CONVERGE

REIMAGINING CANADA'S MENTAL HEALTH SYSTEMS – TOGETHER.

An Information Sharing Framework:

Supporting Enhanced Collaboration between Ontario Organizations Providing Mental Health Services

Acknowledgements

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

The Framework is being used by various groups and organizations in Alberta. Converge and its members recognizes the potential value for its use in other jurisdictions, as the issues are the same across the country, and beyond. Given that, Converge is interested in supporting the adaptation of the Framework materials for use in other jurisdictions. This version has been adapted for such use, with legislative references now placed in the appendices. The sets of appendices are being updated by jurisdiction.

Version Control

v.2	References to Alberta Appendices replaced.

Mental Health Services

Information Sharing Framework

Table of Contents:

Introduction 6
Using the Framework 7
Collaborative Continuum 8
1. Purpose 14
1.1. Purpose 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
2.4. Other Members: 17
3. Roles and Responsibilities 17
4. Governance and Accountability 18
4.1. Lead Organization Structure 18
4.2. Committees/ Advisory Structure 24
4.3. Decision Making 24
4.4. Decision Socialization 24
4.5. Responsibility for Records/Information 25
4.6. Demonstrated Commitment: 25
5. Applicable Legislation 27
5.1. Provincial/Territorial Privacy Legislation 29
5.2. Federal Privacy Legislation 31
5.3. Other Legislation 32
5.4. Matrix 32
5.5. Disclosure Tool 32
6. Policies, Practices, Procedures 32

6.1. Minimum Requirements 33
6.2. Collection, Use, and Disclosure in General: 33
6.3. Collection 36
6.4. Use 39
6.5. Disclosure 39
6.6. Documentation 40
6.7. Indigenous Data Sovereignty 40
6.8. Correction 42
6.9. Retention and Disposition 42
6.10. Terminology / Interpretations 43
6.11. Conflict Resolution 45
6.12. Training 45
6.13. Onboarding 45
7. Information and Records 46
7.1. Required Information 46
7.2. Creating Records 47
7.3. Common Records 47
7.4. Individual Agency Records 48
7.5. Single Source of Truth 48
7.6. Consent 48
7.7. Client Information 49
7.8. Client Access 50
7.9. User Information 50
7.10. Electronic/paper records 50
7.11. Coordinated Case Management Tools 51
7.12. Administrative Information 51
8. Electronic Information Management 51
8.1. Legal Requirements 52
8.2. System Access/Management 52
8.3. Information/Document Management 53
8.4. Storage 54
9. Security and Risk/Mitigation 54
9.1. **Responsible Area** 55

9.2. **Review and Audit (Pre- and post-complaint)** 55
9.3. User Environment 55
9.4. Breaches 56
10. Evaluation and Research 58
10.1. Evaluating Individual Outcomes 59
10.2. Evaluating the overall approach 59
10.3. Using Data for Research 60
List of Jurisdiction Specific Appendices: 61
Appendix A: Applicable Legislation 61
Appendix B: Ontario Privacy Legislation Disclosure Matrix 61
Appendix C: Disclosure Tool 61
Appendix D: Sample Collaborative Approach Training Resource 61
Appendix E: Sample Commitment Agreement 61
Appendix F: Sample Consent Forms 61
List of Generally Applicable Appendices: 61
Appendix G: Capacity Assessment Tool and Companion Guide 61
Appendix H: Guide to Using the Information Sharing Framework 61
Appendix I: Security Measures 61
Appendix J: Additional Resources 61
Appendix K: Sample Information Flow Table 61

Introduction

Back

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

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

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

---

[1] *Mental Illness and Addiction: Facts and Statistics* (CAMH)

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

[3] "Lifeso, N., Parker, N., McInnes, S., Babins-Wagner, R., Scott, C., & Brown, K. (2020) "*Understanding the Current Landscape of Emerging Adult Mental Health Services and Needs in Calgary and Surrounding Area"*. Edmonton: PolicyWise for Children & Families. Emerging Adult - Final Report

