



An Information Sharing Framework:

Supporting Enhanced Collaboration between Organizations

Providing Mental Health Services

CONVERGE Mental Health

Acknowledgements

The materials and development of the following Information Sharing Framework were developed with the input and contributions of a number of organizations and was made possible with funding provided by the Hunter Family Foundation, through CONVERGE Mental Health.

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.

Mental Health Services
Information Sharing Framework

Table of Contents:

Introduction	6
Using the Framework.....	7
Collaborative Continuum.....	8
1. Purpose	14
1.1. Purpose (for Working Collaboratively):	14
1.2. Objectives/Outcomes:	15
2. Membership / Partners	15
2.1. Core Members:	16
2.2. Extended Members:	16
2.3. Ad Hoc Members:	17
3. Roles and Responsibilities	17
4. Governance and Accountability	17
4.1. Lead Organization Structure	18
4.2. Committees/ Advisory Structure	23
4.3. Decision Making	23
4.4. Decision Socialization	23
4.5. Responsibility for Records/Information	23
4.6. Demonstrated Commitment:	24
5. Applicable Legislation	26
5.1. Privacy Legislation	26
5.2. Other Legislation	29
5.3. Matrix	30
5.4. Disclosure Tool	31
6. Policies, Practices, Procedures	31
6.1. Minimum Requirements	31
6.2. Collection, Use, Disclosure in General:	31

6.3. Collection	33
6.4. Use	36
6.5. Disclosure	36
6.6. Documentation	37
6.7. OCAP® - Ownership, Control, Access and Possession	38
6.8. Correction	38
6.9. Retention and Disposition	39
6.10. Terminology / Interpretations	40
6.11. Conflict Resolution	42
6.12. Training	42
6.13. Onboarding	42
7. Information and Records	43
7.1. Required Information	43
7.2. Creating Records	44
7.3. Common Records	44
7.4. Individual Agency Records	45
7.5. Single Source of Truth	45
7.6. Consent	45
7.7. Client Information	46
7.8. Client Access	47
7.9. User Information	47
7.10. Electronic/paper records	47
7.11. Coordinated Case Management Tools	48
7.12. Administrative Information	48
8. Electronic Information Management	48
8.1. Legal Requirements	49
8.2. System Access/Management	49
8.3. Information/Document Management	50
8.4. Storage	51
9. Security and Risk/Mitigation	51
9.1. Responsible Area	51
9.2. Review and Audit (Pre- and post-complaint)	51
9.3. User Environment	52

9.4. Breaches	53
10. Evaluation and Research	54
10.1. Evaluating Individual Outcomes (E.g., of case plans or interventions)	55
10.2. Evaluating the overall approach (i.e., collaborative approach)	56
10.3. Using Data for Research	56
List of Appendices:	58
Appendix A: Applicable Legislation	58
Appendix B: Privacy Legislation Disclosure Matrix	58
Appendix C: Disclosure Tool	58
Appendix D: Capacity Assessment Tool and Guide	58
Appendix E: Sample Commitment Agreement	58
Appendix F: Sample Consent Forms	58
Appendix G: Sample Training Resource	58
Appendix H: Guide to Using the Information Sharing Framework	58
Appendix I: Security Measures	58
Appendix J: Additional Resources	58

Introduction

[Back](#)

It is estimated that 1 in 5 Canadians will suffer a mental health disorder in their lives. Addictions and Mental Health¹ 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.”²

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

¹ For ease of reference, while the Framework refers to mental health supports it should be read as inclusive of addictions.

² “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.

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 a 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

The intent of the Framework is to provide guidance on the areas that need to be considered and addressed as organizations determine there is a need to collaborate. 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 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. 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 an often-narrow perspective of compliance with the individual legislation. 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.

