Community Violence, Threat-making and Risk Assessment Protocol

A Collaborative Response to

Assessing Potential Violence, Threat-making, and Risk Behaviours

The Board of Education of School District 69 (Qualicum)
In Collaboration with Community Partners

SD69 QUALICUM

The Board of Education of School District 69 (Qualicum)
In Collaboration with Community Partners

Community Violence, Threat-making, and Risk Assessment Protocol:

A Collaborative Response to Violence, Threat-making, and Risk Behaviours

◆

The protocol reflects the work of J. Kevin Cameron, Director of the Canadian Centre for Violence Threat Risk Assessment and Trauma Response, the Yukon Violence Threat Risk Assessment Program (Y – TAP) and the Alberta Children and Youth Initiative.

We also thank the following school districts for sharing their resources in the development of this document:

- The North Okanagan – Shuswap Board of Education
- The Sooke Board of Education
- The Kawartha Pine Ride District School Board
- The Peterborough Victoria Northumberland and Clarington Catholic District School Board
- The Limestone District School Board
- The Surrey Board of Education

This document addresses student threat-making behavior. However, in certain circumstances, the process and/or resources outlines will be adapted and applied to situations with adult threat-makers. It is intended to be used with reference to Violence Threat/Risk Assessment Training Guide, Third Edition (2000) and Assessing Violence Potential: Protocol for Dealing with High-Risk Student Behaviours, Eighth Edition (2009)

Protocol Development Partners:

- Oceanside Collaborative Response Committee (OCRC)
- Board of Education of School District 69 (Qualicum)
- Oceanside R.C.M.P. Detachment
- Ministry of Children and Family Development
- Ministry of Child and Youth Mental Health
- Family Resource Association (FRA)
- Society of Organized Services (SOS)
- Island Health Community Nursing
- Island Health Discovery Youth & Family Substance Use Services
- Victim Services (R.C.M.P.)

School District 69 (Qualicum) Safe School Advisory Team (examples below):

- Assistant Superintendent, (Safe School Coordinator)
- District Principal, Alternate Programs
- Vice Principal
- Vice Principal
- Vice Principal
- Consultant

Community Violence, Threat-making, and Risk Assessment Protocol:

A Collaborative Response to
Violence, Threat-making, and Risk Behaviours

Table of Contents

Community Violence, Threat-making, and Risk Assessment Protocol:

A Collaborative Response to Violence, Threat-making, and Risk Behaviours

Rationale

The Board of Education of School District 69 (Qualicum) and its community partners are committed to making our schools safe for all students, staff and community members. As a result, we are collectively committed to responding to all student behaviours that pose a risk to self or other students, staff and members of the community. The term 'partner' in this document is not intended to mean a legal partnership, but rather a collaborative arrangement.

The Board of Education of School District 69 (Qualicum)
In Collaboration with Community Partners

Community Violence, Threat-making, and Risk Assessment Protocol:

A Collaborative Response to
Violence, Threat-making, and Risk Behaviours

◆

Memorandum of Understanding

The protocol has been developed through a process incorporating consultation and input from multiple departments, agencies, and groups. School District 69 and its community partners join together in demonstrating, by the signing of this document, that the safety of our students and staff is of utmost importance to all of us.

As partners, we agree that we will respond without delay to Violence, Threat-making, and Risk behaviours through the multi-disciplinary approach outlined in this protocol and supporting documentation.

Safe and Caring Schools: Community Violence, Threat-making, and Risk Assessment Protocol Signing Partners

Board Chair
Board of Education of School District 69
(Qualicum)

Superintendent of Schools
School District 69 (Qualicum)

Staff Sergeant
Oceanside Division
RCMP

Manager
Community Services
Ministry of Children and Family Development

Team Leader
Child and Youth Mental Health
Ministry of Children and Family Development

Manager
Child, Youth and Family Health
Island Health Authority

Executive Director
Society of Organized Services

Chair
District Parents' Advisory Committee

President
Mount Arrowsmith Teachers' Association

Signed this 3rd day of June, 2016

Protocol Summary:

Partners agreeing to this protocol share a vision of schools that are safe and caring. They accept the responsibility of using this protocol in response to threatening behavior and to plan the interventions necessary to prevent traumatic events in schools.

Partners agree to work together for the common goal of threat and risk reduction and school community safety by proactively sharing information, advice and support to assist in the prevention of traumatic events.

Partners work together for the benefit of children, youth and families by:

- building working relationships based on mutual respect and trust;
- working in ways that promote safe, caring and restorative school environments and practices;
- involving children, youth and their families in planning for services and supports;
- recognizing that each child and youth has unique strengths and needs that should be considered when developing an appropriate service plan;
- realizing that working together successfully is a process of learning, listening, and understanding one another; and
- being patient, trusting and working together to help children and youth become happy, healthy, active, involved, and caring members of the community.

The overriding goal is risk reduction and violence prevention to promote the safety of students, parents/guardians, staff and community members, the school or other buildings or property.

This protocol is designed to facilitate communication so when the Community Violence, Threat-making, and Risk Assessment Team (VTRA) is activated, appropriate community partners and School District 69 personnel may communicate relevant student information, develop a plan of support and obtain services in a timely manner. Partners will take additional actions they deem necessary to ensure safety regardless of the involvement of availability of other community partners.

The Board of Education of School District 69 (Qualicum) and its community partners will commit to ongoing participation and staff development in Violence, Threat-making, and Risk Assessment training and program review.

What is Violence, Threat-making, and Risk Assessment?

Violence, Threat-making, and Risk Assessment is a process of determining if a threat maker actually poses a risk to the target(s) being threatened. Behaviours that lead to Violence, Threat-making, and Risk Assessment include possession of weapons (including replicas), bomb threats, fire-setting, or threatening violence. Members of the School Safety Team are the first responders to determine "initial levels of concern". Members of the Violence, Threat-making, and Risk Assessment Team are engaged if serious risk appears to exist. All members respond after the immediate threat to student/staff/community safety has been contained. A comprehensive plan is developed.

Behaviours Addressed in This Protocol:

This protocol addresses ***Worrisome Behaviours, High Risk Behaviours,*** and ***Immediate Threats*** as defined in the Definitions (Please see Appendix M). These include, but are not limited to:

- serious violence or violence with an intent to harm or kill self or others
- verbal or written threats to harm or kill self or others
- internet threats to harm or kill self or others
- possession of weapons (including replicas)
- bomb threats (making and/or detonating explosive devices)
- fire setting
- sexual intimidation or assault
- gang-related intimidation and violence

Key Approaches in Violence, Threat-making, and Risk Assessment

1. **Sharing of Relevant Information**

   The sharing of information is carried-out by any of the partners on a proactive basis to avert or minimize imminent danger that affects the health and safety of any person (Please see Appendix F)

2. **Investigative Mind-Set**

   This is central to the successful application of the Violence, Threat-making, and Risk Assessment process.

   Violence, Threat-making, and Risk Assessment requires thoughtful probing, viewing information with health skepticism and paying attention to key points about pre-attack behaviours.

   Personnel who carry-out Violence, Threat-making, and Risk Assessment must strive to be both accurate and fair.

3. **Building Capacity**

   Violence, Threat-making, and Risk Assessment training will be provided to as many personnel and community members as possible.

4. **Program Review**

   The Safe School Coordinator will conduct an annual review of the Community Violence, Threat-making, and Risk Assessment Protocol.

   After each Stage II assessment, the Safe School Coordinator will ensure that a review for the individual situation is completed.

Activation Procedure

If there is a belief that danger is immediate or imminent CALL 911. The response can later be downscaled to high risk or worrisome behavior if necessary.

Immediate Threat
CALL 911. A call is made to the Superintendent or designate who informs the Safe School Coordinator who then contacts the Police Liaison Officer (Please see Appendix K). School/district/community partners will respond after the immediate threat to student/staff safety has been contained. The Community Violence, Threat-making, and Risk Assessment Team (VTRA) will assess whether a risk to student/staff safety exists and develop a comprehensive plan to support students involved, the greater student body, staff and community.

High Risk Behaviour/Threats
When the School Safety Team has determined that a student poses a medium to high level of concern to student/staff/community safety, the school principal contacts the Safe School Coordinator to go to Stage II. The Safe School Coordinator will activate the Community Violence, Threat-making, and Risk Assessment Team (VTRA) and will call lead representatives of community partners relevant to the specific threat situation. A process is undertaken to determine if a threat maker (i.e.: someone who utters, writes emails, etc. a threat to seriously harm a target or targets) actually poses a risk to the target(s) he/she has identified and a plan to address this situation is developed.

Worrisome Behaviour
A school principal activates Stage I: School Safety Team to address worrisome behavoiur(s) and he/she may request help from the District Principal – Alternate Programs or community partners during this process to determine if a person of concern may pose a risk to some unknown target or targets at some unknown period of time. Timelines are situational but, as a guideline, Stage I should be accomplished as quickly as possible, ideally during the first three hours and maximally 24 hours from the initial report. He/she will inform the School District 69 Safe Schools Coordinator regarding this investigation and the resulting plan.

Please see Appendix A

Four stages will take place:

Stage 1: Data collection and immediate risk reduction interventions are performed by the School Safety Team, which, at a minimum, includes the Principal, the Counsellor/Integration Support Teacher(s), and the Police Liaison Officer. The initial data collection is often accomplished in one to two hours. It focuses on gathering case specific data using the *Stage 1: School Violence Threat-making, and Risk Assessment Report* form. (Please see Appendix C). The principal is responsible for completing this form, sharing it as appropriate and maintaining a record. At this point it is determined whether or not a multidisciplinary crisis evaluation will be necessary (Stage II).

Stage II: Multidisciplinary crisis evaluation is focused on further data collection. The Community Violence, Threat-making, and Risk Assessment Team (VTRA) is assembled with community partners. The VTRA Team members work in collaboration with the School Safety Team to conduct the formal risk assessment and evaluation. Stage II includes the use of formal, structured professional instruments, concepts, tests and measure by the appropriate Community Violence, Threat-making, and Risk Assessment partner(s). From this a comprehensive multidisciplinary intervention and management strategy is developed. Stage II is documented using the *Stage II: Community Violence, Threat-making, and Risk Assessment Report* form (Please see Appendix D) and the Community *Violence, Threat-making, and Risk Assessment Intervention Planning Worksheet* (Please see Appendix E). The Community Violence, Threat-making, and Risk Assessment Team is responsible for completing these forms, sharing as appropriate and maintaining the record.

Stage III: Trauma response occurs after a traumatic event in conjunction with the School District 69 Critical Incident Response Team (CIRT). Community partners may be called upon to plan for and/or provide post trauma counseling and interventions for students and staff.

Stage IV: A review of Stages I to III will be held with the School Safety Team and the Community Violence, Threat-making, and Risk Assessment Team in order to make recommendations for improvements to the activation procedures using the *Stage IV: Community Violence, Threat-making, and Risk Assessment Debriefing and Feedback* form (Please see Appendix H).

It is important to note that once a *Violence, Threat-making, and Risk Assessment* has been completed for a student, the original document is to be filed at the school – with a note in the student file, and an entry in the Student Information system. As well, a copy of this document **must** be sent to the Superintendent or designate for their records.

Roles

School Principal or Designate

The School Principal or designate will:

- be the School Safety Team Leader
- call and coordinate the School Safety Team
- complete the *Stage I: School Violence, Threat-making, and Risk Assessment Report* (Please see Appendix C)
- contact the Safe School Coordinator to discuss possible activation of the VTRA Team after a student has been determined to pose a medium or high level of concern to other students, staff or community members
- follow up and coordinate intervention/management/plans developed by the team
- forward the School Safety Team documentation and intervention/management plan to the Safe School Coordinator
- participate with the Stage II VTRA Team when this step is initiated
- store the intervention/management plan securely
- participate in Violence, Threat-making, and Risk Assessment training

School Team: Counsellor/Integration Support Teacher/Behaviour Support/YFC/other staff who know the student

The School Team will:

- assist in data gathering as assigned by the principal
- assist the principal in completing the *Stage I: School Violence, Threat-making, and Risk Assessment Report* (Please see Appendix C)
- be available for consultation on general issues regarding Violence, Threat-making, and Risk Assessment procedures relating to mental health
- ensure that the student body is made aware about the signs of stress and anxiety and encourage students to report concerns to an adult
- assist in developing plans or other interventions (i.e.: behavior plan, safety plan) and in facilitating access to programs or resources
- respond to the student's educational needs if consent has been obtained
- help families obtain needed assistance
- as a member of the School Team, participate in Violence, Threat-making, and Risk Assessment training
- assist the VTRA Team in Stage II as necessary

Safe School Coordinator

The Safe School Coordinator will:

- be designated by the School District 69 Superintendent and CEO to lead the Safe School Advisory Team and the Violence, Threat-making, and Risk Assessment Team (Please see Appendix J)
- consult with the principal leading the School Safety Team
- contact community partner leads to move to Violence, Threat-making, and Risk Assessment Team status and invite relevant participants to the process

- facilitate the completion of the *Stage II: Community Violence, Threat-making, and Risk Assessment Report* (Please see Appendix D) and the Community *Violence, Threat-making, and Risk Assessment Planning Worksheet* (Please see Appendix E)
- follow up on recommended interventions/management plans including possible referral to an Education/Student Review
- participate in Violence, Threat-making, and Risk Assessment training
- supervise the Violence, Threat-making, and Risk Assessment review process and complete the Community *Violence, Threat-making, and Risk Assessment Debriefing and Feedback* form (Please see Appendix H)

Community Partner Staff

The Community Partner Staff will:

- have appropriate staff members participate in the VTRA Team as requested
- participate in a review of the School Safety Team findings
- participate in completion of the *Stage II: Community Violence, Threat-making, and Risk Assessment Report* (Please see Appendix D) and the Community *Violence, Threat-making, and Risk Assessment Planning Worksheet* (Please see Appendix E)
- facilitate timely community services that may be required by the threat maker(s) or the victim(s)
- participate in Violence, Threat-making, and Risk Assessment training

Police

The Police Officers will:

- participate in Stage I: School Safety Team Risk and Violence, Threat-making, and Risk Assessment Meetings and Stage II VTRA Team Meetings
- share any pertinent information and history with the team
- follow-up with a home visit, if needed
- determine whether a crime has been committed

Safe School Advisory Team

The Safe School Advisory Team members will:

- establish a Community Violence, Threat-making, and Risk Assessment protocol and review process with community partners and district personnel
- provide Violence, Threat-making, and Risk Assessment training
- provide training about the Community Violence, Threat-making, and Risk Assessment protocol
- oversee policy and implementation
- implement emergency response procedures

Communication:

1. **School District**

   The School District will be the lead partner in application of the Protocol. The Safe School Coordinator as appointed by the Superintendent of Schools will maintain an up-to-date list of the Community Violence, Threat-making, and Risk Assessment Partners and will distribute a copy of the list to all community partners. If the lead contact is not available, an alternative will be appointed and the community partners will be notified of their name and contact information.

2. **Community Partners**

   - To ensure the timely activation of a School District 69/Community VTRA Team, community partners will forward the lead contact name for their agency to the Safe School Coordinator in School District 69 (Qualicum). The names of changes in personnel will be forwarded without delay throughout the year (Please see Appendix K)
   - When a staff member of a community partner determines the need to activate the VTRA Team, they will notify his/her designated lead Community VTRA Team member who will contact the School District 69 Safe School Coordinator
   - Partners will at times take any actions seen as necessary to ensure immediate safety regardless of the involvement or availability of other community partners

3. **Meeting Space**

   Whenever possible, meetings will occur on the school premises. The lead partner will be the school board/school administration.

4. **Media**

   As part of the Violence, Threat-making, and Risk Assessment process, the Safe School Coordinator and the community partners involved in the assessment process may decide to develop a joint press release; however, the Superintendent of Schools is the media contact for all Violence, Threat-making, and Risk Assessments and manages media releases. In the case of criminal investigation, the police will be the lead regarding media releases. Whenever possible, media releases will be provided to affected community partners in advance of release to the media.