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

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

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

Using the Framework

Information sharing in and of itself is not the end goal, but rather a means of facilitating organizations to collectively work with individuals and families to provide them with the supports and services they may require. This Framework is meant to provide guidance on the areas that should be considered and addressed as organizations determine there is a need to develop or enhance their existing collaborative service delivery approaches. While not all elements will be required in every situation, consideration should be given to the areas that do apply. As noted in the section on the Collaborative Continuum (below), the greater the degree of collaboration, especially when organizations start to work in an integrated manner, the greater the amount of formalization, and potentially changes, in processes and policies are required. Additionally, the greater the degree of collaboration, the greater the need for the partnering organizations to ensure the appropriate application of the provisions in the privacy legislation they are subject to. To that end, the Framework is meant to support organizations to collectively apply an *'information sharing lens'* in how they apply those provisions. It will assist such organizations to put in place processes where personal and health information is readily shared where required, to support a holistic approach to meeting the needs of the individuals they support, as they will have gone through the process of applying and validating the necessary authorities to do so; and to do so in a privacy conscious manner. It should be noted that there already exists a robust number of resources developed to support the application of the various individual privacy legislations. However, those resources are often developed with a relatively narrow focus on compliance with the individual legislation, without balancing the risks that may emerge if information is not made available for legitimate uses. As such, the application of an 'information sharing lens' through the use of the framework is meant to augment those resources by demonstrating how the various legislations can be collectively applied in support of a collaborative approach such that all the members can see how the integration can work.

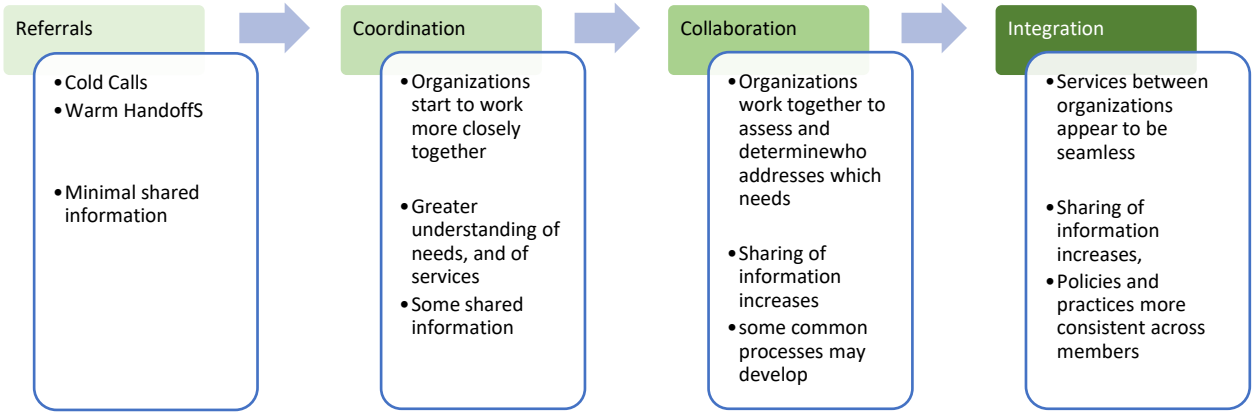
Given the broad range of supports and services provided by an even broader range of organizations from different sectors that are subject to differing legislation, the Framework is at times written at a relatively high level. For this reason, it is important that as organizations work through the template,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

Collaborative Continuum

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

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

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



Collaborative Continuum

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

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

Service Required	Collaborative Process	Name	Contact Information	Initial Needs Identification	Initial Needs Assessment	In Depth Needs Assessment	Health Information	Financial Information	Safety Information	Case Management Plan
		Type of Information								
All Services	Referral									
Support to person in need in community	Warm handoff	X	X	X						
	Coordinated support	X	X	X	X				X	
	Collaborative support	X	X	X	X	X			X	2
	Integrated support	X	X	X	X	X	X	X	X	3
Supports for youth homelessness	Warm handoff	X	X	X						
	Coordinated support	X	X	X	X		X	X	X	1
	Collaborative support	X	X	X	X	X	X	X	X	2
	Integrated support	X	X	X	X	X	X	X	X	3
Supports for adult homeless-ness	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	X					
	Coordinated support	X	X	X	X		X		X	1
	Collaborative support	X	X	X	X	X	X		X	2
	Integrated support	X	X	X	X	X	X	X	X	3
Risk of Harm to Self	Warm handoff	X	X	X	X					1
	Coordinated support	X	X	X	X		X	X	X	1
	Collaborative support	X	X	X	X	X	X	X	X	2
	Integrated support	X	X	X	X	X	X	X	X	3

Service Required	Collaborative Process	Name	Contact Information	Initial Needs Identification	Initial Needs Assessment	In Depth Needs Assessment	Health Information	Financial Information	Safety Information	Case Management Plan
		Type of Information								
Risk of harm to minor	Warm handoff	X	X	X	X				X	
	Coordinated support	X	X	X	X		X	X	X	1
	Collaborative support	X	X	X	X	X	X	X	X	2
	Integrated support	X	X	X	X	X	X	X	X	3
Risk of harm to adult	Warm handoff	X	X	X	X				X	
	Coordinated support	X	X	X	X		X	X	X	1
	Collaborative support	X	X	X	X	X	X	X	X	2
	Integrated support	X	X	X	X	X	X	X	X	3

Case Management Plan Levels

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

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

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

Sample Scenario:

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

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

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

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

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

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

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

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

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

[5] See Appendix A - Specific Legislative References, Note 1, Legislation that Might Apply to the Scenario.
[6] See Appendix A - Specific Legislative References, Note 14, Disclosure.