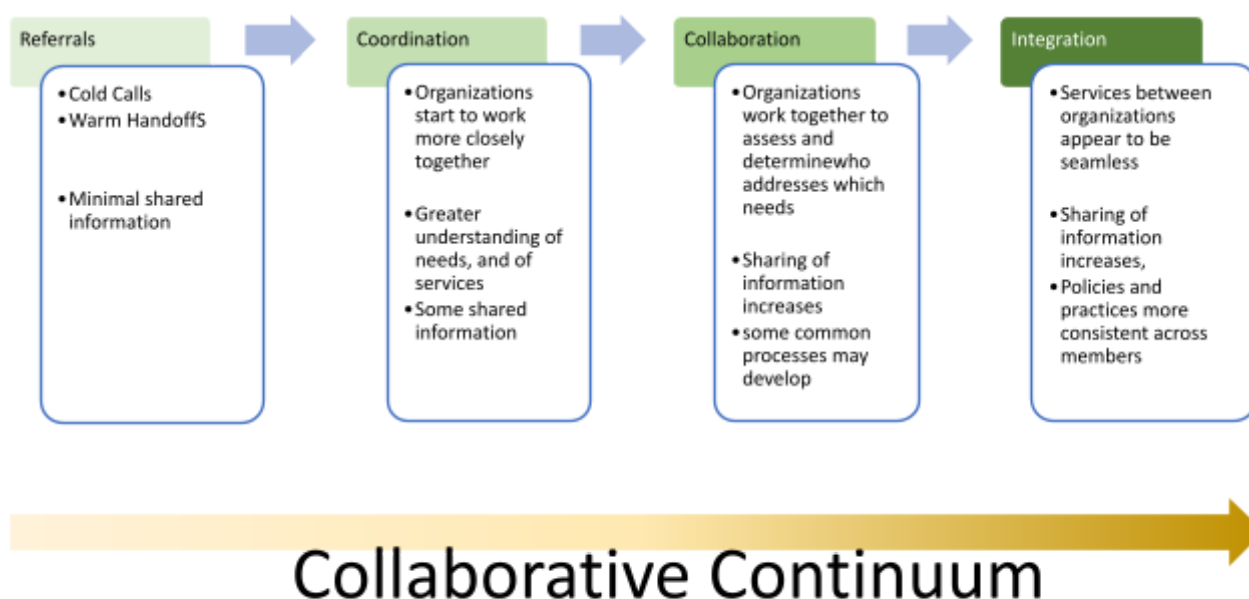
Given the broad range of supports and services provided by a broad range of organizations from different sectors that are subject to differing legislation, the Framework is at times written at a relatively high level. For this reason, it is important that as organizations work through the template, they ensure 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 Office of the Information and Privacy Commissioner (OIPC). The OIPC is also a strong resource and has prepared many publications for use by organizations

that manage personal and health information in Alberta. 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

The following graphic demonstrates the Collaborative Continuum. As engagement between organizations moves increasingly to the right of the continuum, there is an increased need for the organizations involved to collaborate, and 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, it should be noted that as collaboration moves closer to the right side of the continuum, the need for formalized processes in support of integration of those services between the partnering organizations 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 continuum³. As such, the framework addresses those potential variations in service delivery approaches. Each section of the framework will identify the starting points on the continuum at which they could be applied (i.e. Coordination, Collaboration, Integration).



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.

³ 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 the Coordinated, Collaborative or Integrated Service Delivery.

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.

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
All Services	Referral	X	?							
Support to person in need in community	Warm handoff	X	X	X						
	Coordinated support	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
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

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
	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

1. Basic: no true dependencies per se, but relationship between needs may exist.
2. Collaborative: some dependencies may exist, some increased level of information sharing required, such as reporting on progress.
3. 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, who is a custodian under the *Health Information Act* (HIA) to ensure that there are sufficient and effective mental health supports for the students they have responsibility over. The school board is subject to the *Freedom of Information and Protection of Privacy Act* (FOIP). 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 includes:

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

- For the purpose it was collected, [s.40(1)(c)]
- With consent, [s.40(1)(d)]
- To determine eligibility for a program or service, [s.40(1)(l)]
- To avert the risk of harm to a minor, [s.40(1)(ee)(i)]
- To avert the risk of imminent harm to a person, [s.40(1)(ee)(ii)]
- To avert risk to the safety of the public, [s.32] or
- In the best interest of the minor [s.40(1)(gg)].