5. **Parents/Guardians**

   At the beginning of the school year, principals will distribute the *Fair Notice Letter* (Please see Appendix G) to all parents and guardians. This notification will also be posted permanently on the School District 69 website. The school-based administration will inform the school community about the outcome of a Violence, Threat-making, and Risk Assessment as necessary. Information from parents/guardians may assist the Violence, Threat-making, and Risk Assessment and development of an intervention plan. Without compromising safety, parental/guardian involvement in the intervention can be crucial to its success. At the same time, extended family and community support, particularly in our First Nations communities, can help with a positive outcome.

6. **School Staff**

Annually, the school principal will review the *Community Violence, Threat-making, and Risk Assessment Protocol* and its purpose with staff members and underscoring their duty to report. Staff members will participate in the School Safety Team and the collection of data. They will be advised about threats as appropriate by the school principal and informed as necessary about the results of a Violence, Threat-making, and Risk Assessment. The input and support of staff members is vital to the successful prevention of harm.

All school personnel, working in conjunction with the School Safety Team, will ensure that students are advised regarding signs of stress and anxiety and will encourage students to seek adult assistance when they observe or experience worrisome/risky behavior.

7. **Students/Parents**

Students should know that the Community Violence, Threat-making, and Risk Assessment Protocol protects them. The school principal will determine the appropriate way to engage students in developing an understanding of how the protocol accomplishes this. Notification will be sent home to all families each year as outlined in Appendix G - Fair Warning.

Occasionally, affected students and their parents will need to know the results of a Violence, Threat-making, and Risk Assessment.

8. **Intra-agency**

At the beginning of each school year, the Safe School Coordinator will send the *Fair Notice Letter* (Please see Appendix G) to community partners with a request to update the contact information. Internal communication regarding the protocol will be the responsibility of each partner to the protocol.

Occasionally, community agencies that were not involved in the Violence, Threat-making, and Risk Assessment training or are not one of the partners will need to know the results of an assessment.

9. **Information Sharing**

The general intent of access to information and protection of privacy legislation is to regulate the collection, use and disclosure of personal information. Wherever possible and reasonable, consent to disclose personal information should be obtained. The individual should know what he/she is consenting to, and understand the consequences of the intended disclosure. The individual must be made aware that he/she can withdraw consent at any time by giving written or verbal notice. However, in the case of threats, Violence, Threat-making, and Risk Assessment Teams are able to share information within the Freedom of Information Act and the Protection of Privacy Act and the Health Information Act. While protecting individual rights to privacy, the legislation:

- enables the sharing of necessary information about children and youth among service providers

- supports an integrated approach to service delivery by strengthening the ability to share information
- enables effective coordination of supports and services by service providers
- provides a foundation for the sharing of information among government ministries (Please see Appendix H)

10. Documentation

The Community Violence, Threat-making, and Risk Assessment Team records the proceedings of their meetings using the *Stage II: Community Violence, Threat-making, and Risk Assessment Form* (Please see Appendix D) and the *Community Violence, Threat-making, and Risk Assessment Intervention Planning Worksheet* (Please see Appendix E). The designated recorder will distribute completed copies of these documents to each team member, the Superintendent of Schools and the District Safe Schools Coordinator as soon as possible after the meeting. Team members ensure that this record stays confidential, each according to their agency's protocol.

During the Community Violence, Threat-making, and Risk Assessment meeting, the team schedules an appropriate time to reconvene and discuss the effectiveness of the intervention and complete the *Community Violence, Threat-making, and Risk Assessment Debriefing and Feedback Form* (Please see Appendix F). These forms may be used by the Steering Committee during their annual review to determine improvements in the protocol.

Community Violence, Threat-making, and Risk Assessment Protocol:

A Collaborative Response to
Violence, Threat-making and Risk Behaviours

Appendices

Appendix A:	Responding to Threats – A Guide
Appendix B:	Principal's Checklist for Immediate Threat/High Risk Behaviours
Appendix C:	Stage I: School Violence, Threat-making, and Risk Assessment Report
Appendix D:	Stage II: Community Violence, Threat-making, and Risk Assessment Report
Appendix E:	Community Violence, Threat-making, and Risk Assessment Intervention Planning Worksheet
Appendix: F:	Community Violence, Threat-making, and Risk Assessment Debriefing and Feedback Form
Appendix G:	Fair Notice Letter
Appendix H:	Communication and the Law
Appendix I:	Responding to Suicidal Risk in Students: A Staff Guide
Appendix J:	School District 69 Safety Program
Appendix K:	Community Violence, Threat-making, and Risk Assessment Contact Checklist
Appendix L:	Contact List
Appendix M:	Definitions
Appendix N:	Information Sharing in the Context of Child and Youth Mental Health and Substance Use in BC
Appendix O:	Privacy for Parents and Caregivers
Appendix P:	Information Sharing for Young People

Appendix A

Responding to Threats – A Guide

Any person who is concerned will CALL 911 in the event of an immediate threat.

High risk behaviours that may pose a risk/threat to others must be reported to the **SCHOOL PRINCIPAL/DESIGNATE** who will initiate Violence, Threat-making, and Risk Assessment Protocol

Immediate Threat **CALL 911**	**High Risk Behaviours**	**Worrisome Behaviours**
Included but not limited to: • weapon in possession that poses serious threat to others • plan for serious assault • homicidal/suicidal behavior that threatens safety • fire • violent intruder/assailant • specific bomb threat	*Included but not limited to:* • Possession of weapon/replica • bomb threat plan • verbal/written/internet threats to kill/injure (specific and plausible) • internet threats to kill or injure self/others • fire setting • threatens other acts of violence • increase of intensity and/or frequency of worrisome behaviour	*Included but not limited to violent content:* • drawing pictures • writing stories/journals • vague threatening statements • unusual interest in fire • significant change in child's baseline behaviour
⬇	⬇	⬇
Implement Emergency Preparedness Plan (School Safety Alert) • lockdown/lockout or evacuation • contact Superintendent/designate • refer media to Superintendent of Schools • Superintendent to inform Safe School Coordinator and police liaison	**Community Violence, Threat-making, and Risk Assessment Team (VTRA Team)** *Lead: School principal consults with **the VTRA Team** to develop a plan* • Principal will contact the Safe School Coordinator (Assistant Superintendent) to initiate VTRA Team • contact District Principal • access community partners as appropriate • complete Stage II: Community Violence, Threat-making, and Risk Assessment Report with intervention plan/course of action(s) • Send copy of VTRA to Assistant Superintendent	**In School Safety Team** *Lead: School principal consults with School Safety Team and staff to develop a plan and consider:* • determine level of threat using above framework • complete Stage I: School Violence, Threat-making, and Risk Assessment Report • consult District Principal as necessary • access VTRA Team community partners as necessary • Send copy of VTRA to Assistant Superintendent
⬇	⬇	⬇
Immediate Crisis Resolved • VTRA Team to meet, debrief, and support, possible CIRT • involve community partners • investigation and assessment/review • complete Stage I and II Violence, Threat-making, and Risk Assessment Reports with intervention plan/course of follow up action(s) • retain documentation in red file • Send copy of VTRA to Assistant Superintendent	**Case Management** • treatment and interventions • possible criminal charges • discipline as per District policy • monitoring through appropriate community partners • retain documentation in red file • VTRA Team review process	**Monitoring** • School based team review • community partner consultation as required • offer support and interventions as required • retain documentation and create red file as necessary

Appendix B

Principal's Checklist for Immediate Threat/High Risk Behaviours

Recognizing the every situation is unique and responses will vary

☐ **Step 1:** **CALL 911** if there is imminent danger

☐ **Step 2:** **School Principal/designate informed**

☐ **Step 3:** Ensure student safety: lockdown or evacuate if necessary

☐ **Step 4:** If immediate threat, call Superintendent or designate

☐ **Step 5:** In not an immediate threat, initiate Stage I protocol

☐ **Step 6:** To prevent use of weapons, do not allow access to desks, coats, backpacks, lockers or vehicles

☐ **Step 7:** Monitor and/or detain student(s) until the police arrive or as appropriate. Do not put yourself or others in harm's way

☐ **Step 8:** Determine if threat maker(s) has access to weapon(s)

☐ **Step 9:** Collect initial data from all participants in order to understand situation or circumstances

> *If possible and without compromising safety, parents/guardians or a child advocate should be present* for in-depth interviews. If a legal investigation is likely to occur, police/MCFD members should conduct these interviews.

☐ **Step 10:** Begin process of recording dates and times of calls/interviews

☐ **Step 11:** Notify the threat maker's parent(s) or guardian(s)

    ☐ Parent(s)/guardian(s) have been notified of the situation and this assessment

    ☐ Parent(s)/guardian(s) have not been notified because: ______________________

    ____

☐ **Step 12:** Notify the victim(s) parent(s) or guardian(s)

    ☐ Parent(s)/guardian(s) have been notified of the situation and this assessment

    ☐ Parent(s)/guardian(s) have not been notified because: ______________________

    ____

☐ **Step 13:** If necessary, move to Stage II

☐ **Step 14:** Contact Safe School Coordinator to initiate VTRA

☐ **Step 15:** Contact District Principal

☐ **Step 16:** Fax completed *Stage I: School Violence, Threat-making, and Risk Assessment Report* (Please see Appendix C) to Safe School Coordinator

☐ **Step 17:** Participate with VTRA Team to complete *Stage II: Community Violence, Threat-making, and Risk Assessment Report* (Please see Appendix D) with intervention plan/course of action

☐ **Step 18:** Send copy of VTRA to Assistant Superintendent

☐ **Step 19:** Retain documentation in red file

☐ **Step 20:** Participate in review process

Appendix C

Stage I: School Violence, Threat-making, and Risk Assessment Report

Convene the school team and discuss all relevant information regarding the student. Data may be obtained from multiple sources including former administration/support staff, teachers, and other school/district staff as well as students, targets, threat maker's parents/caregivers and others.

- Current and previous school/discipline records
- Law Enforcement, Probation, Diversion, etc.
- Parent interview: offer support, seek their help in understanding, clarifying interest in/access to weapons
- Searches of the student(s) lockers, backpacks, vehicles, etc.
- Searches of the student(s) bedroom, etc.
- Other agencies: mental health, social services, etc.
- Activities: internet histories, diaries, notebooks

As a team, ask the following questions, "To what extent does the student pose a threat to school/student safety? Does he/she pose a threat to themself or someone outside the school (i.e.: family)?

While maintaining the integrity of the process, Stage I should ideally be accomplished within the first three hours, and maximally twenty-four hours, from the initial threat.

Worrisome Behaviours

Risk to the target(s), students, staff and school safety is minimal.

Threat is vague and indirect.

- Information contained within the threat is inconsistent, implausible, or lacks detail; threat lacks realism
- Available information suggests that the person is unlikely to carry out the threat or become violent
- Typical baseline behavior

High Risk Behaviours

The threat could be carried out, although it may not appear realistic. Violent action is plausible.

- Threat is more plausible and concrete than low level threat. Wording in the threat and information gathered suggests that some thought has been given to how the threat will be carried out (i.e.: possible place and time)
- No clear indication that the student of concern has taken preparatory steps (i.e.: weapon seeking), although there may be ambiguous or inconclusive references pointing to that possibility. There may be a specific statement seeking to convey that the threat is empty (i.e.: "I'm serious!")
- Moderate or lingering concerns about the student's potential to act violently

Immediate Threat

The threat of situation of concern appears to pose an imminent and serious danger to the safety of others.

- Threat is specific and plausible. There is an identified target. Student has the capacity to act on the threat.
- Information suggests concrete steps have been taken toward acting on threat. For example, information indicates that the student has acquired or practiced with a weapon or has had a victim under surveillance
- Information suggests strong concern about the student's potential to act violently
- Significant increase in baseline behaviour

Violence, Threat-making Behaviours (Examples of high-risk behaviours addressed in this protocol include but are not limited to):

- Serious violence or violence with intent to harm or kill
- Verbal/written threats to kill others ("clear, direct, and plausible")
- Internet (Facebook, Youtube, etc.), text messaging, threats to kill others (refer to Appendix B of the National Training Protocol for abbreviations commonly used on the Internet and texting)
- Possession of weapons (including replicas)
- Bomb threats (making and/or detonating explosive devices)
- Fire Setting
- Sexual intimidation or assault
- Gang-related intimidation and violence

Three Primary Hypotheses in VTRA:

One: Is it a conscious or unconscious "Cry for Help"?
Two: Conspiracy of two or more! Who else knows about it? Who else is involved?
Three: Is there any evidence of fluidity?

Pre-interview Considerations

1. When possible, interview the Threat-maker(s) or Student of Concern **after** initial data has been collected such as locker check, interviewing the individual who reported the threat as well as the police member doing an occurrence check for prior police contacts. This will help to avoid the "uni"-dimensional assessment" and provide the interviewer(s) with data to develop case specific hypotheses and verbatim questions that can be asked in a strategic VTRA interview to test those hypotheses.
2. There should **never** be more than two people in the room interviewing the Threat-maker or Student of Concern.
3. Remember to distinguish between **Assessing the Threat** versus **Assessing the Threat-maker**.

Step 1:

School Administrators: make sure you know the whereabouts of the target(s) and threat-maker(s) and address any immediate risk factors if they exist.

- **If necessary, appropriately monitor and/or detain the student(s) of concern until the police member of the team is present.**
- **Do not allow "student(s) of interest" access to coats, backpacks, desks, or lockers.**
- **Determine if the threat-maker has immediate access to the means (knife, gun, etc.)**

Step 2:

School Administrators: If appropriate, check the locker, backpack, desk, etc.

Step 3:

Call the "trained" VTRA police member, share initial data and police will determine if a history of weapons possession, use, or violence is noted in police accessible records.

Step 4:

School Administrator will notify the Community VTRA Team contact of the Stage I Team activation.

<u>Step 5</u>:

Principal (Vice-principal), and VTRA Police member, in collaboration with the counseling member will determine who will strategically interview sources of data including all participants directly and indirectly involved as well as "hard" data collection as outlined below:

Immediate Data may be obtained from multiple sources including:

- **Reporter(s)**
- **Target(s)**
- **Witnesses**
- **Teachers and other school staff (secretaries, teacher assistants, bus drivers, etc.)**
- **Friends, classmates, acquaintances**
- **Parents/caregivers (Call both parents)**
- **Current and *previous* school records (call the sending school)**
- **Police record check**
- **Check the student(s) locker, desk, backpack, recent text books/assignments, binders, cars, etc for data consistent with the threat making or threat-related behavior**
- **Check/search or question parents/caregiver about the student(s) bedroom, etc.**
- **Activities: Internet histories, diaries, notebooks**
- **Other**

STAGE 1: School Violence, Threat-making, and Risk Assessment Report

School:		**Administration:**	
Name of Threat-maker:		**Date:**	
Relationship to School:			
Grade:	**DOB:**	**Age:**	**Designation:**
Parent(s)/Guardian(s):		**Contact:**	
Family Structure:			
Other agencies/doctors involved:			
Name of victim(s)/potential victim(s)/target(s):			
Name of Reporter(s):			

1. What was the specific threat? (detail language, weapons, etc.)

2. Where did it happen?

3. When did it happen?

4. Who was present and under what circumstances did the incident occur? (include cause/triggers)

5. Observations/information that would indicate intent to follow through:

6. What was the response of the target (if present) and others who were present at the time of the incident?

7. Was/were there:
   - Stated justification for the threat? ☐ Yes ☐ No ☐ Unknown
   - Means to carry out the threat? ☐ Yes ☐ No ☐ Unknown
   - Consequences weighted out? (i.e.: 'I don't care whether I live or die?') ☐ Yes ☐ No ☐ Unknown
   - Conditions that would lower the risk? (i.e.: 'Unless you take that Facebook post down, I will stick my knife in your throat.') ☐ Yes ☐ No ☐ Unknown
   - Others involved that may intentionally or unintentionally be contributing to the justification process? ☐ Yes ☐ No ☐ Unknown
     If yes, explain:
   - Attack related materials in their locker, backpack, etc. at school? ☐ Yes ☐ No ☐ Unknown
   - Attack related materials in their bedroom, shed, etc. at home? ☐ Yes ☐ No ☐ Unknown

NOTES:

8. Is there:
   - Recent change or escalation in mood and behaviours? ☐ Yes ☐ No ☐ Unknown
     If yes, please explain:
   - A history of depression or suicidal thinking/behavior? ☐ Yes ☐ No ☐ Unknown
   - A history of using illegal drugs or alcohol? ☐ Yes ☐ No ☐ Unknown
   - A peer who could assist with a plan or obtain weapons? ☐ Yes ☐ No ☐ Unknown
   - A healthy relationship with a mature adult? ☐ Yes ☐ No ☐ Unknown
   - An inordinate knowledge or interest in violent events including prior school-based attacks? ☐ Yes ☐ No ☐ Unknown
   - A history of expressed violent themes in their writings, drawings? ☐ Yes ☐ No ☐ Unknown
   - A different baseline of behavior than his/her peer group? ☐ Yes ☐ No ☐ Unknown
   - Demonstrated empathy with the feelings and experiences of others? ☐ Yes ☐ No ☐ Unknown

NOTES:

9. Describe how the incident ended and what happened to the threat-maker after the incident:

   Has the threat-maker:
   - Been seeking revenge for a perceived injury or grievance? ☐ Yes ☐ No ☐ Unknown
   - Attempted to gain access to weapons they have threatened to use? ☐ Yes ☐ No ☐ Unknown
   - Developed a plan? ☐ Yes ☐ No ☐ Unknown

- Sought out information consistent with the threat-related behavior? ☐ Yes ☐ No ☐ Unknown
- Sent communications containing ideas or intentions to attack a target currently or in the past? ☐ Yes ☐ No ☐ Unknown
- Been engaged in suspicious behavior such as unusual interest in alarm systems, video surveillance, etc? ☐ Yes ☐ No ☐ Unknown
- Engaged in rehearsal behaviours such as brandishing fake/real weapons? ☐ Yes ☐ No ☐ Unknown
- Forewarned others? (i.e.: 'Something is going to happen?' ☐ Yes ☐ No ☐ Unknown
- Had a history of violence/threats? ☐ Yes ☐ No ☐ Unknown

If yes, note target, frequency, intensity, recency: ______________________

NOTES:

10. Who is the threat-maker's peer structure and where does he/she fit? (i.e.: leader, follower)

____

Who is the target's peer structure and where does he/she fit? (i.e.: leader, follower)

____

11. What does the threat-maker "fill himself/herself" with (i.e.: fascination with prior school-based attacks, violent events, graphic games, inappropriate internet searches, etc.) and does it appear to influence his/her behavior?