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

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

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

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

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

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

1. Purpose

Back

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

1.1. Purpose (for Working Collaboratively):

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

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

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

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

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

developed, outlining the areas that individual member organizations are taking responsibility for, especially if there are any service dependencies identified.

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

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

1.2. Objectives/Outcomes:

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

2. Membership / Partners

Back

Member organizations that will be involved may fall into a number of categories. Identifying them will assist in a number of areas, including defining the roles they will play within the collaborative approach, the legislation that may impact how those roles are enabled, and the type and level of detail of the information they may require to fulfill those roles. It’s also important to recognize the potential for different roles to exist within an organization, which may influence not only what information is required by the staff in those different roles, but also how the

information will be managed within the organization (e.g., degree or amount of access). Examples of different roles within an organization include: intake, which may involve an initial high-level assessment of need, and counselling, which could require a deeper dive into underlying issues; or the difference in the roles police services may play between community engagement, which may require members to be involved in assessment, early intervention and support, and law enforcement, which may require urgent responses to crisis situations.

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

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

2.1. Core Members:

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

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

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

2.2. Extended Members:

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

Alternatively, extended members may refer to organizations who do not require the sharing of significant amounts of personal and health information, if any. For example, the agency may only need to know the name and some contact information of the person(s) being referred, and perhaps that the individual being referred is involved with the collaborative approach (perhaps as evidence of the eligibility for the referred to services).

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

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

2.3. Ad Hoc Members:

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

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

2.4. Other Members:

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

3. Roles and Responsibilities

Back

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

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

Sample Table of Roles and Required Information

Information listed in the table below should be specific to the collaborative approach and membership.

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

4. Governance and Accountability

Back

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

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

4.1. Lead Organization Structure

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

The following options are not all-inclusive, and other ones may exist that are more suitable to the circumstances and jurisdictions within which you operate. What is important, is the need to

identify accountability that not only reflects how the various member organizations manage the personal and health information they require and use, but also provides assurance to the individuals and families they support that their personal information will be managed in a privacy-conscious manner.

Option 1: Lead (Primary) Organization:

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

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

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

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

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

Option 2: Shared Leadership

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

In this model, the leadership could be structured to have more than one level, the Leadership Table itself, comprised of executive/senior level representatives of the partners, who would provide oversight and upper-level decisions; as well as a team made up of middle management or

other level representatives who could be largely responsible for the day-to-day decisions and management.

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

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

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

Option 3: Fully Autonomous Organizations

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

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

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

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

Across All Options:

Area of Responsibility	Activities
Participating Agency Staff	This includes staff who are selected by their organization to participate in the collaborative service delivery approach. These staff are responsible to: • become educated on and implement any policies and practices that have been developed and identified for use within the collaborative partnership,

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

4.2. Committees/ Advisory Structure

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

4.3. Decision Making

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

4.4. Decision Socialization

The process by which decisions are published or made available to those staff, organizations or clients for which there are implications or changes required should be outlined. Updates to

policies, practices and procedures should be made, with effective dates identified and logged. It may be necessary to demonstrate what policies, etc. were applied when, so records of previous policies and their effective dates should be maintained as needed.

4.5. Responsibility for Records/Information

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

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

4.6. Demonstrated Commitment:

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

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

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

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

- manage personal and health information in accordance with the policies and practices developed under the framework,
- ensure their staff are trained on the framework, and any changes that may be required in their roles,
- work with all member organizations, and
- address any issues or concerns, including potential privacy or security breaches, through the identified area responsible (may be an individual, specific role or position, or a committee).

Member organizations will demonstrate their commitment to:

4.6.1. The Collaborative Approach:

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

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

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

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

4.6.2. Ensuring staff are trained:

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

Training may also include areas such as the following:

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

5. Applicable Legislation

Back

The following discussion on applicable legislation deals primarily with personally identifying information. It is important to note that it is not only the provisions dealing with collection, use, and disclosure that need to be taken into consideration, as legislation contains a number of other provisions that may also have an impact. For example, privacy legislation expressly or implicitly requires organizations to only disclose information to the extent necessary to carry out the purposes identified in a reasonable manner and to the highest degree of anonymity that is possible in the circumstances. These and other provisions must be considered within the context of what the organizations are intending within their collaborative approach[7].

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

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

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

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

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

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

5.1. Provincial/Territorial Privacy Legislation

5.1.1. Freedom of Information and Protection of Privacy Act (FIPPA)

The *Freedom of Information and Protection of Privacy Act* applies to institutions in Ontario, defined to include Includes provincial ministries, service provider organizations as per the *Ministry of Government Services Act*, and hospitals, amongst others. (see FIPPA s.2)

The Act deals with personal information, which is defined to mean recorded identifying information about an individual, including but not limited to information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; any identifying number, symbol or other particular assigned to the individual.