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 or 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)].

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 or social worker who would also be required to follow their Professional College's Standards of Practice. The Standards of both Colleges listed (College of Alberta Psychologists, Alberta College of Social Workers) strongly advise of the use of informed consent before disclosing the personal information of their client, but also recognize that information can be disclosed without consent in situations where there is a risk of severe and imminent harm, or where authorized and required by law.

If the student is a minor, and if the health professional is employed or working on behalf of a custodian, or a public body, then the *Children First Act* could apply, in addition to the HIA or FOIP. Privacy legislation, including FOIP and the HIA have provisions that authorize disclosure without consent where other legislation authorizes or requires the disclosure of information.

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. 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 being potentially causative of the youth's mental health concerns).

Guidance or decisions regarding at what point a student may be deemed to be at sufficient risk of causing harm (i.e., where is the bar set?) should be determined in advance and there would be value in providing training to all stakeholders on any agreed upon processes.

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.
- ii) The results of the assessment and potential need for some intervention may be information that is of value for the student and for the school, so that they 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. 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.

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.

The **Framework** would 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, there are a variety of touch points, reasons why organizations may work together, and degrees to which they may 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 an initial assessment of services required or requested by the individual will be conducted, perhaps by the first point of contact, with the intent of sharing that initial information, along with the individual's contact information, after which each member organization that determines they may be in a position 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 collaborative per se, although the identified service needs may serve to provide a direction for the client.
- **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 that determines they may be in a position to provide services would work independently with the client. In this situation, only the initial collection of information is shared between the member organizations. 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 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 they will conduct an initial assessment of needs and strengths of the individual, followed by the development of a comprehensive or coordinated case management plan, one that identifies the responsibilities of the involved member organizations. The involved member organizations would use the case plan as their starting point, and may need to update it periodically, indicating progress, although additional information they collect as they provide 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 possibly 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.

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 to 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 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, 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 important to recognize the potential for different roles to exist within an organization, which may not only influence 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: the differences within a service delivery organization between 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 most likely ones 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 are 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 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 include:

List the organizations here.

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. 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 include organizations to which referrals are made but who do not require the sharing of significant amounts of personal and health information. For example, the agency may only need to know the name and some contact information of the referral, and perhaps the knowledge that the individual being referred is involved with the collaborative (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 for this initiative include:

List the organizations here.

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.

3. Roles and Responsibilities

[Back](#)

The roles and responsibilities will vary according to the type of membership, 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.

Information listed here should be specific to the collaborative approach and membership.

Role	Description	Requires Type of Information
<i>E.g., Intake, (Service Provider)</i>	<i>Completes initial intake/ assessment</i>	<i>Contact information, needs/ presenting issue identification</i>
<i>E.g., Counselling, (Service Provider)</i>	<i>Provides counselling support</i>	<i>More in-depth client information such as have led to mental health status – may include personal and health information</i>
<i>E.g., Eligibility for Needs, (Service Provider)</i>	<i>Determines eligibility for and ongoing management of benefits and services</i>	<i>Client information required to determine and maintain eligibility</i>
<i>Advisory Committee</i>	<i>Reviews processes</i>	<i>General, no identifying information</i>

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 reality 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.

Accountability is critical in the management of personal and health information by organizations. Having the appropriate accountabilities outlined and in place serve 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 public bodies subject to FOIP, or Custodians subject to the HIA 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.