____

12. Is there evidence of fluidity and/or religiosity?

____

13. Is there information to suggest that there is hopelessness, desperation and/or despair? (i.e.: a recent failure, loss, difficulty coping with stressful event(s), suicidal or ideation, etc.?)
Explain:

____

Summary Statement/consensus:

☐ Worrisome Behaviour ☐ High Risk Behaviour ☐ Immediate Threat

RECOMMENDATIONS:

A. ☐ Develop an intervention plan (Please see Appendix E)
B. ☐ Move to Stage II: Principal contact the Safe School Coordinator to initiate VTRA
C. ☐ Monitor and review situation by **Click here to enter a date.**
D. ☐ Other:

Date: ______________________

Completed by: ______________________

Team Members:

Appendix D

Stage II: Community Violence, Threat-making, and Risk Assessment Report

School:	**Administration:**
Name of Threat-maker:	**Date:**

☐ Stage I data collected from School Safety Team

☐ Data collected from community partners, parents, etc. (please specify source(s)

1. Supports in place:

2. Additional information required:

3. Does the threat-maker have the capacity to carry out an act of targeted violence (i.e.: organized thinking, access to a weapon, etc.)? Please specify:

4. Has the baseline behavior escalated?

5. Risk Level: ☐ Low ☐ Medium ☐ High

Recommendations:	To be implemented by:	Target completion date:
Recommendations:	To be implemented by:	Target completion date:
Recommendations:	To be implemented by:	Target completion date:

Date: ______________________________ Completed by: ______________________

Team Members (NAMES and ROLES):

Appendix E

Community Violence, Threat-making, and Risk Assessment Intervention Planning Worksheet

Attach additional pages as required

Name of Student: **Date:**

Based on the information considered during the Violence, Threat-making, and Risk Assessment, the consensus of this team is that overall, this threat is a:

☐ Worrisome Behaviour ☐ High Risk Behaviour ☐ Immediate Threat

Consult with threat-maker's parent(s)/guardian(s)	☐ Yes	☐ No	☐ Not at this time
Disciplinary action by the school	☐ Yes	☐ No	☐ Not at this time

Details:

Notify intended victim	☐ Yes	☐ No	☐ Not at this time
Notify intended victim's parent(s)/guardian(s)	☐ Yes	☐ No	☐ Not at this time
Hospitalization	☐ Yes	☐ No	☐ Not at this time

Details:

Continued assessment	☐ Yes	☐ No	☐ Not at this time

Details:

Suicide assessment initiated by:	☐ Yes	☐ No	☐ Not at this time

on (date)

Referral to a pediatrician/psychiatrist/psychologist	☐ Yes	☐ No	☐ Not at this time
Contract not to hurt self or others created (please attach)	☐ Yes	☐ No	☐ Not at this time
Staff alerted on a need-to-know basis	☐ Yes	No	☐ Not at this time
Daily check in with:	☐ Yes	No	☐ Not at this time

(name and title)

Weekly check in with:	☐ Yes	No	☐ Not at this time

(name and title)

Daily check out with:	☐ Yes	☐ No	☐ Not at this time

(name and title)

Weekly check out with: ☐ Yes ☐ No ☐ Not at this time

(name and title)

Backpack, coat, and other belonging check in and check out by: ☐ Yes ☐ No ☐ Not at this time

(name and title)

Late arrival and/or early dismissal times: ☐ Yes ☐ No ☐ Not at this time

Modify daily schedule by: ☐ Yes ☐ No ☐ Not at this time

Social/academic support ☐ Yes ☐ No ☐ Not at this time

Details:

Functional Behaviour Assessment/Behaviour Intervention Plan (attach a copy) ☐ Yes ☐ No ☐ Not at this time

Staff Safety Plan (attach a copy) ☐ Yes ☐ No ☐ Not at this time

Increased supervision in these settings: ☐ Yes ☐ No ☐ Not at this time

Drug and/or alcohol intervention ☐ Yes ☐ No ☐ Not at this time

Details:

If Special Education student, review IEP goals and placement options ☐ Yes ☐ No ☐ Not at this time

Review/recommend community based resources ☐ Yes ☐ No ☐ Not at this time

Details:

Conduct Integrated Case Management Meeting ☐ Yes ☐ No ☐ Not at this time

Other action (describe) ☐ Yes ☐ No ☐ Not at this time

Parent(s)/Guardian(s) – attach additional pages as required

☐ Parents will provide the following supervision and/or intervention:

☐ Parents will:

Monitor this Intervention Plan regularly and modify it as appropriate	
Violence, Threat-making and Risk Assessment Team members:	Signatures: Date:
Principal or Vice-principal:	Signature: Date:
Student Services Staff:	Signatures: Date:
Agency (i.e.: police):	Signatures: Date:
Other:	Signature: Date:
Other:	Signature: Date:

Review Date: ______________________________

Appendix F

Stage II: Community Violence, Threat-making, and Risk Assessment Debriefing and Feedback Form

Name of Threat- Maker: **Date:**

Date of Violence, Threat-making, and Risk Assessment:

Meeting Format (email, phone, etc.):

Participants:

Name:	______________________	**Role:**	Safe School Coordinator (Chair)
	______________________		______________________
	______________________		______________________
	______________________		______________________
	______________________		______________________

Part I: Debriefing the Threat

1. Has the intervention plan been successfully implemented?

____

2. What are the next steps?

____

Part II: Feedback on the Process

1. What aspect(s) of the Violence, Threat-making, and Risk Assessment worked well?

____

2. What should we change?

____

Appendix G

Fair Notice Letter

A copy of the following Fair Notice letter will be sent to parents/guardians of all students at the beginning of each school year, shared with community partners and posted on the District website.

SCHOOL DISTRICT No.69 (QUALICUM)

Dear Parents:

School District 69 (Qualicum) is committed to a safe and supportive environment for all. We take all threatening comments and behaviours seriously. Students, staff and parents should be aware of the Community Violence, Threat-making, and Risk Assessment Protocol that can be found on the District website and in all school main offices. Please take note of the following information.

What is a Threat: What behaviours warrant a Student Violence, Threat-making, and Risk Assessment to be initiated?

- A threat is an expression of intent to do harm or act out violently against someone of something
- A threat may be verbal, written, drawn, posted electronically, or made by gesture
- A threat may include any high-risk behavior such as possession of a weapon or replica weapon

What is Threat Assessment: Threat assessment is a process that is followed when a school becomes aware of a threat made against a student, staff member, or the safety of the school building and its occupants. When any form of threat is made, a threat assessment team will investigate and appropriately enact the Community Violence, Threat-making, and Risk Assessment Protocol. A threat assessment team is made up of individuals who have received formal threat assessment training. Each school has a multi-disciplinary Violence, Threat-making, and Risk Assessment team. The team may include the School Principal, Vice-principal, R.C.M.P., Ministry of Children and Families, Senior District staff, and others. It is important for all parties to engage in the Violence, Threat-making, and Risk Assessment process. If for some reason there is reluctance to participate in the process, by the threat-maker or parent/guardian, the threat assessment process will still continue in order to ensure a safe and caring learning environment for all.

What Parents and Students Need to Know:

- Any threat must be reported to the school administration, counselor or some other trusted adult
- Investigation may involve the police and/or other community agencies
- Investigation may involve locker or personal property searches
- Interviews will be held with the threat-maker and other students or adults who may have information about the threat
- Parents of students who are directly involved will be notified
- Threatening behavior may result in discipline for a student
- An intervention plan may be developed for the student making the threat and a support plan developed for any individuals targeted by threats

Everyone Has a Duty to Report: Often when we hear in the media about a violent incident, we learn that the threat-maker had made threats in advance of acting violently. To keep our school communities safe, students, parents, staff and community members must report all threat-related behaviours and high-risk activities. Every threat must be taken seriously, thoroughly investigated, and a response and follow-through completed.

Thank you for your attention to this matter.

Sincerely,
G. Wilson, Assistant Superintendent of Schools

Appendix H

Communication and the Law

Information Sharing

Violence Threat Risk Assessment Teams are able to share information within the Freedom of Information and Protection of Privacy Act and the Health Information Act. While protecting rights to privacy, this legislation:

- Enables the sharing of necessary information about children and youth among service providers
- Supports an integrated approach to service delivery by strengthening the ability to share information
- Enables effective coordination of supports and services by service providers

Green Light	Yellow Light	Red Light
Relevant personal information CAN be shared in these circumstances:	**Obtain more information and receive direction from a supervisor, consultant or lawyer in these circumstances:**	**Information can NEVER be shared in these circumstances:**
• With written consent • To avert or minimize imminent danger to the health and safety of any person • To report a child who might need protection under the Child, Family and Community Service Act (CFCSA) • By order of the Court • To facilitate the rehabilitation of a young person under the Youth Criminal Justice Act (YCJA) • To ensure the safety of students and/or staff • To cooperate with a police and/or child protection investigation	• Consent is not provided or is refused but there may be a health or safety issue for any individual or groups • To share YCJA information from records, where there is a demand or request to produce information for a legal proceeding • When a professional code of ethics may limit disclosure	• There is a legislative requirement barring disclosure • No consent is given and there is no need to know nor are there overriding health/safety concerns • Consent is given but there is no need to know nor are there overriding health/safety concerns

The ***Supreme Court of Canada*** has established legal precedent by ruling (in R. Vs. M (M.R.)) that in certain situations, the need to protect the greater student population supersedes the individual rights of the student. The ruling explicitly acknowledges that school officials must be able to act quickly and effectively to ensure the safety of the students and to prevent serious violations of the school rules. Two principles relevant to Violence Threat Risk Assessment protocols were established by the Supreme Court:

- The individual Charter Rights of the student are lessened to protect the collective need for safety and security of the general student population.
- School officials have greater flexibility to respond to ensure the safety of the general student population in an educational setting than law enforcement officials have in a public setting.

Therefore, if an individual is in possession of information that may indicate that there is an imminent danger to the health and safety of any person or persons and the source of the information is reliable, *the information can be shared without consent*. If information has been shared without consent the individual shall be advised with whom the information was shared.

Fair notice should be provided to youth and their parents/legal guardians that staff will respond to all information pertaining to threats in a professional manner to provide for a safe, healthy and caring environment while at school. Any direct threats or threat making behaviours will be assessed.

Sharing Youth Justice Information: Youth Criminal Justice Act

All sharing of youth justice information (i.e. relating to young persons aged 12-17 inclusive who are being dealt with under the criminal law or territorial offences) is subject to the non-disclosure provisions under ss. 119(2) of the Youth Criminal Justice Act.

Under ss.125(6), the Youth Criminal Justice Act enables information in a YCJA record to be shared with any professional or other person engaged in the supervision or care of a young person – including a representative of any school board or any other educational or training institution – for a range of reasons, including safety of staff, students or other persons. *Such sharing of information does not require the young person's consent.*

The recipient of youth justice information is responsible for ensuring compliance with legislated restrictions on its use and disposal under YCJA ss.126(7). This provision requires that the information must be kept separate from any other record of the young person, that no other person must have access to the information except as authorized under the YCJA or for the purposes of ss.125(6), and that it must be destroyed when it is no longer needed for the purpose for which is was disclosed.

Children's Act Records

Section 176(1) enables the Superintendent/Delegate to consent to the disclosure of records maintained under the Children's Act. There is no time period limiting this.

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA) provide exceptions for the release of information where there are imminent risks to health and safety. MFIPPA notes 'compelling circumstances affecting the health and safety of an individual...' (Part II, 32(h), MFIPPA). PHIPA notes that 'a health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.' (2004, c. 3, Sched. A, s. 40(1) PHIPA)

The Child and Family Services Act (RSO 1990, c.C.11, as amended) states there may be disclosure of information without consent 'if the service provider believes on reasonable grounds that, (i) failure to disclose the person's record is likely to cause the person or another person physical or emotional harm, and (ii) the need for disclosure is urgent." (CFSA 182, 1(e), (f)).

The Occupational Health and Safety Act (OHSA) S.32.0..5(3) states, "an employer's duty to provide information to a worker under clause 25(2)(a) and a supervisor's duty to advise a worker under clause 27(2)(a) include the duty to provide information, including personal information, related to risk of workplace violence from a person with a history of violent behaviour if, (a) the worker can be expected to encounter that person in the course of his or her work; and (b) the risk of workplace violence is likely to expose the worker to physical injury."

The Freedom of Information and Protection of Privacy Act (FOIPPA) (RSBC 1996, Chapter 165) recognizes the need to share information when it pertains to potential risks to health and safety. FOIPPA states that one must "consider all the relevant circumstances, including whether the disclosure is likely to promote public health and safety" (S.22 2(b)). The document continues to state "a disclosure of personal information is not an unreasonable invasion...if there are compelling circumstances affecting anyone's health or safety" (S.22 4(b)).

The Child, Family and Community Services Act (RSBC 1996, Chapter 46) specifically addresses the needs of the child through its statement that "a person must not disclose...except if the disclosure is necessary for a child's safety or for the safety of a person other than a child" (S.24 1(d)).

The Workers Compensation Act BC (RSBC 1996, Part 3, Division 3) states, "an employer must ensure that the employer's workers are made aware of all known or reasonably foreseeable health or safety hazards to which they are likely to be exposed by their work" (S.115 2(b)i).