5.1.2. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

The *Municipal Freedom of Information and Protection of Privacy Act* applies to institutions in Ontario, and applies to local government institutions in Ontario, including municipalities, police service boards, school boards, conservation authorities, boards of health and transit commissions, among others. (see MFIPPA s.2)

The Act deals with personal information, which is defined to mean recorded identifying information about an individual, including but not limited to information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; any identifying number, symbol or other particular assigned to the individual.

5.1.3. Personal Health Information Protection Act 2004

The *Personal Health Information Protection Act* applies to health information custodians in Ontario, defined to include

- A health care practitioner or a person who operates a group practice of health care practitioners,
- A health service provider or person or entity that is part of an Ontario Health Team and that provides a home and community care service pursuant to funding under section 21 of the Connecting Care Act, 2019. A health service provider or person or entity that is part of an Ontario Health Team is a health information custodian in connection with the provision of any home and community care service within the meaning of the Connecting Care Act, 2019, even where a particular home and community care service is not funded under that Act.
- A person who operates one of the following facilities, programs or services:
    - A hospital within the meaning of the Public Hospitals Act, a private hospital within the meaning of the Private Hospitals Act, a psychiatric facility within the meaning of the Mental Health Act or an integrated community health services centre within the meaning of the Integrated Community Health Services Centres Act, 2023.

- A long-term care home within the meaning of the Fixing Long-Term Care Act, 2021, a placement co-ordinator described in subsection 47 (1) of that Act, or a care home within the meaning of the Residential Tenancies Act, 2006.
- A retirement home within the meaning of the Retirement Homes Act, 2010.
- A pharmacy within the meaning of the Drug and Pharmacies Regulation Act.
- A laboratory or a specimen collection centre as defined in section 5 of the Laboratory and Specimen Collection Centre Licensing Act.
- An ambulance service within the meaning of the Ambulance Act.
- A home for special care within the meaning of the Homes for Special Care Act.
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care.

And includes an agent, defined to mean a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian. [PHIPA section 2]

The Act deals with personal health information, which is defined to mean identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019,
- relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- is the individual's health number, or
- identifies an individual's substitute decision-maker.

and includes

- identifying information that is not personal health information described in subsection (1) but that is contained in a record that contains personal health information described in that subsection.

5.1.4. Connecting Care Act, 2019

- The Act applies to service providers as defined within the Act,
- Outlines the intent for delivery of an integrated care system,
- Establishes Ontario Health Teams as authorized entities,
- Recognizes that Indigenous peoples have a role in the planning and delivery of health services in their communities.

5.2. Federal Privacy Legislation

5.2.1. Privacy Act

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

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

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

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

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

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

The Act does not apply to an organization that conducts its business within a province that has been deemed to have substantially similar legislation, including Alberta, BC, and Quebec.[8] who have passed their respective private sector privacy laws. Several provinces have enacted health sector legislation that is also deemed substantially similar to PIPEDA. These include New Brunswick, Newfoundland and Labrador, Nova Scotia, and Ontario. However, if an organization transports personal or health information in a commercial context across provincial boundaries, the information is likely subject to PIPEDA.[9]

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

---

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

[9] 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*.

5.3. Other Legislation

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

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

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

5.4. 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”

5.5. Disclosure Tool

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

See “Appendix C: Disclosure Tool”

6. Policies, Practices, Procedures

Back

Applicable to Collaborative partnership:
The policies, practices and procedures outlined and adopted by the Collaborative Approach are in addition to those of the member organizations, and should be agreed upon by all participating member organizations, for use during activities that come under the collaborative approach. Where there is a discrepancy between these policies and the organization’s own internal ones, there should be agreement that these will apply. Any areas of conflict should be brought to the attention of the home organization’s lead for the collaborative partnership for resolution. In situations where the Lead is not able to resolve the conflict in keeping with the direction of the

collaborative approach, they matter can be addressed by the identified position(s) or committee responsible for resolution.

6.1. Minimum Requirements

Legislation serves as a minimum standard that should be applied across the board. Where there is potential to involve organizations that are not subject to any oversight legislation as members of a collaborative partnership, a set of minimum standards should be established that mirror the expectations placed on other member organizations through their applicable legislation. Such organizations would be required to demonstrate how they meet those minimum requirements, and assistance to those who are not at the required level could be offered if their involvement is desired.

