrals	• Assesses eligibility and provides benefits if approved • Provides status update	• Collection, s.33 (a)(c) • Disclosure with consent			• Referral status[58]	• Authorized agency staff requiring information, if involved
Agency FB (Food Bank) – Extended member peripheral to integrated service		**Agency not subject to privacy legislation but aligns with provincial or federal private sector privacy legislation.**				
	• Provides food hampers	• No collection, minimal information may be disclosed to Food Bank to indicate the referral came from agency "X"				
Agency SR (Addiction Support and Rehab)[59] – Ad hoc member of integrated service		**Licensed rehab centre, may be aligned with provincial or federal private sector privacy legislation, or subject to health privacy legislation if working under a contract or agreement with a health custodian.**				
Intake and counselling staff.	• Respons to referral, • Assesses and provides counselling, • May provide limited status update (i.e., confirmed	• Collection with consent • Collection/use • Disclosure with consent – Note the consent may be part of the initial referral	• Referral status (may be expanded for	• Members requiring information, if involved in case planning	• Referral status	• Authorized agency staff requiring

[58] Referral status may be restricted to whether the individual was seen, not whether they were eligible for benefits or services.
[59] The involvement of this agency and the referral status should be considered from the perspective of case-planning and -management if it involves the agency.

Staff (Role)	Services and Information Required	Legislative Authority	Information Stored in IEIMS[52]	Accessed By[53]	Information Stored in Other Central Platform/System	Accessed By[54]
	participation) with consent.		case planning purposes)			information, if involved
Agency HS (Health Care Service)[60]		**Health Sector Privacy Legislation**				
Medical and support staff	• Responds to referral, • Assesses and provides services, • May provide limited status update (e.g., confirmed participation) with consent.	• Collection • Use • Disclosure with consent – Note the consent may be part of the initial referral	• Referral status (may be expanded for case planning purposes)	• Members requiring information, if involved in case planning	• Referral status	• Authorized agency staff requiring information, if involved
Agency CL (Peripheral Co-located Agency)		**May be aligned with provincial or federal private sector privacy legislation, or subject to public sector privacy legislation if working under a contract or agreement with a public sector organization.**				
Housing Support	• Responds to referral, Assesses and provides services, • May provide limited status update (participation) with consent.	• Collection with consent – Note the consent may be part of the initial referral • Disclosure with consent – Note the consent may be part of the initial referral	• Referral status (may be expanded for case planning purposes)	• Members requiring information, if involved in case planning	• Referral status	• Authorized agency staff requiring information, if involved

[60] The involvement of this agency and the referral status should be considered from the perspective of case-planning and -management if involved.