Appendix I

Responding to Suicidal Risk in Students: A Staff Guide

Please DO the following:

- Remain calm
- Take the situation seriously
- Use language that supports disclosure
- Reinforce the need to involve others who can help
- Seek support from supervisor
- Remain with student
- Ensure the student is accompanied to the hospital by an adult; e.g. parent, police officer
- If escort is not parent/guardian, ensure parent/guardian is informed that student has gone to hospital
- Document the event afterwards
- Ensure student is with an adult at all times

Steps to take when:

Attempt: A student makes an attempt at school or returns to school having made an attempt

- Call 911
- Notify principal/designate
- Contact the parent/guardian immediately
- Ensure the student is accompanied to the hospital when it is safe to do so
- Consult with The Suicide Prevention/Crisis Line – Vancouver Island Crisis Society (telephone: 1-888-494-3888)

Disclosure: A student discloses recent suicidal thoughts/self-injury

- Call Child Youth Mental Health to request assistance (telephone: 250-954-4737 or 1-800-663-9122)
- Notify the principal/designate who may initiate Violence Threat Risk Assessment process
- Seek counselling services for the student to address risk and youth's reaction to having parent notified
- Notify the parent/guardian
- Contact 911 and request on-site assistance, when the safety of the student indicates this is necessary
- Ensure that an adult accompanies the student to hospital when safe to do so and parent/guardian is unavailable

Concern: A student's behaviour suggests suicidal risk, or concern is expressed for a student's safety

- Consult with your principal/supervisor who may initiate the Violence Threat Risk Assessment process
- Consult with counselling services
- Contact parent/guardian and/or student to discuss concern and develop a plan for support
- Call Child Youth Mental Health for consultation and recommendations (telephone: 250-954-4737 or 1-800-663-9122)

When contacting Child Youth Mental Health talk to personnel directly:
Do not leave a voice mail message

Appendix J

School District 69 (Qualicum) Safety Program

Safe School Advisory Team

- establish Community Violence, Threat-making, and Risk Assessment Protocol and review process with community and district
- provide Violence, Threat-making and Risk Assessment training
- provide Violence, Threat-making and Risk Assessment protocol training
- oversee policy and implementation
- implement emergency response procedrues

School Safety Team

- activate school level Critical Incident Reponse Team
- conduct school level threat assessment for worrisome behaviour
- establish anti-bulling programs
- implement policy administrative procedures
- review Codes of Conduct
- oversee programs such as restitution, restorative practices, Friends and Roots of Empathy

District Critical Incident Response Team

- initiate immediate onsite incident response
- manage pre and post incident response
- provide counselling
- establish community liaison
- initiate communication within school district and community
- identify access to supports

Community Violence, Threat-making, and Risk Assessment Team

- conduct threat assessments
- address high risk behaviours
- ensure thorough data collection
- communicate with community agencies

follow up with possible student or education review

Appendix K

Community Violence, Threat-making, and Risk Assessment Contact Checklist

A suggested script for principals, vice principals and community partners

Identify yourself: Confirm your name, role and school or agency

Identify the purpose of your call: I am activating the Violence Threat Risk Assessment Protocol. I am contacting you with serious concerns regarding an individual's potential imminent risk to harm self or others. I am collecting data to determine if the individual is engaging in behaviour consistent with the threat.

Explain the incident and make the case for information sharing:

The individual's name is ______________________________ Date of Birth ____________________

Describe the alleged incident and violence/threatening behaviours. Do they include:

- Serious violence or violence with intent to harm or kill
- Verbal/written threats to harm or kill others ('clear, direct, and plausible')
- Internet threats to harm or kill self or others
- Possession of weapons (including replicas)
- Bomb threats (making and/or detonating explosive devices)
- Fire setting
- Sexual intimidation or assault
- Gang related intimidation and violence
- Other

Outline what has been completed so far: interviews, record checks, police notification, locker and backpack check, parent contact, computer check, etc.

Ask

We feel that there is an imminent risk of harm to self or others. Is there anything that you could share at this time?
Can you please check to see if the individual is known to you?
Is or was the individual a client?
Please indicate if you have any information to disclose to us.
Please respond to this message by calling me back today on this number ____________________________

A suggested script for community partners when responding

Identify yourself: Confirm your name, role and agency

Respond to the enquiry

1. We have done a check of our files and we have nothing to report back to you; OR
2. We have done a check of our files and this is the information we feel is relevant to the situation and the individual in question; OR
3. Based on the information you shared with us earlier, we feel this situation is an indication of escalation towards violence because __________; OR
4. Please send a Release of Information request immediately so that I may fully share the contents of the file.

Appendix L

List of Contacts

Safe School Coordinator: Assistant Superintendent
Tel: 250-248-4241 Direct Line: 250-954-3078 Fax: 250-248-5767

ORGANIZATION	TEAM LEADER	OPERATIONAL CONTACT	CONTACT DETAILS

Appendix M

Definitions

Baseline – An individual's characteristic level of functioning from which one can assess changes in his/her behaviour or mood.

- **Affective baseline** – An individual's characteristic display of feelings, emotions, moods and temperament that can be used to assess his/her changes in behaviour or mood.
- **Cognitive baseline** – An individual's characteristic level of functioning in the processes involving sensing, perceiving, remembering and thinking that can be used to assess changes in behaviour or mood.
- **Individual/peer group baseline** – A characteristic level of behaviour by the individual and/or his peer group from which one can determine if there has been a change in typical behaviours (i.e., an increase in deviant behaviours such as drug or alcohol use, violence, gang related behaviours, isolation)

Behaviour Intervention Plan – A plan which outlines the supports and interventions required by a student having behaviour challenges. It would include but not be limited to: behaviour goals/skills, academic supports required, targeted skill development, replacement behaviours, reinforcers/consequences and progress monitoring

Community Violence, Threat-making, and Risk Assessment Team – A multi-agency team of professionals trained in Violence Threat Risk Assessment and in the use of this protocol.

Empty Vessel – Metaphor to describe the dramatic lack of connection that has existed between almost all school shooters and a healthy mature adult and their lack of clear identity, place and purpose. Their parental and other adult relationships have often been marked by extremes on a continuum from neglect to over-involvement: some experiencing both extremes at different times and other experiencing predominantly one or the other.

Fluidity – Changing back and forth between suicide ideation and homicidal ideation, and often with increasing rapidity as one becomes closer to a violent act.

Functional Behaviour Assessment – A process for determining how a student's behaviour is influenced and supported by conditions in the environment. It focuses on social affective, cognitive and/or environmental factors. Elements examined include setting events, triggering antecedents, the behaviour itself, maintaining consequences, functions and replacement behaviours.

High Risk Behaviours – Behaviours that express intent to do harm or act out violently against someone or something. High risk behaviours include but are not limited to: interest in violent content, unusual interest in fire/fire setting, and escalation of physical aggression, significant increase in anti-social behaviour, unusual interest in and/or possession of a weapon/replica of a weapon, bomb threat, and internet threat to kill or injure self and/or others. The School Safety Team should be activated and, after consultation with the Safe School Coordinator may lead to the activation of the Community Violence, Threat-making, and Risk Assessment Team.

Imitator/Innovator – Most school shooters attempt to look, act like or follow the example of a tormented character they identify with (i.e., copycat killers). In contrast, innovators make changes and introduce new methods of wreaking havoc on school populations.

Immediate Threat – In the case of immediate threat, staff will **CALL 911** and then contact the school principal/designate. The principal will contact the Superintendent of Schools or designate who will then activate the Community Violence, Threat-making, and Risk Assessment Team through the Safe School Coordinator.

Integrated Case Management Meeting – An interagency meeting with school and community partners, often including parents/guardians and/or the student, which is designed to support the safety and success of the student in the home, community and at school.

Justification Process – The process by which an individual rationalizes the purpose and intent of violence. This includes the fact, circumstance, or the grounds for action, defence or complaints the potential offender seeks, or is given the means to justify the intended violence.

Multi-System/Wraparound Plan – These plans involve home, school and usually community agency personnel. They are developed out of an integrated case management meeting.

Religiosity – The artificial or unnaturally heightened way an individual behaves or talks about his/her religious feelings.

Risk Assessment – A Risk Assessment is typically a lengthy process that involves a number of standardized tests and measures that go beyond the scope of the School Safety Team or Community Violence Threat Risk Assessment Team. A Risk Assessment determines if a student poses a risk to some known or unknown target(s) in some unknown period in time. Unlike the Violence, Threat-making, and Risk Assessment, the Risk Assessment is meant to be a comprehensive evaluation of all risk reducing (protective factors) and risk enhancing factors affecting the student's functioning and is used to guide longer term intervention and treatment goals. Community partners work with schools to access this specialized service.

Rule the Roost Mentality – Where parents have set few or no limits on the child's conduct and regularly give into his/her demands. The student insists on an inordinate degree of privacy, and parents have little information about his/her activities, school life, friends, or other relationships. The parents seem intimidated by their child. They may fear that he/she will attack them physically if they confront or frustrate him, or they may be unwilling to face an emotional outburst, or they may be afraid that upsetting the child will spark an emotional crisis.

School District 69 Safety Program – The overall program that addresses safety in Qualicum School District. (Please see Appendix J)

Safe School Advisory Team – A team of school administrators, including the District Principal, who work with the Safe School Coordinator to oversee the development of safe school policy and its' implementation.

Safe School Coordinator – The Safe School Coordinator is appointed by the Superintendent and CEO. He/She leads the Safe School Advisory Team and all safety initiatives in the School District including, but not limited to, the Critical Response Team and the Community Violence, Threat-making, and Risk Assessment Team.

School Safety Team – A team of school based professionals (i.e., principal, vice principal, student services personnel, police, etc.) who are trained to assess a threat to student safety by a student or group of students.

Staff Safety Plan – A safety plan is designed to offer safety for the people working with a child who can harm others.

Target Selection – Where victims of a crime are specifically targeted based on their personal identities (i.e., "*I know John and he is going to pay for what he did to me.*") or where the victims are non-specific (random) but associated with a general target for the perpetrator(s) (i.e., '*jocks*', females or the school staff).

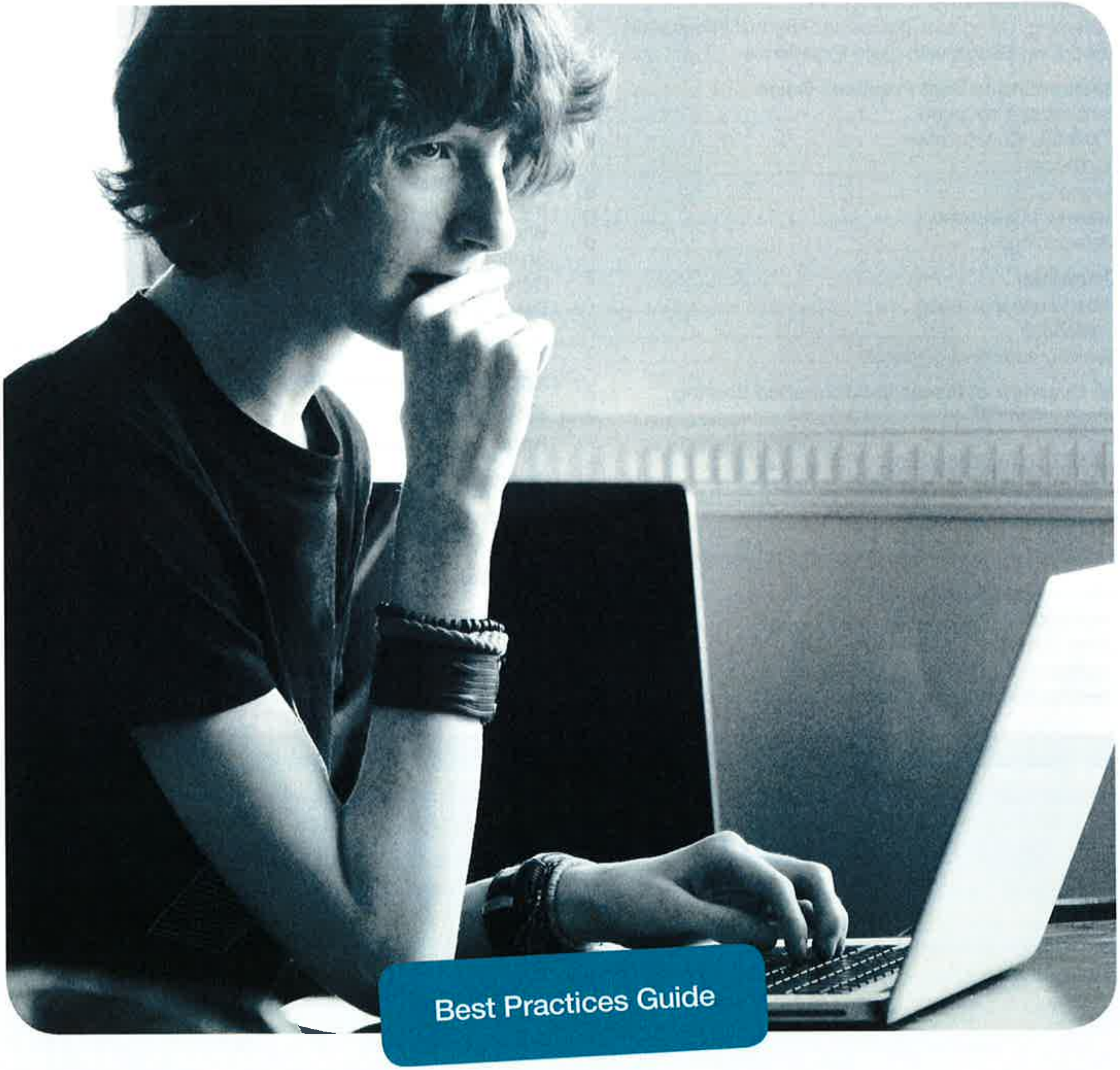
Threat – Defined as any expression of intent to do harm or act out violently against someone or something. Threats may be spoken, written, drawn, posted on the internet (MSN, Facebook) or made by gesture only. Threats may be direct, indirect, conditional or veiled.

Violence, Threat-making, and Risk Assessment – Violence, Threat-making, and Risk Assessment is the process of determining if a threat maker actually poses a risk to the target(s) being threatened. School Safety Teams and multi-agency Community Violence, Threat-making, and Risk Assessment teams collect information to determine the level of risk and to plan interventions.

Threat-Making Behaviours – Any action that an individual, who in any manner, knowingly utters, conveys or causes any person to receive a threat.

Worrisome Behaviour – Those behaviours which cause concern and may indicate that a student is moving toward a greater risk of violent behaviour. Worrisome behaviours include but are not limited to: drawing pictures that contain violence, stories/journal writings that contain violence, making vague/generalized statements about violence towards others that do not constitute a threat. Worrisome behaviours may be an early sign of the development of more serious high risk behaviours. All worrisome behaviours should be addressed. These situations may involve actions by the School Safety Team.

Information Sharing in the Context of Child and Youth Mental Health and Substance Use in BC



Best Practices Guide

Canadian Mental
Health Association
British Columbia
Mental health for all

BRITISH
COLUMBIA

Contents

Acknowledgments

Individuals with lived experience, family members, service providers, and leaders from across BC have provided valuable contributions to this report. The findings and guidance found in this report have been shaped by contributions from individuals from provincial government ministries, health authorities, school boards, community-based organizations, and clinicians in private practice. CMHA BC Division would like to thank families and youth with direct experience for their input on early findings of this work.

In particular CMHA BC Division wishes to thank the following people:

- Pamela Liversidge, Acting Director, Substance Use and Mental Health, Ministry of Health
- Patrick Egan, Senior Investigator, Office of the Information and Privacy Commissioner
- Monica Muller, Legal Counsel, Information Access, Vancouver Coastal Health

CMHA BC Division would also like to thank the Province of British Columbia who initiated and funded this work.

Note

Readers of this report will notice the emphasis upon the child and youth mental health and substance use (CYMHSU) system. Our rationale for producing a standalone child and youth mental health and substance use issues report and best practices guide is linked to the reality that the child/youth and adult mental health and substance use systems are so contrasting that they merit distinct consideration. Further, while there are elements within existing legislative frameworks that apply to children, youth, *and* adults, there are particular pieces of legislation (e.g. *Child, Family, and Community Service Act*) that have particular relevance for people under the age of 19. Once government feedback has been provided on this report, the structure and content will be adapted to account for the people and their family members interfacing with the adult mental health and substance use system.

Introduction

Context

An estimated 12.6% of youth in BC (aged 4–17 years) currently experience clinically-significant mental health problems—a total of about 84,000 youth.[i] The majority of mental health problems originate in childhood—a critical time for intervention and prevention to mitigate the risk of future illness.[ii] Youth with mental health and/or substance use challenges are often involved with multiple health care providers and in multiple healthcare systems.

Personal information about a person experiencing mental health and/or substance use problems is often needed by service providers to provide effective care and services. Care coordination can involve sharing personal information about individuals across organizations, ministries or providers. Increasingly, care providers are working in interdisciplinary teams across sectors and geographic areas. These factors make sharing information an important facet of effective health care provision and support.