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

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

6.2. Collection, Use, and Disclosure in General:

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

The intent in using the framework is to develop or outline a set of criteria that if met enables an effective and efficient flow of information. The degree of comfort with this may evolve over time. If situations emerge where reasons to not disclose appear, further discussion at the

appropriate group or committee may be necessary. **Note that having been approved as a member organization in the initiative does not give a user authority to access information broadly.** Rather, the user is only authorized to access the information they require of individual clients they are assessing or providing support to.

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

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

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

The following sections reflect the potential application of legislation.

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

Personal information will only be collected, used and disclosed in accordance with the provisions under the applicable legislation[10], 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.

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

6.2.2. By Health Organizations subject to Health Information legislation:

Health information will only be collected, used and disclosed in accordance with the provisions under the applicable health legislation[11], in keeping with and in support of the collaborative partnership's stated purpose and objectives. Where disclosure is clearly aligned with the collaborative partnership's objectives, the default will be to disclose the information where required and authorized, unless there is a strong overlying reason not to. Such disclosures will be the minimum amount required to achieve those objectives.

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

Personal information will only be collected, used and disclosed in accordance with the provisions under the applicable legislation[12], 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.[13]

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

6.2.6. By organizations not subject to any privacy legislation:

Where an organization or person is not subject to any privacy legislation[15], 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 and Electronic Documents Act* or substantially similar provincial/territorial legislation. In addition, the non-privacy legislated

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

organization should enter into an agreement with the partner organizations, such as that contained in Appendix E: Sample Commitment Agreement, to demonstrate some level of accountability.

6.3. Collection

Clearly articulating the reasons or purposes[16] for the collection of personal and health information about an individual, along with the manner in which members of the collaborative partnership will undertake that collection, are cornerstones of, and reasons for, the development and implementation of the framework. Privacy legislation generally requires that the personal and health information of an individual be collected directly from the individual it pertains to, subject to specific exceptions. That may seem to preclude the notion of reducing the number of times that an individual needs to repeat his or her story, one of the benefits of a collaborative or integrated service delivery approach. However, the legislation also recognizes and authorizes situations where personal and health information can be collected indirectly. It is critical therefore, that the manner of collecting be defined and that any indirect collection be authorized in accordance with any applicable legislation.

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

6.3.1. Direct Collection

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

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

A. Collaborative Service Delivery

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

B. Integrated Service Delivery:

[16] See Appendix A - Specific Legislative References, Note 8, Collection.

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

6.3.2. Notice

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

Individuals whose information is being requested directly from them must be provided Notice. Providing Notice means advising the individual of the authority for the collection of their information: what information is being requested, for what purpose (i.e., how it will be used), and to whom it may be disclosed. As well, the contact information of a person/position who can answer any questions the individual may have about the collection must be provided. Legislative references pertaining to informing individuals/providing Notice are listed in Appendix A.[17]

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

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

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

A. Coordinated Service Delivery

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

B. Collaborative Service Delivery

[17] See Appendix A - Specific Legislative References, Note 9, Notice.

When Notice is provided regarding the collection of personal and health information for the use by a collaborative service delivery, such Notice shall include information about the collaborative services, and the purpose for which the information is collected, the legal authority for the collection, and indicate that the information will be disclosed for use by the member organizations involved with the individual in the assessment and delivery of services through the collaborative partnership.

C. Integrated Service Delivery:

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

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

6.3.3. Indirect Collection

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

Indirect collection (i.e., where information is collected from someone other than the individual to whom it pertains) is authorized by legislation and by the policies of this collaborative partnership in the following situations:[18]

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

< 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.>

[18] See Appendix A - Specific Legislative References, Note 10, Indirect Collection.

6.4. Use

Privacy legislation restricts the use of information about an individual to the purpose(s) for which it was collected.[19] Personal and health information that is collected for the purposes and objectives set out in this collaborative partnership will only be used for those purposes, unless otherwise authorized. *(The collaborative partnership leads should identify how decisions on what is acceptable to meet the criteria of 'unless otherwise authorized' are made. Sample situations for such uses may include "where authorized or required by law".)*

In addition to the direct or initial purpose, there may be consistent purposes[20] that should be considered. For example, when determining whether or not particular services are beneficial to the individual, conducting an evaluation of the services is consistent with their delivery. Services cannot be effectively provided in isolation of gauging their effectiveness, at both the individual and organizational level.

As noted earlier, there may also be situations where information needs to be used to prevent or deal with situations where there is a potential risk to health and safety of individual(s). If the purpose was identified as one of the initial reasons for collection, then it is duly authorized and used for that initial purpose. If however, that purpose was not identified as part of the original purpose, there is then a need to rely on the provisions in the privacy legislation that authorize such collection and use.[21]

6.5. Disclosure[22]

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

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

[19] See Appendix A - Specific Legislative References, Note 11, Use.
[20] See Appendix A - Specific Legislative References, Note 12, Consistent Purpose.
[21] See Appendix A - Specific Legislative References, Note 13, Health and Safety.
[22] See Appendix A - Specific Legislative References, Note 14, Disclosure.