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	<p>Responsible to coordinate the leadership team and activities, which includes to:</p> <ul style="list-style-type: none"> • 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. Office of the

Area of Responsibility	Activities
	<p>Information and Privacy Commissioner, regulatory body(-ies), should the need exist),</p> <ul style="list-style-type: none"> • contract for (if necessary), manage any support areas, and oversee the secretariat activities as required on behalf of the partnership. • responsible for management of (common) records and information
Leadership Table	<p>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:</p> <ul style="list-style-type: none"> • 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)	<p>Responsible for the coordination of relevant activities, which includes to:</p> <ul style="list-style-type: none"> • 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. Office of the Information and Privacy Commissioner, 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	<p>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:</p> <ul style="list-style-type: none"> • 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

Area of Responsibility	Activities
	<p>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, there should be a process agreed to that includes vetting and approval of drafts put forward for approval.)</p> <ul style="list-style-type: none"> • 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)	<p>Each organization would maintain its own responsibility for their organization’s activities, as well as their participation in the collaborative partnership including to:</p> <ul style="list-style-type: none"> • 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. Office of the Information and Privacy Commissioner should the need

Area of Responsibility	Activities
	<p>arise), although a decision to have a representative for the collaborative partnership could be made,</p> <ul style="list-style-type: none"> • 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	<p>Membership includes the leads for each of the core partners of the collaborative partnership. Responsible to:</p> <ul style="list-style-type: none"> • 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:

Participating Agency Staff	<p>This includes staff who are selected by their organization to participate in the collaborative service delivery approach. These staff are responsible to:</p> <ul style="list-style-type: none"> • 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,
----------------------------	--

	<p>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,</p> <ul style="list-style-type: none"> ● 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.
--	--

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, evaluation committees, and so forth.

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 a record of previous policies and their effective dates may be necessary.

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: Member Organization 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 **<Insert Name of the Collaborative Approach>** do so with the full understanding that they agree to:

- manage personal and health information in accordance with 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 **<Insert name of the committee or leads that will address these>**.

Member organizations will demonstrate their commitment:

4.6.1. To the <Insert Name of 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 **<Insert name of the committee or leads that will address these>**.

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 (e.g., 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, they may have to come to an agreement about a common consent for disclosure form that potentially differs from the one their organization has in place.); through determining what evaluation processes and reporting requirements will be agreed on (E.g., consideration of data requirements, efficiencies in collection, and reporting by whom, ...); and potentially even the use, obligations and language of contracts with agencies who may also be involved in contracting with other members.

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 the services rendered 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. The first area can work well with other member organizations, becoming involved earlier, when there is the potential for early intervention to de-escalate or prevent the risk from evolving to a higher level that requires significantly more intrusive measures. However, 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. To 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 G: Sample 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 the legislation contains a number of other provisions that may also have an impact. For example, FOIP requires that a public body only discloses information to the extent necessary to carry out the purposes identified in a reasonable manner (s.40(4)). Similarly, the HIA identifies one of its purposes to prescribe rules regarding the collection, use, and disclosure in the most limited 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.

The collection, use and disclosure of non-identifying information is generally authorized by the legislation, either implicitly (e.g. FOIP, PIPA) or explicitly (HIA ss. 19, 26, 32). It should be noted 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.

5.6. Privacy Legislation

5.6.1. Freedom of Information and Protection of Privacy Act (FOIP)

The *Freedom of Information and 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 contact, financial, employment, educational, and health information. Note that health information managed by public bodies is deemed to be personal information. By way of example, a custodian under the HIA, such as a physician, may use health information to fill in a form requesting medical information from a public body. 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 FOIP, 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: providing access by an individual to their own information, or to records held by a 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.

5.6.2. Health Information Act

The *Health Information Act* applies to custodians in Alberta, defined to include the department of Health, hospital boards, regional health authorities, and regulated health service providers who provide a health service, as currently defined in the regulations (Chiropractors, Optometrists, Pharmacists, Dentists, Registered Nurses, Denturists, Midwives, Opticians,

Physicians and Surgeons, Podiatric Physicians, Dental Hygienists). Many of these health professionals are employed by organizations who may in fact be defined as a custodian under the Act, such as Alberta Health Services, 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, 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; 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 circumstances⁴; 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 .

5.6.3. Personal Information Protection Act

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

⁴ 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 discuss the individual and information on how they are progressing; but an agency that is seeking advice regarding potential referral for services for a client may not have to identify the individual to obtain the advice.