Balancing service providers' needs for information with individuals' rights to privacy and confidentiality can involve making decisions that do not have clear-cut solutions. Most information-sharing situations require service providers to use their judgment and assess the context while interpreting the legislation or guidance documents. Often judgment occurs under time constraints. There is a clear need to improve information sharing strategies across organizations and agencies while remaining respectful of privacy and confidentiality.

In particular, children and youth have complex information sharing needs. Often family members or other caregivers need to share information with health care providers. Issues of consent can further complicate information-sharing scenarios. Clinicians, physicians, school counsellors and others who work in mental health and substance use (MHSU) services in BC are seeking a better understanding of what information can be shared under which circumstances.

This guide intends to function as a reference tool that service providers can use not only to comply with relevant legislation and policies, but also to feel empowered to share information appropriately in a timely way—across sectors and with family and families. Explicit guidance in this area, however, is difficult to provide. Information sharing in the area of MHSU is complex; service providers are governed by overarching privacy legislation, as well as policies and guidance documents at the regulatory college, organization and agency level. Information sharing decisions are rarely black and white, but require sound judgment, knowledge and understanding of the particular situation, context and individual.

Key Concepts

Privacy and Confidentiality

Privacy and confidentiality, although they are often used interchangeably, have different meanings.

Privacy relates to an individual.

For example, people may not want to be seen entering a place that might stigmatize them, such as a mental health centre that is clearly identified as such by signs on the front of the building. Privacy concerns people.

Examples of privacy-related situations include the following: the curtains are closed during physical examinations; health history or exam results are discussed in a private area, which may include asking an accompanying family member to leave the room temporarily.[iii]

Confidentiality relates to information or data about an individual.

For example, a counsellor's agreement with clients about how information shared during sessions will be handled, managed and shared.

Information sharing relates to sharing personal health information about an individual.

For example, information may be shared between service providers, individuals and families for the purpose of providing health care. Sometimes information sharing is called disclosure. Disclosure is showing, sending, sharing or giving personal information to another organization, agency or person.

Personal Information

Personal information is defined by the legislation as any identifiable information about an individual. This report defines personal information in the same way as legislation.

Personal information may include

- Name
- Age
- Marital status
- Employment history
- National/ethnic origin
- Political or religious beliefs
- Sex
- Contact information
- Address
- Personal opinions*
- Fingerprints
- Blood type
- Health insurance
- DNA information
- Biometrics
- An individual's health care providers
- Educational, financial and criminal history
- Health numbers (such as care card number)
- Information related to health care

*unless they are about someone else

Personal information does not include

- Business contact information, for example, an individual's title, business telephone number, business address, business email or facsimile number
- De-identified information
- Aggregate information, for example, general statistics, de-identified data used for program evaluation or quality improvement purposes or service-use data

Collecting, Using and Disclosing Personal Information

There are three main questions to consider when discussing information privacy:

1. How is personal information **collected?**
2. How is personal information **used?**
3. How is personal information **disclosed (shared)?**

How information can be collected, used and disclosed in BC is outlined in the legislation:

Legislation	***Freedom of Information and Protection of Privacy Act (FIPPA)***	***Personal Information Protection Act (PIPA)***
Who does it apply to?	Public bodies and their employees • School boards • Health authorities • Municipal police boards • Provincial government	Private sector • Businesses • Private organizations • Not-for-profit organizations • (Includes physicians in private practice)

Though *FIPPA* and *PIPA* are the primary Acts that address information sharing, other Acts, such as the *Child, Family and Community Service Act,* also include information about the collection, use and disclosure of personal information. Sections of several Acts are discussed in more fulsome detail in the Legislation section of the report and in the Appendices.

Describing People with Lived Experience

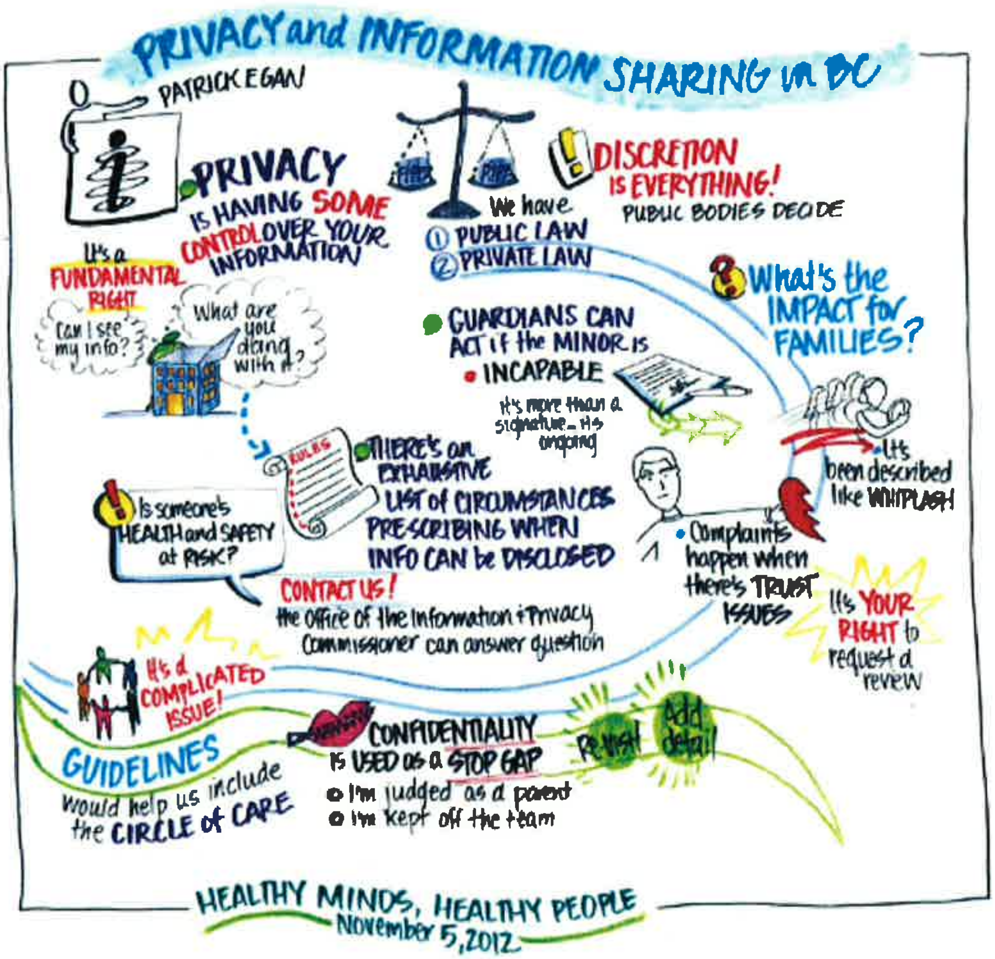
- **Individual, Person (or People) With Lived Experience:** This report uses the term individual to describe those who have lived experience with mental health and/or substance use problems. In this report, they are often those who are accessing mental health and/or substance use supports or who have accessed mental health and/or substance use supports in the past.
- **Family:** In this report, the term "family" encompasses the full range of relationships of importance to individuals, including significant others who provide support and/or care on a regular basis.
- **Service provider:** In this report, "service provider" means those who are providing mental health and/or substance use services, care, or other supports. They could be doctors, social workers, counsellors, school teachers and many others.

Background to Best Practices Guide

Families at the Centre

On November 5 and 6, 2012, a special gathering took place at the Morris J. Wosk Centre for Dialogue in Vancouver. Over 150 people—including family members, government representatives, service providers and educators—came together with a particular focus in mind: moving toward a more family-friendly mental health and substance use care system. The event convened as part of the Healthy Minds, Healthy People Knowledge Exchange Series, was designed to put the experiences of families front and centre.

During the panel discussion and audience participation, one main theme that arose from the discussion related to the experience of family members being excluded from a loved one's care[iv]. Information sharing and the related issues of privacy and confidentiality were subsequently identified as major areas for further exploration in moving towards more family-centered mental health and substance use care. The graphic below summarizes the main discussion points of the event as it related to privacy and information sharing in BC.



Following this event, the Ministry of Health commissioned CMHA BC to complete a research project with the objective of developing a set of helpful resources for individuals, their family members and service providers. The current phase of the project is focused on the development of (a) a synthesis of current issues and the available knowledge base into a resource for service providers and (b) resources for individuals and their family members. As noted previously, the emphasis of the first set of resources is the child and youth mental health and substance use system.

CYMHSU Collaborative

In parallel to the initiation of this project, the Child and Youth Mental Health and Substance Use (CYMHSU) Collaborative in BC was established in 2013. Using the Breakthrough Series Collaborative approach to quality improvement, the Collaborative has worked to bring community partners together to strengthen the child and youth mental health and substance use system at local, regional, and provincial levels.

The purpose of the Collaborative is to engage children, youth and their families, Aboriginal peoples, physicians, clinicians, provincial ministries, health authorities, schools, and communities to:

- Increase the number of children, youth and their families receiving timely access to integrated mental health and substance use services and supports throughout the province.
- Document examples and results of the involvement of children, youth and families in decisions related to program and system design, clinical practice and policy development, which manifest the 'family-first, people-centered' goals of *Healthy Minds, Healthy People.*

The CYMHSU Collaborative offers assistance and provides engagement and concept/tool testing to address information sharing barriers that sectors and providers face. The CYMHSU Collaborative is funded by the Shared Care Committee with a contribution from the Specialist Services Committee.

The Collaborative is mentioned in particular because privacy, confidentiality, and information sharing have emerged as priority issues amongst Collaborative participants. The Collaborative has been very assistive to this project by providing opportunities to engage participants around this document, helped create learning opportunities to test out key ideas in this resource, and has helped create momentum for knowledge, policy, and practice shift.

Audience

There are two primary audiences for this report.

1. **Front-line staff**—those who make decisions about disclosure and information sharing in their work to support children and youth with mental health and/or substance use issues. Front-line staff includes school counsellors and educators, clinicians and health care professionals, physicians, psychiatrists, counsellors, social workers, child protection workers, youth forensic psychiatrists and youth probation officers. Front-line staff may be primarily interested in information to help guide them in making disclosure decisions.
2. **Decision makers**—those who work in the provincial government as well as leadership in the areas of education, healthcare, social work, child protection, youth corrections, and other areas. Decision makers may be primarily interested in principle-based best practices, which could help shape future policies or systems-level change, as well as recommendations for future research.

Appropriate and effective information sharing can improve outcomes for both children/youth and their families. Although **individuals and families** are critical stakeholders, they are not a primary audience for this report. Instead, clear and concise information sheets are being developed to support those with lived experience and families in knowing their rights to information; understanding requests for information, disclosure of personal health information and consent; and finding other resources and information they may need. The youth and children and family information sheets are currently being developed and expected public release is early 2015.

Scope

The scope of this report is information sharing restricted to the context of child and youth mental health and substance use services in BC.

Specifically, this report will describe:

1. An overview of issues in information sharing
2. A discussion of information sharing in BC
3. The Traffic Light Tool: A guide for disclosure
4. Recommendations for information sharing

The report does not address the following related topics: freedom of information requests, technical and physical barriers to information sharing (e.g., electronic health records, firewalls), secondary use of data (e.g., research and quality improvement initiatives) and sharing information which is not defined as "personal information" (as in *FIPPA*, schedule 1 and *PIPPA*, s. 1).

Research Questions

This report aimed to answer the following research questions:

1. What are the **main issues** in information sharing, specifically in the area of mental health and substance use?
2. What are the **best practices** identified in the literature and other jurisdictions?
3. What are the **information needs** of individuals, families and services providers?
4. What **guidance** can be provided to help improve information sharing in BC?
5. How can legislation, policies and best practices **be interpreted** in a BC context?
6. What are some **recommendations** for future work in his area?

Methodology

To answer the research questions, a review of academic and grey literatures was conducted. The main focus of the literature review is on academic publications from 2000 to 2014 and grey literature, including reports and other publications, from the United States, the United Kingdom, Australia and New Zealand.

Stakeholders were directly engaged at various points throughout the research process. Stakeholders included individuals with lived experience, families, service providers, provincial government ministries and the Office of the Information Privacy Commissioner for British Columbia. These groups helped to identify current issues in information sharing in BC and, specifically, the information needs this report should address. Stakeholders also reviewed early drafts of the report and provided input on how to best create a practical and useful final product.

The next steps for this report are as follows:

- Content to be reviewed by government ministries, the Office of the Information Privacy Commissioner and/or the Officer of the Chief Information Officer, and others.
- Content to be finalized and approved for broader distribution and feedback.
- Content to be adapted to account for people and family members interfacing with the adult mental health and substance use system.
- Examination of application to diverse contexts, including Indigenous systems of care.
- Knowledge translation activities to be conducted to support services providers in implementing the principles and tools in this guide in their daily work.

Disclaimer

How to use this report

This report is for general information only. It is not intended to take the place of legal advice or legislation, policies, procedures and other formal standards. It is intended to be used as a tool for education and discussion only. The Canadian Mental Health Association, BC Division and the BC Ministry of Health accept no responsibility for the use of this material.

Limitations

This report is limited as it applies only to BC legislation, which differs from other provinces and countries. Guidance from other jurisdictions may not be of relevance in BC. Additionally, best practice in information sharing—especially in healthcare—is constantly shifting.

Given the breadth of service provider roles and areas in the scope of this guide, it is not possible to provide a comprehensive list of information sharing scenarios with specific guidance for each scenario. Disclosure decisions require professional judgment and consideration of the unique factors in each situation; therefore, absolute rules about disclosure are not provided in this report.

Best practices for a particular field or scope of practice should be documented at the local level in local or organizational practice documents and protocols.

Seeking additional guidance

Service providers are advised to contact their local privacy office, privacy officer, or other organizational advisor for further guidance on interpreting legislation and local policy or protocols. In particular, **public bodies** (such school boards, health authorities and provincial government ministries) should have an office or individual who can provide guidance on *FIPPA*'s requirements.

Businesses and **non-profit** organizations should have an appointed privacy officer who can provide guidance on *PIPA*'s requirements.

The Office of the Chief Information Officer also operates a Privacy Helpline that provides support, direction and training on *PIPA*'s requirements to the public and private sector organizations including businesses, private organizations and not-for-profits.

Phone: 250-356-1851
Email: Privacy.Helpline@gov.bc.ca

An Overview of Issues in Information Sharing

Introduction

The purpose of this overview is to provide a summary of issues in information sharing from the academic and grey literature, incorporating information gathered from consultations with identified stakeholders. This section discusses the benefits of sharing information and the known barriers to effective information sharing that are within the scope of the report. It will also explore evidence of the importance of involving families and of sharing information among service providers in order to achieve collaborative care and better outcomes for individuals.

The Benefits of Appropriate Information Sharing

Appropriate information sharing can improve outcomes for both children/youth and their families[v]. Effective information sharing promotes continuity of care, safety and quality. It helps families provide more appropriate, timely care and better services. We examine some of the ways appropriate information sharing, when balanced with an individual's right to privacy, can help with the provision of integrated and coordinated care, with family member inclusion.

Better Care and Services

Appropriate information sharing is critical for enhancing continuity of care, especially in the BC child and youth mental health and substance use system. In this system, services are rarely fully integrated. Individuals access services from a variety of organizations over the course of their health care journey (e.g., Health Authorities, family physicians and the Ministry of Children and Family Development (MCFD).) Service providers can also use information sharing to promote safety on behalf of the individual and their family, themselves and other providers and, very rarely, the public.

Better Relationships with Individuals and their Families

Sharing information helps service providers provide more efficient, effective services to individuals. Without adequate information, providers may waste time duplicating efforts or risk breaking individuals' trust. Individuals may question, *"Why are you asking me this again?"* and have to tell their story multiple times.