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

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

6.5.1. Information Flow

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

Sample flow charts are included in Appendix K.

6.6. Documentation

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

6.7. Indigenous Data Sovereignty

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

OCAP®[23] refers to the rights of First Nations to establish and manage sovereignty over their own data. The principles of OCAP® outline[24]:

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

Control asserts that First Nation people, their communities, and representative bodies must control how information about them is collected, used, and disclosed. This extends to all aspects

[23] 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.
[24] From: OCAP® FAQ, OCAP®-FAQs-compressed.pdf, Alberta First Nations Information Governance Centre.

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 First Nations Information Governance Centre (FNIGC) may provide further support in understanding how to work within these principles.

6.7.2. Tri Agency Framework

The principles of Ownership, Control, Access and Possession (OCAP®) are one model for First Nations data governance, but this model does not necessarily respond to the needs and values of distinct First Nations, Métis, and Inuit communities, collectives and organizations. The agencies recognize that a distinctions-based approach is needed to ensure that the unique rights, interests and circumstances of the First Nations, Métis and Inuit are acknowledged, affirmed, and implemented.[25]

6.7.3. National Inuit Strategy on Research

The National Inuit Strategy on Research (NISR) outlines the coordinated actions required to improve the way Inuit Nunangat research is governed, resourced, conducted, and shared. This strategy builds upon the important strides taken by Inuit towards self-determination in research by offering solutions to challenges our people have grappled with for decades.[26]

[25] From Tri-Agency Research Data Management Policy
[26] From National Inuit Strategy on Research

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[27].

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

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

6.9. Retention and Disposition

As noted previously, individuals have a right of access to their own information,[28] which lasts as long as an organization has retained it; as well as a right to know who has accessed their information. Legislation should be reviewed to determine:

- Any requirements an organization has to retain information used to make a decision that directly affects the individual, and for what length of time,
- Any requirements on the organization to document and retain information regarding access to or disclosure of an individual's personal information, and for what length of time[29].

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

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

[27] See Appendix A - Specific Legislative References, Note 15, Corrections.
[28] See Appendix A - Specific Legislative References, Note 16, Right of Access by Individuals.
[29] See Appendix A - Specific Legislative References, Note 17, Retention.

- This retention period does not apply to records that are maintained by the individual members, as their own retention and disposition polices and schedules will apply.

6.10. Terminology / Interpretations

Words matter. However, words are also subject to interpretation, and impacted by work environments, areas of specialization, and other factors. If organizations are going to work together, they have to establish or acknowledge what is meant by the terminology that they have in use. This becomes critical not only with various terms, but also with themes and other elements, including those that are identified within the framework. For this reason, it is incumbent on the organizations to work through what is meant and what is required by areas such as Purpose, Outcomes, and Objectives. Policies and practices should also be examined to identify any areas where there may be dissonance or some level of conflict or disagreement.

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

The following terms are samples of ones that may need to be clarified in how they are to be understood within the context of this collaborative approach.

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

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

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

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

Legislative provisions that might apply include:

- Health and Safety provisions[30],

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

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

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

[30] See Appendix A - Specific Legislative References, Note 13, Health and Safety.

- If a new consent from is adopted for use by the collaborative members, are there any potential implications for consent forms used individually by the member agencies?

See Section 7.6 Consent, below.

6.11. 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 committee or area empowered to address it. The outcome of any discussions should be shared as appropriate, and where they have an impact on the larger membership, should be noted accordingly and brought to all staff's attention, as appropriate.

6.12. 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, additional member organizations to be identified. As such, the following process may be used when potential organizations are to be considered and invited to participate. Approvals will involve the core membership through the appropriate leadership table.

- The new/potential organization will be provided a copy of the framework or outlined approach, including a description of the purpose, which in turn includes desired objectives and outcomes.
- At a minimum, the new organization is expected to manage information in a confidential manner, and have the technical and environmental capacity to access any systems appropriately (i.e., confidentially, with appropriate security safeguards in place). The capacity assessment (See: "Appendix G: Capacity Assessment Tool and Companion Guide") can be useful to demonstrate any additional requirements. Depending on the outcomes of the assessment, the organization will be

  - Supported to address any shortcomings
  - Expected to address any shortcomings
  - Approved to participate
- Once approved to participate, they will be asked to sign the Commitment Agreement *(or whichever similar tool has been developed and implemented)*, and to train their participating and relevant staff.
- Staff must be trained prior to activating their participation, especially when they will be provided with any credentials for access to systems or databases.