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.

5.6.4. Privacy Act (federal)

The federal *Privacy Act* applies to government institutions in Canada, defined to mean any department or ministry of state (...) of the Government of Canada, and any parent Crown Corporation (...).

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.

5.6.5. Personal Information Protection and Electronic Documents Act (federal)

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) 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 and BC, who have passed their respective Personal Information Protection Acts. However, if an organization transports personal or health information in a commercial context across provincial boundaries, the information is subject to PIPEDA versus PIPA.⁵

The Act also 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.

5.7. 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.

5.7.1. Children First Act

The *Children First Act* applies to

- ‘service providers’ – defined to mean Government of Alberta departments, educational bodies as defined in FOIP (does not include private schools), police services as defined in the Police Act (includes the RCMP), and individuals or agencies providing programs or services for children under an agreement with a (FOIP) public body; and to
- ‘custodians’ as defined under the HIA.

The Act recognizes in its preamble that programs and services for children are most effective when they are provided through a collaborative and multi-disciplinary approach; and that the appropriate sharing of information between individuals and organizations planning or providing programs and services for children is critical to ensuring successful outcomes for children and families. It enables the sharing of personal information of a child, or of the guardian of a child between service providers where it is necessary for the planning and enabling of services or benefits for the child. It also enables the sharing of health information of a child by a custodian to a service provider where it is necessary for the planning and enabling of services for the child.

The Act also requires that the service provider or custodian (holder of information) making the disclosure is of the opinion that the disclosure is in the best interests of the child. That sets out the opportunity for dialogue, as the service provider seeking information may need to provide some information themselves in order to encourage or convince the holder of information that it is in fact in the child’s best interest.

⁵ 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](#).

5.7.2. Health Professions Act and corresponding Regulations

(including Codes of Conduct, Standards of Practice)

The *Health Professions Act* sets out authority for the establishment of a ‘college’ (meaning the college of a professional association) and the authority through which specified professions are regulated and managed. The Act currently applies to 28 health professions, as listed in the Schedules. The Act is important not only from the perspective of how it enables the creation of Standards of Practice by the Colleges for their members, but it also serves as the source from which custodians may be included under the Health Information Act and Regulations.

The Standards of Practice provide guidance and requirements for the members on a number of areas, including the disclosure of information, which then serve as another process that influences how a member will manage the personal and health information of their clients. There is the potential for such processes to be interpreted as more restrictive, so it will be important to clarify how information held by regulated health professionals that is required to be shared in the context of collaborative practices can and will be managed. Depending on the relationship the health professional has (e.g., as an employee, affiliate, or as a professional corporation, and with whom) there may be a need for more clarity on the intersection of these sets of legislation and professional requirements to ensure clarity amongst all those members who need to work together.

It is worth noting that the application of legislation to a health professional under the *Health Information Act*

5.8. 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”

5.9. 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 <Insert Name of the Collaborative Approach> are in addition to, and 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, 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 will address the matter at the <Insert name of the committee that will address these>.

6.6. 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 areas have been approved by the <Insert Name of the 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 <Insert name of the committee or leads that will address these>.

6.7. Collection, Use, 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, and to match them against the services they deliver. Working together, the organizations should broadly determine what needs to be collected. 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 behind 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.

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. By Public Bodies subject to FOIP:

Personal information will only be collected, used and disclosed in accordance with the provisions under the *Freedom of Information and Protection of Privacy Act* (specifically, Part 2), 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.

6.2.2. By Custodians subject to the HIA:

Health information will only be collected, used and disclosed in accordance with the provisions under the *Health Information Act* (specifically, Parts 3 - 5), 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 PIPA:

Personal information will only be collected, used and disclosed in accordance with the provisions under the *Personal Information Protection Act*, (specifically, Part 2), 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.

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), 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 legislation, 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 followed, such that the organization is acting as if subject to the *Personal Information Protection Act*.