Information sharing supports service providers in providing care. They can better identify appropriate services, conduct needs assessments and provide appropriate and responsive services. Additionally, it helps providers engage with families and other service providers to monitor and support treatment and more rapidly identify relapse and the need for intervention.[vi]

Information sharing can be of benefit to families in reducing their stress and isolation and can help providers support the relationship between individuals and their families.[vii] Information sharing is necessary for the following:

- Providing seamless, wrap-around care and integrated services[viii]
- Reducing duplication
- Ensuring information that is collected is complete and accurate
- Providing a complete understanding to guide other service providers and families in supporting and caring for individuals
- Avoiding adverse events[ix]

Building Trusting Relationships

Ideally, individuals can trust that service providers will keep their information confidential, service providers can trust that their colleagues will share important information when necessary (e.g., when there are safety concerns) and families can trust that they have the information they need to support and care for their loved ones. Additionally, individuals with lived experience are less likely to share all relevant information with service providers if they lack trust in them.[x] Trust is critical in the provision of quality care.

Information Sharing Among Service Providers

BC health systems, in alignment with other jurisdictions, are moving toward collaborative care models and providing service in interdisciplinary teams.[xi] Studies show that interventions from integrated primary care and mental health and substance use teams result in better outcomes for individuals and decrease the need for emergency and hospital services[xii]. Due to the nature of the child and youth mental health and substance use system in BC, information is shared across multiple transition points and among multiple providers. Information sharing among service providers is important within an integrated system, but for reasons we explore later in this report, providers generally tend to err on the side of caution and under-share information with each other.

In Ontario, the policy framework for child and youth mental health describes child and youth mental health as a "shared responsibility".[xiii] This is especially important when working with children and youth, who may have multiple people responsible for their care. Describing youth mental health as a "shared responsibility" may help foster collaboration among those who care for youth, including health care and service providers, families, communities, governments and other public sector agents.[xiv]

It is also important to remember the schools are important settings for child and youth mental health, not only because they provide mental health promotion and prevention, but also because they provide pathways to service for children and youth. Most mental illnesses first emerge in schools, and first symptoms provide critical opportunities for early identification and intervention[xv].

Schools are part of a family-centered approach to care for many important reasons, including:

- Teachers, principals, and school counsellors spend significant amounts of time with students and know them well.
- Schools can connect students with resources and support them.
- School is a setting for promoting positive mental health, focusing on early identification and intervention.

Information Sharing with Families

Sharing basic information can help improve outcomes for both families and individuals and has been shown to decrease the frequency of relapse.[xvi] Families are particularly important individuals in the care and treatment of children and youth with mental health or substance use challenges.

Some jurisdictions have taken the approach of explicitly outlining information sharing with families in legislation. As far back as the late 1990s, some states in the US had statutes in place that permitted sharing information with families without individuals' consent if it had been verified that the families were directly involved in care or monitoring treatment and the information disclosed was necessary for this purpose.[xvii] In the UK, 'carers' have rights to information enshrined in legislation. Currently, privacy law in BC does not specifically mention families.

Families often have an in-depth knowledge of the individual receiving care, can be a source of constant long-term support for the individual and may be able to provide support if a crisis does not occur during regular office hours.[xviii] Individuals can benefit from family who recognize signs of relapse, encourage them to seek help, know how to support them, can connect directly with their physician, psychiatrist or service providers.[xix] Families often need to know treatment goals, signs and symptoms, potential effects of medication, dose, and other information to be able to provide care for their loved ones.

Families also require information for their own mental and physical well-being.[xx] Gathering information from families with permission from the individual is especially important when the individual is unable to provide information about their illness on their own. Symptoms of mental illness, including withdrawal, confusion and isolation, can make involving the individual's family even more crucial.[xxi]

Recent research shows that, in general, families accept an individual's right to withhold consent, but acknowledge the impact that lacking information can have on the standard of care they provide. Families recognize how important information that is relevant to their support role is, but feel they do not need or want to know everything about the person they are supporting.[xxii]

Despite this understanding, providers tend to under-share information with families. Questions about information sharing with families are complex. How and when should service providers share information? What information is necessary to share? What do they do if the individual does not consent to sharing information?

From our scan of policies and guidance documents, there seems to be little available in B.C. to answer these questions. We note that this may be shifting—for example, Vancouver Coastal Health (VCH) has recently taken a new approach to family involvement in mental health and addiction services[xxiii] and implemented a new policy on this issue. They describe family involvement as a vital component in the recovery framework.[xxiv] This document is responding to an identified gap in the resource base.

Barriers to Information Sharing

Barriers to appropriate information sharing is a cross jurisdictional issue. We have learned about barriers to information sharing from documented challenges faced in other jurisdictions and sectors. For example, challenges in sharing information between health and social services in the UK[xxv] have been linked to professional culture, physical and systems barriers and lack of information.

We can also learn about barriers to information sharing from areas outside of child and youth mental health and substance use services. In particular, a 2012 project to develop an Information Sharing Strategy led by the Alberta Ministry of Human Services identifies several key barriers.[xxvi] The work in Alberta was initiated to improve information sharing within government and services agencies in the areas of health, education and safety of children and families.

The following lists of barriers to information sharing are documented examples of barriers that are faced by service providers and front-line staff in their daily work. These barriers can be real or perceived. They can be legal and technical in nature. They involve professional culture, systems-level issues and general information-sharing issues.

Professional Cultural Barriers

- A lack of trust among professions[xxvii]
- Service providers tend to be over-cautious due to concerns for patient confidentiality; this can occur on both an intra- or inter-agency level[xxviii]
- Differences between professional cultures[xxix]
- Cultural differences between professionals, e.g., among nurses and physicians and community-based mental health service providers
- Differences between professional ideologies, e.g., the medical model focuses on the patient and the social work model focuses on the individual and their community/networks/families[xxx]
- A lack of role clarity
- A lack of confidence[xxxi]
- An emphasis on the importance of privacy for individuals with lived experience
- Diversity and cultural differences between the individual and their family and service providers[xxxii]

Information Barriers

- A lack of clarity in the information provided
- Systems Barriers
- Firewalls between ministries, health authorities, and between structures within the same jurisdiction
- Issues with integrating electronic medical records
- System complexities
- A lack of time or resources for providers to fully involve families or family[xxxiii]
- Strict and inconsistent professional codes of conduct

After recently engaging with hundreds of participants from government ministries, community service agencies, school boards, Alberta Health Services, Child and Family Services Authorities and many others, researchers found the following barriers and success factors to be of importance[xxxiv]:

Barriers

- Multiple consent forms and different procedures and policies
- Rules not widely shared or not easy to understand
- Inconsistent application of relevant legislation
- Lack of clarity using 'sensitive information'
- Fear of reprisal when making decisions to share information
- Lack of consistent training for all levels

The researchers also found that the barriers contributed to unintended consequences, such as less effective treatment outcomes/service delivery and duplication of efforts by each agency, resulting in higher administrative and resource costs.[xxxv]

Success Factors

- Strong relationships—trust needs to be in place to promote the development of interpersonal and inter-organizational trust
- Clear, simple, agreed upon procedures and policies need to be developed and implemented with clear standards for consent and information sharing
- Understanding the mandates and goals of partnering organizations and having respect for differences in organizational business practices
- Support for culture change
- Individual-focused information sharing and appropriate, individual-centric risk assessment and management
- Consistent application of legislation
- Need for on-going oversight, through some form of advisory team, to ensure consistent acceptance and application of the new approach to information sharing
- Consistent training that is ongoing and mandatory for all levels
- Information sharing between government departments at all levels and with partners in a way that supports staff and individuals with lived experience

Individuals' Information-Sharing Preferences

Recent research finds that individuals' preferences about information sharing depend on the type of information being shared, who the information is being shared with and what role the individual receiving the information plays in the care or treatment of the individual with lived experience.[xxxvi] Research also shows that the requirement for consent is linked to an individual's self-esteem, personal choice, independence, autonomy, general wellbeing and empowerment.[xxxvii]

Though there are few studies on individuals with lived experience and their perspectives on information sharing, a recent study of individuals with lived experience in New Zealand revealed that the majority felt they had incomplete or insufficient information about how their personal health information would be shared.[xxxviii] They were generally comfortable with information sharing among clinical staff, but less comfortable with information sharing for secondary purposes.[xxxix]

Unlike in some areas of the United States,[xl] individuals in Canada generally do not have full copies of their health records. People in Canada do not have the ability to bring their information to appointments and share it as they wish. Thus, learning about and documenting information sharing preferences may be even more critical in jurisdictions like BC, where individuals do not generally have access to their full and up-to-date records without making a formal request.

Information Sharing in BC

This section will provide an overview of legislation in BC as it relates to making information sharing decisions. This section is primarily written for service providers who make disclosure decisions in their daily work.

Legislation

The first step in making a decision about disclosure is to determine which legislation applies. Any time a disclosure of personal information occurs, it must be authorized by legislation. In BC, the relevant legislation depends on the organization you work for.[1]

This guide will primarily discuss the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Personal Information Protection Act (PIPA)*. These Acts provide general legal guidance with regards to information sharing; however, the Acts are flexible frameworks, and they provide room for open information sharing. Although some direction is provided in "must/must not" terms, the majority of the relevant legislation uses the verb "may" and therefore relies on service provider judgment. Within this framework, the individual's preferences should always be respected to the greatest extent possible.[xli]

FIPPA applies to all records in the custody or under the control of **public bodies** (*FIPPA*, s. 3(1)) in BC. Public bodies (*FIPPA*, schedule 1) include school boards, health authorities, municipal police boards (e.g., the Vancouver

---

[1] The federal government and its employees are governed by the federal Privacy Act, which is not discussed in this guide.

Police Department), the provincial government and its ministries, including the Ministry of Children and Family Development. *FIPPA* also applies to services providers contracted by or providing services on behalf of a public body. If an organization is not sure if they are a service provider they should ask the public body they contracted with.

PIPA applies to the **private sector**, including businesses and private or not-for-profit organizations (*PIPPA*, s. 3), including physicians in private practice and not-for-profit service providers, such as the Canadian Mental Health Association (CMHA) branches.

Other Guidance Documents

In addition to *FIPPA* and *PIPA,* you will need to be familiar with the policies and procedures of your organization, codes of ethics and college/professional association standards. These policies and standards should already be compliant with relevant legislation—including *FIPPA* or *PIPA*—and will provide guidance for interpreting and applying legislation in you role, organization or profession.

Legislation and Policies vs. Practice

During the consultation process for this guide, service providers acknowledged a discrepancy between information sharing that is authorized by legislation, organizational policies or other formal guidance documents and information sharing that occurs in practice. Often physical or practical barriers to information sharing, such as firewalls or paper copes of records, prevent the sharing of information even when authorized by law.

This report acknowledges that in addition to legislative and formal barriers, there are practical and informal barriers to information sharing, which must be addressed. As previously discussed, local organizational culture, local knowledge and practice play a significant role in when, how and how much information is shared.

Seeking Additional Guidance

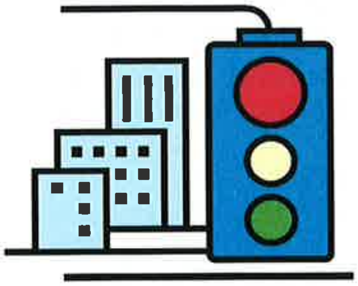
For information on seeking appropriate guidance on disclosure decisions, please see the Disclaimer: Seeking Additional Guidance.

In addition, Appendix 1 provides some useful links for BC privacy legislation, tools and websites.

Requests for Information

Under both *PIPA* and *FIPPA*, individuals have a right to request information about themselves. Unless the information falls under the legislated exceptions outlined in *FIPPA* and *PIPA*, information must be disclosed within the prescribed time limits and applicants have a right to file an appeal or complaint with the Office of the Information and Privacy Commissioner of BC if they are not satisfied with the response. Further information about requests for personal information from individuals and the request and review process are not discussed in detail in this guide.

The Traffic Light Tool: A Guide for Disclosure



The traffic light tool helps summarize some of the key sections of *FIPPA* and *PIPA* that provide guidance on when information **must** be disclosed ('green light'); when it **may** be disclosed ('yellow light'); and when it generally **may not** be disclosed ('red light').

The disclaimer on the previous page applies to this whole guide, but particularly this tool. This guide is not legal advice. Always refer back to legislation and policies in your area. This guide is not a comprehensive summary of all sections of *FIPPA* and *PIPA.*

Using this Guide

To use the traffic light tool, first check if the disclosure in question meets the requirements under mandatory or required disclosures (a **must** disclose situation). If not, check if the disclosure in question meets the requirements of one of the authorized disclosures in *FIPPA* or *PIPA*, as applicable. If the disclosure is not authorized by a section of *FIPPA* or *PIPA*, then the individual's consent is required.

Relevant sections of *FIPPA:*

- **Section 32:** Use of personal information
- **Sections 33 to 36:** Disclosure of personal information
- **Sections 4 to 25:** Disclosure for Freedom of Information requests (e.g., if an individual requests their own personal information)

Relevant sections of *PIPA:*

- **Sections 17 to 22:** Disclosure of personal information
- **Section 23:** Access to information (when an individual requests their own information)

Traffic Lights

Green light

Must disclose

The tables in Appendix 2 and Appendix 3 outline some common scenarios in which information **must** be shared. They also describe which legislation mandates disclosure. Additionally, the tables include information about the agency that would require the information, their authority and the required proof of authority for disclosure.

FIPPA mandates that information must be disclosed when it pertains to a risk of significant harm to the environment or to the health or safety of a group of people or the public. When disclosure is clearly in the public interest, it must be disclosed (*FIPPA*, s. 25 (1)). This section of *FIPPA* has been interpreted with a high legal threshold: in other words, "there must be an urgent and compelling need for compulsory public disclosure."[xiii] If this section is used, it must also be reported to the person the information is about and the Information and Privacy Commissioner for BC (*FIPPA*, s. 25 (3) and s. 25 (4)).

Disclosure under this section does not require consent; however, this section is used very rarely due to the high threshold required.

Example must disclosures include:

- When there is a suspicion that a child is in need of protection;
- When there is a risk of harm

Anyone with reason to believe a child is being abused or neglected—or is at risk for abuse or neglect—where the parent is unwilling or unable to protect them, has a legal duty to report that concern to a child welfare worker in MCFD or to a Delegated Aboriginal Agency child welfare worker. The duty to report is defined in the *Child, Family and Community Service Act* and explained in *The BC Handbook for Action on Child Abuse and Neglect: For Service Providers* www.mcf.gov.bc.ca/child_protection/pdf/handbook_action_child_abuse.pdf

Yellow light

May disclose

Under *FIPPA* and *PIPA*, information **may** be shared with an individual's consent and for the purposes for which it was collected (i.e., to provide services or care). Both *FIPPA* and *PIPA* outline the requirements for obtaining an individual's consent. Both *FIPPA* and *PIPA* also outline situations in which information may be disclosed without an individual's consent.

If personal information was lawfully collected, **consent is not required to use or disclose it for the same purpose for which it was collected.** This applies to both *FIPPA* (see 32(a) and 33.2(a)) and *PIPA* (see 14(a) and 17(a)).

Consent

FIPPA

May disclose personal information with the consent of the individual if the information is about (s. 33.1 (1) (b))

Consent is required if disclosure is not authorized by a section of *FIPPA* (33.1 and 33.2)[2]

PIPA

Only allows for disclosure of personal information if the disclosure is permitted by the Act (examples are outlined below), or with consent (s. 6(1) and 6(2))

Sections 6 to 9 outline requirements for consent, including when it's required, how it's provided, types of consent, and withdrawal.

---

[2] Legislation relating to consent is not described in full here. For individual who cannot consent (e.g., is a minor, seriously ill or mentally incapacitated) consent may be required from a legal representative (e.g., legal guardian or a person having a power of attorney).

Examples of Authorized Disclosures[3]

FIPPA

Under s. 33.2 (a), may disclose personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose.

This has been interpreted to mean that information for continuity of care purposes on a 'need to know' basis. (Disclosure must meet the necessary test under s. 33.1(1)(e) and (e.1).) Further guidance on this is not provided in the legislation, but is based on case law and best practice. Interpretation and service provider judgement is required.

In summary, a public body may only use personal information:

1. for the purpose for which it was obtained or compiled, or for a consistent purpose. A consistent purpose has a reasonable connection to the original purpose, and is necessary to perform the duties of or operating a legally authorized program, of the public body;
2. if the individual has consented to the use; or
3. for the purpose for which the personal information has been disclosed to it under *FIPPA*.

PIPA

PIPA uses a "reasonable person" test, which means disclosure of information is authorized only for purposes that a reasonable person would consider are appropriate in the circumstances, and that fulfill the purposes for which information was collected (s. 17)

This is true despite consent. In other words, consent is not valid if the individual is convinced to consent to an unreasonable disclosure.