7. Information and Records

Back

7.1. Required Information

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

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

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

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

Additional uses

As noted above, the use of information is primarily linked to the supports, services and benefits that are being assessed for and potentially offered. There may be situations where other downstream uses also exist. For example, the need to evaluate the effectiveness of an intervention or service delivery approach is important as it will help gauge the value of the collaborative approach. Such a use is deemed consistent with the purpose for which information

is collected, as programs and services cannot be delivered in isolation of evaluating their effectiveness.

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

7.2. Creating Records

Organizations that collect and use personal and health information in order to provide services to individuals are bound to keep records of any decisions that may impact on those individuals, including records that contain the information on which those decisions are based. Those records may exist in various formats, including electronic and hard copy (e.g., paper).[31]

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

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

7.3. Common Records

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

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

[31] See Appendix A - Specific Legislative References, Note 18, Records.

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

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

E.g.,

- *Client profile (Name, DoB, Address)*
- *Consent for disclosure form*
- *Common screening and assessment*
- *Common risk assessment*
- *Comprehensive case management plan*

7.4. Individual Agency Records

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

7.5. Single Source of Truth

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

7.6. Consent[32]

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

[32] See Appendix A - Specific Legislative References, Note 19, Consent.

framed as information about the collaborative, as a means of providing clarity about the collaborative – its purpose, types of services, and member organizations.
- **For what purpose**. Individuals have a right to know how the information will be used. The purpose should be clearly stated, and is likely linked to the purpose and objectives for the collaborative approach. There may be additional purposes that are not as evident, such as ones where required or authorized by law.

Additional requirements or best practices include:

- An acknowledgement that the individual providing the consent has been made aware of the reasons why their information is needed and the risks and benefits to the individual of consenting or refusing to consent.
- The date the consent commences, and the date it expires, if any, and
- A statement that the consent may be revoked at any time. (Individuals who withdraw their consent should be advised of the implications of doing so, and that should they revoke their consent, any further disclosures would cease, but the information that has been disclosed prior to the revocation would still form part of a record of services being or having been rendered).

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

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

Note that the use of a common consent for disclosure form does not negate the responsibility of professional staff to explain how the information managed by the professional will be used and disclosed, so to ensure their client is fully aware. Discussions such as these can only serve to enhance the relationships with the individual and support transparency. This requirement is often outlined in the Standards of Practice developed by health and other profession colleges.[33]

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

7.7. Client Information

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

[33] See Appendix A - Specific Legislative References, Note 20, Professional Colleges.

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 have been provided at the point of giving Notice or consent, may need to be reiterated at any point a request is made.

7.9. User Information

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

7.10. Electronic/paper records

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

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

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

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

7.11. Coordinated Case Management Tools

Case management tools are increasingly available for organizations to improve their ability to capture and track the activities taken when supports and services are provided to their clients. They are often implemented through mobile applications, and can be made available to allow multiple individuals and organizations to work on the same case. Organizations that decide to use case management tools as a means of increasing communications and efficiency when working collaboratively need to ensure that they are developed and implemented properly, with the appropriate mechanisms in place to track and monitor the individual user access and inputs. Safeguards will also be required to prevent unauthorized access.

7.12. Administrative Information

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

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

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

8. Electronic Information Management

Back

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

practices with others pay particular attention to doing so in a privacy conscious manner, and implementing the appropriate tools and safeguards.

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

A number of areas within the Framework are related to the use of such a system or platform, and should be considered and applied from that perspective. The following sections touch on some of the areas that should be considered, whether expanding the use of an existing system or implementing a new one.

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

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

8.1. Legal Requirements

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

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

8.2. System Access/Management

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

8.2.1. System Access/Credential Management

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

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

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

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

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

8.2.2. Role Based Access

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

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

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

8.3. Information/Document Management

An electronic information management system can be relatively simple, in that it only holds a minimal amount of information; or can be quite robust, not only having the capacity to hold

significant amounts of information, being able to maintain electronic copies of paper or hard copy records, and to segregate the information in whatever manner is deemed appropriate, such that the data or information can be readily available for the specific uses. For example, segregation of the data could assist in the de-identification for use in evaluation and research. The data has to be appropriately managed in its entirety throughout its life cycle. Putting in place the appropriate electronic system can in effect act as an enhanced file room with efficient indexing processes.

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

8.3.1. Information Access/Flows

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

- What information will be entered, and how?
- Will other systems feed into it, and how will that be managed?
- How will it be accessed, by whom?
- How will it be used, will/can it be copied?
- Will it be streamed into other systems?

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

8.4. Storage

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

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

9. Security and Risk/Mitigation

Back

Privacy legislation generally requires that organizations take reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.[34] 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,

[34] See Appendix A - Specific Legislative References, Note 21, Security of Information.

and through its eventual ceasing of operation. Responsibility for overseeing the implementation and management of secure processes for the collaborative approach should be identified. The process for reporting of issues, incidents, or breaches should be clearly outlined and provided to all staff involved in the collaborative.