6.3. Collection

Clearly articulating the manner in which members of the collaborative partnership will undertake the collection of personal and health information is one of the cornerstones of, and reasons for, the development and implementation of the framework. Privacy legislation requires that the personal and health information of an individual be collected directly from the individual it pertains to. 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 the 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. Staff should be trained on what those circumstances might be.

Privacy legislation requires that the personal and health information of an individual be collected directly from the individual it pertains to unless specified circumstances come into play. (HIA s. 22, FOIP s. 34, PIPA s.12, *Privacy Act* s. 5(1)). For the purposes of this collaborative partnership, 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 will be identified under the following subsection iii.

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 providing services, in keeping with the objectives and outcomes of the collaborative service delivery.

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 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 what information is being requested, for what purpose, how it will be used, and to whom it may be disclosed. As well, the name and contact information of a person who can answer any questions the individual may have about the collection must be provided.

Recognizing that an individual in crisis is not necessarily in the best position or frame of mind to understand 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.

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 in the assessment and delivery of services through the collaborative partnership.

C. Integrated Service Delivery:

When Notice is provided regarding the collection of personal and health information for the use by 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 in the assessment and delivery of services through the integrated partnership.

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 documented here.

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:

- When the individual has consented to such collection, [FOIP s.34(1)(a)(i), HIA s.22(2)(a), PIPA, s. 7(1), *Privacy Act* s.5(1)];
- 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), [FOIP s.34(1)(c), HIA s.22(2)(d), PIPA, s. 14(a)];
- When collecting the information is in, or would prejudice, the best interests of the individual, [HIA s.22(2)(c), PIPA, s.14(a), *Privacy Act* s.8(2)(m)(ii)];
- 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, [FOIP s.34(1)(c), HIA s.22(2), PIPA, s. 14(a)];
- *< 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

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 required by law”.)

In addition to the direct purpose, there may be consistent purposes 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.

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).

6.5. Disclosure

Disclosure, or the sharing of personal and health information, is the reason for the framework to be implemented. 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 such 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, 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 (c) Collection) 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 decide they need to collaborate it is important to determine generally the type of information they will be working 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, from 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.

Sample flow charts are included in **Appendix ____**.

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. OCAP® - Ownership, Control, Access and Possession

OCAP®⁶ refers to the need for First Nations to establish and manage sovereignty over their own data. The principles of OCAP® outline⁷:

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.

⁶ 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.

⁷ From: OCAP® FAQ, <https://afnigc.ca/main/index.php?id=ocap&content=OCAP%20FAQs>, Alberta First Nations Information Governance Centre.

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.

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 Alberta First Nations Information Governance Centre (AFNIGC) may provide further support in understanding how to work with these principles.

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. [FOIP s.35(a),36, HIA s.13, PIPA, s. 33, 25, *Privacy Act* s. 5, 12(2)]

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 **<Insert name of the area that will address this>**, 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 **<Insert name of the area that will address this>**.
- The **<Insert name of the area that will address this>** will make the appropriate correction. Where the information has been previously collected and in use, the **<Insert name of the**

area that will address this will notify organizations that have accessed or used the information of the correction.

- In situations where the client is requesting a change to an opinion, an annotation should be made, indicating what the client is requesting, but the opinion would not be changed.
- In all situations where the correction request is received, the client should be advised of the outcome of the request.

6.9. Retention and Disposition

For the purposes of this collaborative partnership, a retention period of **<The collaborative will need to determine what the retention period (e.g., 10 years) is for records deemed to be in its control or custody. >** will be in place, for common records once the file activity has completed. The records will be retained by **<Identify party responsible>**. This retention period does not apply to records that are maintained by the individual members, as their own retention and disposition policies and schedules will apply.

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.

As noted previously, individuals have a right of access to their own information, which lasts as long as an organization has retained it. FOIP requires that a public body retains information for a minimum of one year if it is used to make a decision that directly affects the individual, (FOIP s. 35).

Individuals also have a right to know who has access to their information. The HIA requires that information about a disclosure be documented and retained for a minimum of 10 years. (HIA s. 41) The use of information stored in the electronic health record by authorized custodians must also be recorded and retained for a minimum of 10 years (HIA s. 56.6).