Authorized Disclosures Related to Health and Safety Concerns

FIPPA

Under s. 33.1 (1) (f), may disclose personal information to an officer or employee of a public body or to a minister, if the information is necessary for the protection of the health of safety of those individuals.

Under s. 33.1 (1) (m), the public body may disclose personal information if:

- The head of the public body determines that compelling circumstances exist that affect anyone's health or safety, and
- Notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that giving this notice could harm someone's health or safety;

Two examples include:

- May disclose personal information the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur. (s. 33.1 (1) (m.1))
- May disclose personal information so that the next of kin or a friend of an injured, ill or deceased individual may be contacted (s. 33.1 (1) (n))

PIPA

Section 18 of *PIPA* outlines when organizations may disclose personal information without the consent of the individual. Some examples of situations under s. 18 (1) include:

- The disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way. (s. 18 (1) (a))
- The disclosure is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent (s. 18 (1) (b))
- There are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates. (s. 18 (1) (k))
- The disclosure is for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual (s. 18 (1) (l))

---

[3] *FIPPA* differentiates between authorized disclosures within Canada only, and authorized disclosures inside or outside Canada

Red light

May not disclose

While *FIPPA* and *PIPA* do not outline specific situations when you cannot share information, we can work backwards from authorized disclosures to conclude that in general, disclosure is usually not authorized if

- The disclosure is not for the purpose of continuity of care and disclosure is not mandated by law. In other words, the individual requesting the information does not have a right to it;
- You are disclosing more information than the person you're disclosing information to (such as the clinician, carer or other agency) needs to know; or
- The individual did not consent and the information is not required to provide care or services

As a general rule, it is wrong to disclose information for a purpose that is different than the purpose for which the information was collected. For example, if you have collected personal information to provide someone with health care, you cannot disclose that information to open a bank account—unless you have consent to do so.

Consent

This guide does not focus on making decisions about whether an individual is able to consent.

However, given that this report focuses on children and youth, it is important to note that in general, parents and guardians can consent on behalf of infants (please note that the legal definition of an 'infant' is a person under the age of 19 years). However, the Infants Act contains information regarding infants providing consent. In this legislation, infants may consent to health care without consent from the infant's parent or guardian. Under Section 17 (3) of the *Infants Act,* this can be the case given the health care provider providing the health care intervention:

a. has explained to the infant and has been satisfied that the infant understands the nature and consequences and the reasonably foreseeable benefits and risks of the health care, and

b. has made reasonable efforts to determine and has concluded that the health care is in the infant's best interests.

In addition, both *FIPPA* and *PIPA* have Regulations that state who may act on behalf of minors and others.

Best Practices for the Consent process

Consent is not required for sharing general information about mental health or substance use issues (e.g., general information about schizophrenia). General information is "information that supports families in their role, without providing new details specific to the service user"[xliii] (p. 152). General information can be useful in addition to personal information about the individual.

A proactive approach to the consent process, on behalf of individuals and their families, helps service providers support rather than wait for individuals or families to request information.[xliv] Further best practices on consent are listed later in the report.

For suggestions of best practices when there is no consent, see Appendix 4.

Life Trumps Privacy

When making a decision on whether or not to share information, it can be easy to focus on the consequences of potentially over-sharing information. Fear of the legal and personal ramifications of over-sharing information can cause providers to act in a more risk averse manner than necessary when considering sharing information.

The former Privacy Commissioner of BC, David Loukidelis, notes that if there are compelling circumstances affecting an individual's health or safety, or if they are ill, the BC privacy laws allow disclosure to next of kin, school officials, health care workers and others. His comment on disclosure and BC privacy laws is as follows[xlv]:

"Individual cases can be fuzzy. But if someone uses common sense and in good faith discloses information, my office is not going to come down on them. Privacy is important, but preserving life is more important [...] I know that frontline decisions have to be made quickly and sometimes the facts may not be as clear as you'd like. But there's no doubt that privacy laws support disclosures to protect health and safety." —David Loukidelis, former Privacy Commissioner of BC

Best Practices: Privacy and Information Sharing

While the legislation provides the absolute rules, best practices can be useful supplemental information in situations where judgment and interpretation is required. Best practices can also be useful to help shape procedures, guidelines, policies or standards at the organizational or professional level. In the absence of guidelines to support a deeper understanding of the legislation, service providers may default to interpret application of the legislation in its strictest form.

The following principles are derived from best practices and recommendations from a scan of relevant Canadian and international literature.

Knowledge

- Understand and comply with the law.[xlvi]
- Know standards and ethical codes of professional bodies[xlvii] and the information-sharing policies and procedures of your organization.
- Policies should be clear, practical and accessible[xlviii] and be accompanied by practical guidance and education. This should fit within systems, which help ensure that rules are followed.[xlix]
- Know whom to approach within your organization or area for guidance.
- Know your responsibilities with respect to privacy and information sharing.[l]
- Differentiate between general and personal information. For example, it may be possible to still give general information without consent if diagnosis is known and information on available supports, services, or programs[li]—this is a judgment call on a case-by-case basis.

Responsibility

- Treat personal information confidentially and respectfully.[lii]
- In addition to the responsibility to protect patient privacy, there is also a responsibility to share information in certain cases[liii]. Know when information must be disclosed. Do not let privacy get in the way of health or safety.
- Keep within your scope of practice.
- Exercise sound clinical judgment and consult with colleagues or supervisors when in doubt.

Purpose

- Identify the purpose of and rationale for sharing information.[liv] The purpose should be broad enough to capture everything you intend to do, but not so broad that it is meaningless.
- Access to personal confidential data should be on a strict need-to-know basis[lv], meaning that essential information is shared, but nothing more. In other words, information should be shared for the purpose of providing safe and effective care.[lvi]
- Use caution when disclosing information that is not for the purposes of providing care (the purpose for which the information was collected)—using personal information for secondary purposes requires consent.

Consent

- Seek the consent of the individual to share their information[lvii], and, with some exceptions, respect an individual's right to object[lviii].
- Use plain language to ensure the individual understands information sharing.[lix]
- Explain the purpose and benefits of sharing information.[lx]
- Let the individual know they can withdraw consent at any time.[lxi]
- Document verbal consent in the individual's file, specific to named agencies rather than staff members.[lxii]
- Seek consent early on in the care relationship (e.g., at intake) and have a conversation about how their information may be used, who should be involved in their care (e.g., family and other service providers), and document the decisions made.[lxiii] Consent should be sought when it is easy to explain what information is being collected, why, how it will be used and to whom it may be disclosed.
- Differentiate between specific consent (sharing a particular piece of information) and general consent (may share all personal or care information with family).
- Where appropriate, review consent at key milestones (e.g., release planning) and on an ongoing basis.[lxiv]
- For best practices on making disclosure decisions situations when there is no consent, see Appendix 4.
- For youth, seek consent of a parent or guardian, unless the youth is able to consent themselves (Infants Act, section 17).[lxv]
- If an individual is unable to provide consent, make an attempt to seek consent when their mental state has improved.[lxvi]

- If an individual doesn't want information shared with family, have a conversation to understand their concerns.[lxvii] Ask: are they refusing consent because they are concerned about a particularly personal or sensitive piece of information? Without a discussion initiated by the service provider, "no consent" may be recorded and an opportunity may be missed.
- Revisit consent on an ongoing basis.
- Seeking consent for disclosure or being open about how an individuals' information may be shared, even when consent is not required, can help build trust.
- Conversations about who to share information with (e.g., seeking consent from the individual to share with family) can help encourage individuals to build their support network.[lxviii]

Communication

- Maintain open communication between individuals, family/families, and service providers.[lxix]
- Communicate with individuals about how their information may be collected, used and disclosed, and inform them of their right to request their own information.[lxx]
- Encourage individuals to understand the value of collaboration and information sharing between service providers.[lxxi]
- Be honest and up front with individuals and their families about limits to privacy and confidentiality.[lxxii]
- Maintain open communication at key milestones for individuals, including service entry, treatment planning, team review, exit planning and relapse response.[lxxiii]

Training and Education

These principles cannot be operationalized without clear direction and support for service providers and families. Training for service providers in the privacy legislation that applies to their practice, namely *PIPA, FIPPA* or other relevant legislation, will help support service providers in understanding this information and applying it to their work. Clear organizational policies, guidelines or protocols help service providers understand the requirements in the legislation in a 'real' and tangible way in order to operationalize legislation guidance.

Research shows that professionals report that when information-sharing policies are well-published in the workplace they are useful documents. In particular, when these documents provide practical guidance on how to resolve information-sharing dilemmas and outline legal and ethical boundaries of professional responsibility they are most useful.[lxxiv]

Service providers who seek additional support or guidance for specific questions or difficult and complex situations should be offered organizational support and guidance. As decisions must often be made quickly with limited information, front line staff should have training in risk assessment.[lxxv] Organizations may also endorse an individual- and family-focused lens in all of their work. This can have positive effects at all levels: from the way information sharing and consent are framed at the initial conversation with an individual and their family, to how, when, and what information is shared, to how consent forms and other materials are designed and what language is used.

Though training and education may be easiest to organize at a local, site or organizational level, opportunities to partner with other service providers (external to the organization) for joint training in the context of local service delivery and collaboration[lxxvi] may allow for discussion and problem solving from a cross-agency perspective. To this end, information sharing questions and scenarios in privacy training would better mirror the real and complex dilemmas service providers face and the applicability of training would increase.

Training should be available to and required of all staff. In addition, if new forms, policies, guidelines or guidance documents are developed, all staff should be trained on the changes.[lxxvii]

Building Tri-Partite Relationships

Literature, evidence, and input from service providers, family, and individuals indicates that a key best practice in information sharing is building of tri-partite relationships—strong relationships between individuals, family and service providers. However, this can be a challenge. Confidentiality smokescreens are a common barrier for families and result in families feeling undervalued and treated unequally. Often this means the flow of information often moves from the family to the service provider, but less often in the other direction. Families may interpret silence, or a lack of information or information sharing, as a stigma (e.g., not talking about it because it's "shameful").[lxxviii]

Confidentiality smokescreens can make obtaining relevant information difficult for families and exclude them from decision-making, ultimately causing important information about an individual to be overlooked.[lxxix] The importance of keeping an individuals' family informed is well-known[lxxx]; however, specific guidance on how to go about sharing information with families is lacking.

The culture of information sharing is shifting toward more formal recognition of the role that family have in the care, recovery and ongoing support of individuals, largely due to initiatives across the province and in other jurisdictions. This cultural shift requires trusting and respectful partnerships, as well as a culture of inclusion, which can mean including families as partners within the circle of care. For example, the circle of care for an individual may include the family physician, care team and service providers, police acting under the *Mental Health Act* and family and families.

The cultural shift also includes a shift of moving beyond treating the individual, and instead working with the individual and identified family members. This means moving towards a Tripartite Relationship: described by a recent report as "the ideal culture of a mental health system [that] involves individuals, families and service providers working in partnership toward positive outcomes for individuals"[lxxxi]. Tripartite relationships require trust as well as open and ongoing communication among these three groups.

The key features of effective Tri-Partite relationships echo the other findings in this report. Service providers can help by listening and receiving information from family, treating family members as part of the care team, and encouraging individuals to see the benefits of including family in treatment/care and sharing information to support the goals of recovery. These are all components of building an effective tripartite relationship.[lxxxii] Ideally, these conversations should occur (and be documented) at the beginning of the care or service relationship.[lxxxiii] This means advance agreements relating to information sharing with families which are established when the individual is well and are shared with families to inform them of specifically to whom information can be shared during times of illness.[lxxxiv]

Overall, this culture shift can be supported with education and guidance documents for service providers on how to build Tripartite Relationships and how to communicate openly with families while still complying with legislation and respecting individuals' privacy.

Recommendations

The following recommendations outline what front-line staff, government, leadership and decision makers can do to better support families and individuals and shift organizational culture toward effective information-sharing practices.

Enablers of success provide guidance for change management strategies, new initiatives or shifts in information-sharing culture. The following questions can help families to discern whether the appropriate groups have been consulted:

- Have individuals and families been appropriately consulted and involved at all stages of the initiative?
- Have front-line staff of all areas been involved and consulted appropriately to ensure that the initiative is practicable, realistic and beneficial?
- Has the Office of the Information Privacy Commissioner been consulted for expertise? (If necessary, has a Privacy Impact Assessment been completed?)

What Government, Leadership and Decision Makers Can Do

- Build trust—organizations need to clearly communicate to their staff that they will not be punished if they share information in good faith for continuity of care, health and safety purposes.
- Raise profile of local expertise, including privacy offices and OIPC hotlines.
- Align policy and procedural documents across organizations—staff of multiple agencies/organizations must collaborate on common CYMHSU goals.
- Construct a joint inter-agency consent form that is individual and family friendly.
- Develop privacy and information sharing agreements as needed between MCFD, community agencies, physicians, Health Authorities, schools and other agencies.
- The OIPC could produce or endorse a guidance document specific to this area (as has been done for interpreting *PIPA* for businesses and organizations).

What Front-Line Staff Can Do

- Communicate barriers to leadership and decision makers so that they can help shape the information sharing culture at a systems-level.
- Build relationships with colleagues in other agencies and organizations.
- Seek out training, education, and guidance. Consult available resources for help.

Shifting Culture

- Continue to build upon success of local interdisciplinary teams – build relationships, clarify roles, learn about how others operate, when they can share information and what the limits of information sharing are.
- Provide practical and applied courses and education sessions at organizations where real-life scenarios are discussed. Consider developing inter-agency training to bring diverse service providers together from different organizations.
- Recognize information sharing is not only about better guidance (i.e., legal interpretation), but also about organizational and professional culture, building trust, and building environments and systems that support information sharing. Focus on shifting culture, building trust, and fostering relationships.
- Share information with families and take a positive approach towards working with them.
- Re-frame information sharing for youth and their families in a positive, comprehensive way. Use language that empowers rather than listing what can go wrong or using complex legal jargon.

Develop a Provincial Learning Community

A community of practice (CoP) is a collaborative framework, which allows for the continual co-learning between members. A CoP is "a group of people who share a concern, a set of problems or a passion about a topic, and who deepen their knowledge and expertise by interacting on an ongoing basis."[lxxxv]

CoPs, or similar frameworks, are used in many disciplines. They are diverse, but share three common elements[lxxxvi]:

1. **A community**—where members interact, discuss, collaborate and build relationships
2. **A shared domain of interest**—in this case it would be information sharing in CYMHSU in BC
3. **A shared practice**—tools, experiences, solutions, plans to implement knowledge that address the shared domain of interest

CoPs are active, participatory, democratic and self-organizing.[lxxxvii] They operate on principles of transparency, community-based decision making and engagement of all members in shared practice.[lxxxviii]

A CoP of service providers would be an effective way to organize a group of people around improving information sharing in CYMHSU in BC. Sharing knowledge, co-designing tools, sharing best practices and building relationships across professions, organizations and sectors could occur as a result of the collaboration that CoPs foster. A CoP would focus on the needs of all members as individuals while building a foundation for improved trust and collaborative relationships. This could translate into better practice and outcomes for individuals and families.

A CoP recognizes that there are individual factors and actions, as well as systems-level barriers, which must be addressed for significant and lasting change. A CoP in CYMH in BC (or several regional CoPs) may also be able to collect and analyze information to report up to decision makers and government or to monitor change after the implementation of new policies or practices.

Moving beyond a network or a local practice team, CYMHSU CoPs in BC have the potential to support shifts in both individual practice and systems-level change.

There are many available resources to support CoP development.[lxxxix xc xci xcii xciii xcv]

Develop High-Quality Education and Training

Ideally, a website with practical scenarios and guidance could be created and updated on an ongoing basis. One example is the Education Development Centre's *Information Sharing* webpage, which is part of their PromotePrevent project.[xcvi] The Education Development Centre is a global nonprofit primarily based in the US that carries out projects in education, health and economic development.[xcvii] Information on this initiative can be found at www.promoteprevent.org.

The website and tools they have created provide an interactive learning experience for service providers that is brief, clear, quick and engaging. They use 20 real-life case examples and walk through various options for each, answering questions such as:

- Who has the information?
- Who wants the information?
- What information does the requester want?
- What does the requester want to do with the information?