9.1. Responsible Area

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

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

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

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

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

9.3. User Environment

9.3.1. Mobile/Work from Home

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

In addition, staff should ensure they:

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

9.3.2. Bring Your Own Device (BYOD)

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

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

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

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

9.4. Breaches

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

All breaches of personally identifying information must be reported as required by the applicable legislation.[35] Breaches that are not addressed under legislation may also be reported, and must be investigated, whether reported to a Commissioner/Ombudsman or not. Breaches under PIPEDA are required to be reported to the federal Privacy Commissioner if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual (s.10.1).

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

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

9.4.1. Preventing a Breach

As noted, legislation (and best practice where an organization might not be subject to legislative oversight) requires organizations to take reasonable safeguards to ensure that any information

[35] See Appendix A - Specific Legislative References, Note 22, Breaches.

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 breach;[36]
- provide any support to that individual to manage the implications of the breach (e.g., access to credit bureau protection in situations where there may be a financial implication, including identity theft)
- advise the Office of the Information and Privacy Commissioner/Ombudsman of the breach;
- implement any additional measures (policy/practice/system changes, additional training, etc.)

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

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

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

10. Evaluation and Research

Back

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

While it may be readily easy for an individual being provided support services to understand why certain information is required to meet their needs, that may not be the case when it comes to understanding the need to measure the effectiveness of the services themselves. Staff should be provided some messaging in this area as it's important to be as open and transparent as possible on how information will be used. A balance must be struck between the 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 (e.g., name, SIN, DoB, address), reduction of specific data (E.g., age instead of date of birth, DA (Distribution Area) instead of postal code, month of service in lieu of date of service…), using larger cell counts, or increasing the level being measured (e.g., going to a higher community level if numbers in a certain target population are too low to preclude re-identification.

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

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

The First Nations Information Governance Centre (FNIGC)[37] provides additional resources, and is a good starting point for further support in understanding how to work with these principles.

Ethical Considerations:

Related to the above, disclosures of personally identifying information should not only be considered from the perspective of their legality, (i.e., they have been properly authorized) but they should also be considered from an ethical perspective – is it the right thing to do, with consideration of the impacts or implications at both an individual and a population or societal level. Guidance in this area can be found in a report completed by PolicyWise for Children and Families.[38]

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

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

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

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

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

The delivery of programs and services also needs to be evaluated at a broader level, beyond their effectiveness in addressing individual outcomes. Are they doing what they are intended to? Are they targeting the right demographics? Are there gaps that are not being addressed? Measuring this in a collaborative service delivery approach goes back to the identified purpose and objectives, and requires the member organizations to collectively determine how that will be measured. It will also require the sharing of certain information or data that is gleaned from the services that have been delivered, and the success rates of supporting achievement of individual

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

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

outcomes. However, the analysis should be done at a population trend level, and not include any identifying information in either the analysis, or the reporting, as a general rule. If there is a need to link information at an identifying level, the identifiers should be removed at an early stage in the process, and prior to the analysis being done, with the appropriate safeguards put in place.

The appropriate authorities to share the information even for the purposes of evaluation must be identified, and there may be legislative implications, depending on the legislation that applies. As such, the disclosure of that information may need to be specified in the consent, or somehow be linked to the authorized reasons for disclosure. Where multiple organizations are involved, that becomes more difficult, and there may be a need to rely on a specific member organization to conduct any evaluations, depending on the legislative requirements.[39]

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.

10.3. Using Data for Research

There is significant interest in accessing health and social data for research purposes. Organizations should determine in advance if they will be undertaking such use themselves, or entertaining external requests for data for research. If so, there are legislative provisions dealing with such use, and there may be additional procedures required.[40]

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.

[39] See Appendix A - Specific Legislative References, Note 23, Evaluation.
[40] See Appendix A - Specific Legislative References, Note 24, Research.

List of Jurisdiction Specific Appendices:

Appendix A: **Applicable Legislation**
Appendix B: **Ontario Privacy Legislation Disclosure Matrix**
Appendix C: **Disclosure Tool**
Appendix D: **Sample Collaborative Approach Training Resource**
Appendix E: **Sample Commitment Agreement**
Appendix F: **Sample Consent Forms**

List of Generally Applicable Appendices:

Appendix G: **Capacity Assessment Tool and Companion Guide**
Appendix H: **Guide to Using the Information Sharing Framework**
Appendix I: **Security Measures**
Appendix J: **Additional Resources**
Appendix K: **Sample Information Flow Table**

Prepared by: George Alvarez
on behalf of CONVERGE Mental Health

CONVERGE

Converge Mental Health | Changing The Mental Health Approach In Canada