The PIPA requires that information be retained for as long a period of time as the organization reasonably requires it for business or legal purposes, and then either destroys or renders it non-identifying within a reasonable period of time. (PIPA s. 35)

6.10. Terminology / Interpretations

The following terms are ones the member organizations have agreed need to be clarified in how they are to be understood within the context of this collaborative approach.

List any such terms or 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 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.

- 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 health and safety. 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, consideration must note 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 especially might 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 work through how they will respond. Areas to be considered 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?

Health and Safety provisions that might apply include:

FOIP s.40(1)(ee); HIA s.35(1)(m); PIPA s.20(g); PIPEDA s.7(3)(e); *Privacy Act* 8(2)(m)(ii)

Other provisions including best interests that might apply include:

FOIP s.40(1)(gg); HIA s.35(1)(p); PIPA s.20(a); *Privacy Act* 8(2)(m)(ii)

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 stricter 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 in Alberta is not 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, the HIA? If so, it may be best if an adopted consent form meets the requirements under the HIA, which impose additional requirements.
 - If a new consent form is adopted for use by the collaborative members, are there any potential implications for consent forms used individually by the member agencies? (See also: H.5.Consent Forms, p.39)

6.11. 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 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 **<Insert name of the committee or area that will address this>**. 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.

6.12. 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.

6.13. Onboarding

While the membership will generally be determined at the outset of the collaborative approach, there is potential for new potential member organizations to be identified. As such, the following process will be used when potential organizations are to be considered and invited to participate. Approvals will involve the core membership through the **<Insert Name of the Identified Leadership or Advisory Table>**.

- The organization will be provided a copy of the framework, including a description of the purpose, including desired objectives and outcomes.
- At a minimum, the organization is expected to manage information in a confidential manner, and have the technical and environmental capacity to access any systems appropriately (e.g., confidentially, with appropriate security mechanisms in place). As such they should complete the capacity assessment (See: “Appendix D: Capacity Assessment Tool”) and otherwise 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, 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

The information that is required by organizations involved in the collaborative approach in order 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
<i>E.g., Contact information, including name, DoB, address</i>	<i>E.g., Identification, contact</i>	<i>E.g., Intake</i>
<i>E.g., Identified Needs, capacity</i>	<i>E.g., Conducting an initial screening and assessment for services</i>	<i>E.g., Intake</i>
<i>E.g., Medical, health, social background</i>	<i>E.g., Conducting a more in-depth assessment once referred to member organization for counselling</i>	<i>E.g., Caseworker, counselling</i>
<i>E.g., Family history, educational background, employment history,</i>	<i>E.g., Identifying underlying issues to determine additional supports if required</i>	<i>E.g., Caseworker, housing and employment</i>

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, the collaborative operates in an environment that optimizes the health and safety of the individuals being provided supports. Working to maintain a 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)

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.

FOIP defines a record to include any information stored or recorded in any form but does not include the mechanism or software that produces the record. [FOIP s.1(q)] Further, the Act requires that any information that is used to make a decision that directly affects the individual, that information (and as per the above, a record), must be retained for at least one year... [FOIP s.35]

The HIA defines a record in a similar manner to include any health information stored or recorded in any form but does not include the mechanism or software that produces the record. [HIA s.1(1)(t)]

PIPA defines a record to include a record of information in any form or in any medium... [PIPA s. 1(1)(m)]

When organizations work in a collaborative or integrated service delivery approach, the information they share is found in records they hold, and may 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 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, in a secure manner.

Records that have been 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*
- *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 maintain it within their own systems will need to be alerted or advised of changes to the parent information.

7.6. Consent

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.

The HIA places additional requirements. Consent under the HIA must also include:

- An acknowledgement that the individual providing the consent has been made aware of the reasons why their health 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
- 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).

Both the HIA and FOIP recognize the validity of consent being in writing or electronic form provided that the management of the electronic consent meets the outlined requirements (See HIA s.34(2), FOIP s.40(1)(d) and FOIP Reg.s.7). The FOIP Act and Regulations go further and allow for oral consent but there must have been rules established by the head of the public body as to the circumstances and the manner under which either electronic or oral consent would occur.

The *Personal Information Protection Act* also addresses consent, authorizes consent to be provided in writing, electronically, or orally; and further, also requires the capacity for an individual to withdraw their

consent. The federal *Personal Information Protection and Electronic Documents Act* essentially outlines similar expectations but provides a more thorough explanation of what must be considered; while the federal *Privacy Act* simply outlines that consent is a requirement.

Consent for disclosure, as noted, is common across all privacy legislation as a means to authorize the disclosure of personal and health information. 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, ideally those under the HIA. 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. Individuals in crisis may not always attend to what they are being told, and in some situations may agree to whatever they think will enable their receiving the services or supports they require. Revisiting consent in these types of situations 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.

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 be 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 credentialing 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 is not adequate.

On the other hand, information that is stored electronically can be much more easily provided, and even pushed out, to stakeholders and users. 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.

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. There may be a need 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. There may be a need to ensure use of a consistent approach.

Training materials are generally deemed to be administrative, not requiring 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 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

Access to the system or platform, should be delegated to a specific, central role, often linked to 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 (every 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.

Not all systems can implement role-based access controls (RBAC), or may not be able to apply them to all data elements. As such, there may be a need to implement both the technical (RBAC, access trails) and administrative 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 an efficient indexing process.

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?
- 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 requires that organizations take reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. (FOIP s. 38; HIA s.60; PIPA s.34; PIPEDA s.4.7 in Schedule 1) 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.

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 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 to the Office of the Information and Privacy Commissioner under the HIA (s. 60.1) and PIPA (s. 34.1). Breaches under FOIP may also be reported, and must be investigated, whether reported to the Office of the Information and Privacy Commissioner 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 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 breach⁸;
- 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 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 is required, that

⁸ 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 generally be to notify the individual(s) but there may be circumstances where that may create a greater risk to the individual, for example if due to their mental health it may trigger a crisis situation. These are likely rare situations.

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 \(oipc.ab.ca\)](https://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 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 community level higher if number 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 control and own 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 Alberta First Nations Information Governance Centre (AFNIGC) provides additional resources, and is a good starting point for further support in understanding how to work with these principles.

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 Families⁹.

10.3. 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 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 will it be shared, and
- How will it be managed? (E.g., how will an access request from the individual be managed?)

10.4. 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

⁹ Ethical Decision-Making Framework for Information Sharing: A Guide for the Homeless-Serving Sector by PolicyWise for Children & Families:
<https://afnigc.ca/main/index.php?id=resources&content=community%20resources>

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. The HIA under section 27(1)(g) authorizes the use of individually identifying health information for internal management purposes, including evaluation. However, disclosure provisions do not specifically include evaluation. As such, the disclosure of that information would need to be specifically need to be included in 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 the custodian of the information to conduct any evaluations, if they are part of the collaborative approach.

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.
- 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.

10.5. 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. For example, the use of any health information for research purposes requires a submission of the proposed research protocol to a research ethics review board. [HIA s.49] Further, the use of health information in data matching may require obtaining consent of the individuals, and the submission of a PIA. [HIA s. 68 – 72] Alberta Health has provided a template to support the completion of the assessment (see Appendix J: Additional Resources).

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.

List of Appendices:

Appendix A:	Applicable Legislation
Appendix B:	Privacy Legislation Disclosure Matrix
Appendix C:	Disclosure Tool
Appendix D:	Capacity Assessment Tool and Companion Guide
Appendix E:	Sample Commitment Agreement
Appendix F:	Sample Consent Forms
Appendix G:	Sample Training Resource
Appendix H:	Guide to Using the Information Sharing Framework
Appendix I:	Security Measures
Appendix J:	Additional Resources

Prepared by: George Alvarez
on behalf of CONVERGE Mental Health