- Which laws are relevant in this situation?
- What do the laws permit and what do they prohibit?
- How can the service provider proceed?

The scenarios involve communication across multiple roles and laws. Service providers are asked to think through a scenario rather than read a list of rules. Providers practice making difficult decisions about disclosure and build capacity. Issues are identified at the beginning of each scenario so that service providers can browse the scenarios most relevant to their role or work. Learners watch illustrated dialogue, then must select which conditions of the laws are met in order to disclose/not disclose information. The training also allows the learner to select options to see how the scenario would turn out if different choices were made. There also provide seven illustrated scenario-based e-learning activities for children.

The website also describes how to use the three Bold Steps of *Partner-Plan-Act* to create an information-sharing system that works for everyone involved. More specifically, the site explains how to collaborate with others to share information; create interagency agreements support information sharing; develop uniform consent forms; train staff and use technology to share information, develop and refine policies and protocols; communicate with shareholders; and allocate time and funding for information sharing.[xcviii]

We highlight this educational tool as an innovative approach to training that could be used as a model to develop something similar in BC.

Conclusion

Effective information sharing begins with the individual and their family. For the purposes of continuity of care, effective information sharing must be compliant with legislation and other rules. It includes up front and ongoing communication with an individual and their family about how information will be used. Decisions regarding information sharing are documented and are a topic of ongoing discussion between individuals, families and service providers.

Effective information sharing, first and foremost, requires a cultural shift. Information sharing needs to be viewed by all as an asset, not a burden or risk. Barriers such as confidentiality smokescreens and a culture of fear surrounding privacy can prevent service providers and families from sharing information in an effective manner. We hope that by focusing on education, communication, relationship building and collaboration, families, service providers and individuals can overcome existing cultural barriers to sharing information. Following that, practical barriers to effective information sharing can be addressed.

Service providers encounter complex situations when applying relevant legislation and best practices to their daily work. Scenario-based education can provide the opportunity for providers to practice thinking through situations relevant to their practice. Education is best focused on empowering individuals by helping them understand what they can do, rather than focusing on what they cannot do. This encourages service providers to make better-informed and balanced decisions.

We hope that organizations, agencies and public bodies will focus on developing clear policies and procedures for sharing information that supports cross-system collaboration and family-centered care in a meaningful way.

Privacy should not be a barrier to health, safety or the provision of high-quality care. In fact, appropriate and effective information sharing is an important ingredient to a family-centred mental health and substance system. And above all, we all need to remember that "life trumps privacy."[xcix]

Appendix 1: Links to PIPPA and FIPPA Guidance

Organizations

- Office of the Information & Privacy Commissioner for British Columbia: www.oipc.bc.ca
- Office of the Chief Information Officer: http://www.cio.gov.bc.ca

Provincial Privacy Legislation

- *BC Freedom of Information and Protection of Privacy Act (FIPPA)*
- *BC Personal Information Protection Act (PIPA)*

Reference Guides

- *A Guide to PIPA for Businesses and Organizations* (April 10, 2012). Published by the Office of the Information & Privacy Commissioner for BC. Accessible on the OIPC's Guidance Documents site.
- *Privacy Toolkit for Physicians* (June 15, 2009). Published by the BC Medical Association, the Office of the Information & Privacy Commissioner for BC, and the College of Physicians and Surgeons

BC Privacy and Access Helpline

For public bodies and private sector organizations with inquiries specific to privacy matters can contact the BC Privacy Help Line: Phone: 250-356-1851 • Fax: 250-953-0455 • Email: Privacy.Helpline@gov.bc.ca

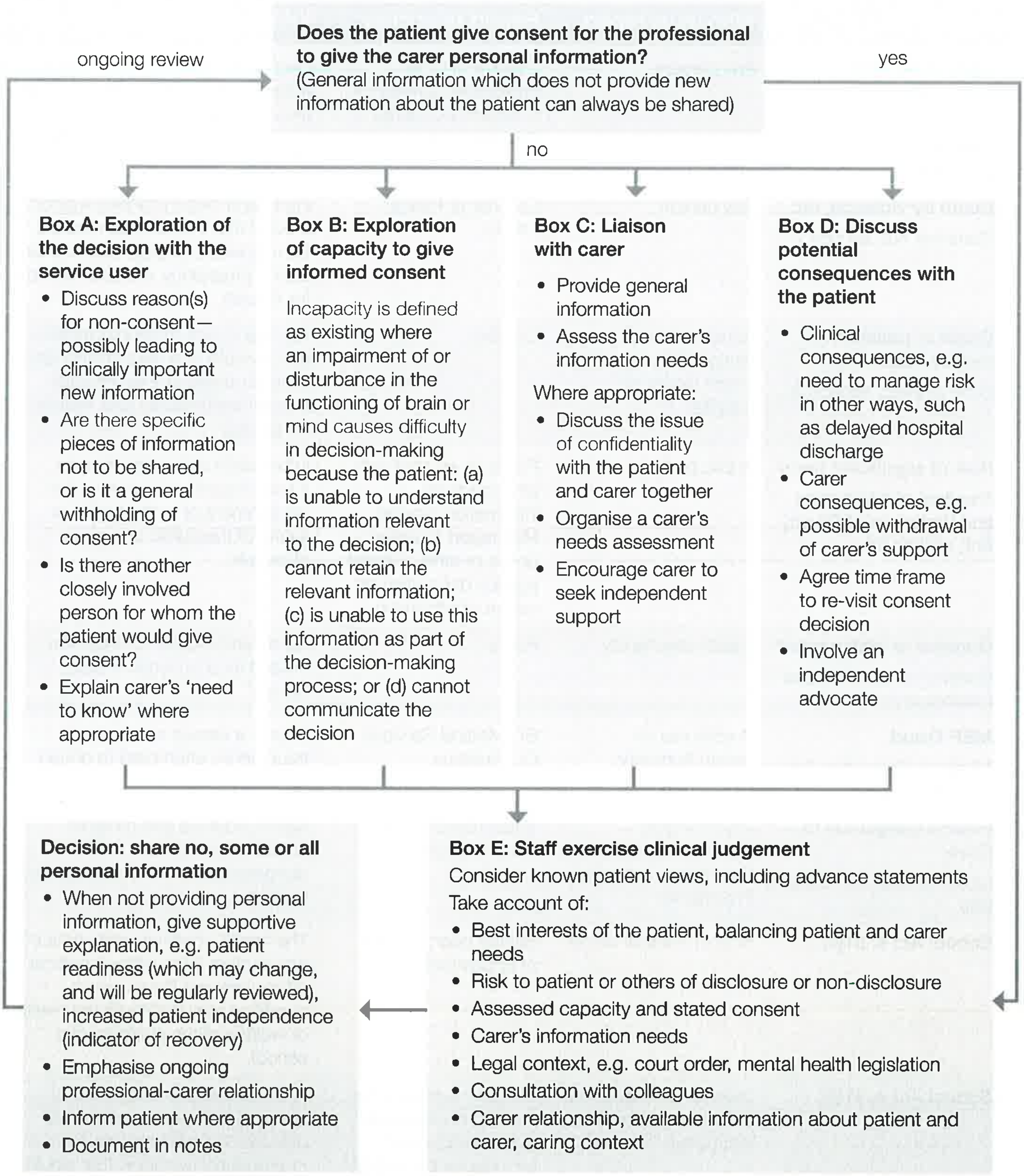
Appendix 2: Mandatory Demands for Production

Agency	Authority to demand	Proof of authority
Community Care Facilities Licensing Community Care and Assisted Living Act, section 9	Director of licensing or a medical health officer may require the community care facility to produce relevant records	Written request with letter of delegation or production of credentials to confirm identity.
Coroner *Coroners Act*, section 11	Coroner may inspect, copy and seize any records relating to the deceased person or the circumstances of the death that the coroner has reason to believe are relevant to the investigation—person receiving request must promptly comply	Written request or production of credentials to confirm identity.
ICBC Insurance (Vehicle) Act, section 28	Where a person is injured in a motor vehicle accident in BC, ICBC may require a report of injuries, diagnosis, treatment and prognosis.	Request from ICBC for completion of a CL19 Medical Report. (But refer to Health Records any other ICBC request for copies of health records).
Ministry of Children and Family Development Child, Family and Community Service Act, section 96	Director of Child Protection (or delegate) has the right to any information of a public body necessary to exercise his or her powers/ duties under the Act	Written request with letter of delegation or production of credentials to confirm identity
Representative for Children and Youth Representative for Children and Youth Act, section 10	Representative has the right to any information of a public body necessary to exercise his or her powers/duties under the Act	Written request or production of credentials to confirm identity

Appendix 3: Reporting Required by Law

Law	Who must report	Report to agency	Information to be reported
Child in need of protection Child, Family and Community Service Act, section 14	Any person	Director of Child Protection, Ministry of Children and Family Development	Facts and circumstances supporting a belief that a child (a person under the age of 19) needs protection (see section 13 of the Act for examples of child in need of protection)
Death by violence, etc. Coroners Act, section 2	Any person	Coroner or Peace Officer	Facts and circumstances supporting a belief that a death has resulted from violence, negligence, suicide, during pregnancy, etc. (see section for details)
Death of patient in mental health Coroners Act, section 4	Administrator of designated mental health facility or hospital	Coroner	Facts and circumstances relating to the death of a person who dies while a patient of a designated mental health facility (see section for details)
Risk of significant harm Freedom of Information and Protection of Privacy Act, section 25	Public body	Public or an applicant who made an information request. May report to police police or other relevant agency depending on nature of information	Information necessary to avert a risk of significant harm to the environment or to the health or safety of the public or a group of people.
Gunshot or stab wound Gunshot or Stab Wound Disclosure Act	Health care facility	Police	Name and location of a person treated for a gunshot or stab wound
MSP Fraud Medicare Protection Act, s. 47.1	Practitioner or Health Authority	BC Medical Services Commission	Report a person who has fraudulently attempted to obtain benefits
Patient dangerous to drive Motor Vehicle Act, section 230	Psychologist, Optometrist, Medical Practitioner or Nurse Practitioner	Superintendent of Motor Vehicles	Name, address and medical condition of a patient who is dangerous to drive and continues to drive.
School Act s. 91(2)	School medical officer	School board (Board of Education)	The health condition and name of any student if the school medical officer believes the student's condition may endanger the health or welfare of the students of a school.
School Act s. 91(5)	Teacher, principal, vice principal or director of instruction	School medical officer, school principal and superintendent of schools for the district	A student who is suspected of suffering from a communicable disease or other physical, mental or emotional condition that would endanger the health or welfare of other students.

Appendix 4: Framework for Best Clinical Practice When Consent is Not Given[4]



Does the patient give consent for the professional to give the carer personal information?
(General information which does not provide new information about the patient can always be shared)

Box A: Exploration of the decision with the service user

- Discuss reason(s) for non-consent—possibly leading to clinically important new information
- Are there specific pieces of information not to be shared, or is it a general withholding of consent?
- Is there another closely involved person for whom the patient would give consent?
- Explain carer's 'need to know' where appropriate

Box B: Exploration of capacity to give informed consent

Incapacity is defined as existing where an impairment of or disturbance in the functioning of brain or mind causes difficulty in decision-making because the patient: (a) is unable to understand information relevant to the decision; (b) cannot retain the relevant information; (c) is unable to use this information as part of the decision-making process; or (d) cannot communicate the decision

Box C: Liaison with carer

- Provide general information
- Assess the carer's information needs

Where appropriate:

- Discuss the issue of confidentiality with the patient and carer together
- Organise a carer's needs assessment
- Encourage carer to seek independent support

Box D: Discuss potential consequences with the patient

- Clinical consequences, e.g. need to manage risk in other ways, such as delayed hospital discharge
- Carer consequences, e.g. possible withdrawal of carer's support
- Agree time frame to re-visit consent decision
- Involve an independent advocate

Box E: Staff exercise clinical judgement

Consider known patient views, including advance statements

Take account of:

- Best interests of the patient, balancing patient and carer needs
- Risk to patient or others of disclosure or non-disclosure
- Assessed capacity and stated consent
- Carer's information needs
- Legal context, e.g. court order, mental health legislation
- Consultation with colleagues
- Carer relationship, available information about patient and carer, caring context

Decision: share no, some or all personal information

- When not providing personal information, give supportive explanation, e.g. patient readiness (which may change, and will be regularly reviewed), increased patient independence (indicator of recovery)
- Emphasise ongoing professional-carer relationship
- Inform patient where appropriate
- Document in notes

---

[4] From Slade, M.; Pinfold, V.; Rapaport, J.; Bellringer, S.; Banerjee, S.; Kuipers, E. & Huxley, P. (2007). "Best practice when service users do not consent to sharing information with carers: National multimethod study." *The British Journal of Psychiatry,* 190, 148-155.

Definitions

Access: "the process of viewing and/or obtaining data and/or personal information".[c]

Circle of Care: "a principle that recognizes and understands the practicality of the need for implied consent for relevant information to flow from one health care provider to another in order to ensure the best level of patient care, unless the health care provider who provides the information is aware that the individual has expressly withheld or withdrawn consent".[ci] The Circle of Care is an evolving concept that speaks to the challenges of obtaining informational consent in the health care environment.[cii]

Collection: "the gathering, acquisition, receipt, or obtaining of personal information".[ciii]

Confidentiality: "the ethical principle or legal right that a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure".[civ]

Consent: "means agreement. There are two types of consent: Express Consent and Implied or Implicit Consent. Express Consent means that you have expressed your consent either in writing or by giving verbal instructions. Implied or Implicit Consent means that it is assumed that you agree, because in the situation it is obvious why your personal health information is collected, used or disclosed".[cv]

Disclosure Directives: "an individual's ability to control when and by whom his or her personal health information will be accessed".[cvi]

Disclosure: "making information available to another organization or third party, or to the individual the information is about".[cvii] Disclosure means "to give out or allow information to be seen by a person or organization".[cviii]

Expressed Consent or Explicit Consent: "consent signified by the willing agreement of an individual for the collection, use, and disclosure of personal information for a defined purpose (opt-in model). The consent can be given verbally or in writing—see also Implied Consent".[cix]

Family: Family or families may include family members, friends or other individuals who provide support or care to individuals. The term family intends to signify a broader, person-centered approach to care providers. Family members are people who have been identified by the individual, the representative or care provider who provides support to the individual on a regular basis or someone identified as being in a relationship of importance to the individual.

Freedom of Information and Protection of Privacy Act (FIPPA)**:** "BC legislation that governs personal information collected, used, and disclosed by public bodies including Health Authorities and the Ministry of Health Services".[cx]

Implied Consent or Implicit Consent: "consent signified by the acceptance by a reasonable individual for the collection, use, and disclosure of information for an obvious purpose where it is understood that the individual will indicate if he or she does not accept (opt-out model). For implied consent to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution-see also Expressed Consent".[cxi]

Individual: "the person/patient about whom information is collected. This includes persons who are authorized to exercise rights on behalf of an individual/patient (e.g., parents on behalf of a child; guardian or trustee; personal representative)". [cxii]

Need to know principle: "access to personal information based on a legitimate relationship with the patient and a need to access or use the personal information for the execution of one's duties".[cxiii]

Individual with lived experience: all people receiving care or services. Sometimes individuals with lived experience are referred to as individuals, clients or patients. The term individual is used in this document.

Personal Health Information: "information about an individual that identifies the individual and the individual's health history including physical or mental health; the provision of health services that individual; the registration of the individual for the provision of health services; payments or eligibility for health care; and any information collected in the course of the provision of health services to the individual".[cxiv]

Personal Information Protection Act (PIPA): "BC legislation that governs personal information collected, used and disclosed by all private sector organizations, including physicians' private practices and other private health care facilities".[cxv]

Personal Information: "any information about an identifiable individual, but does not include business contact information (e.g., Individual's title, business telephone number, business address, business email or facsimile number). Examples of personal information include: name, age, marital status, employment history, national/ethnic origin, political or religious beliefs, sex, sexual orientation, contact information, address, and health care, educational, financial, criminal, opinion (unless it is about someone else), fingerprints, blood type, DNA information, biometrics, individual's health care providers, health numbers (such as care card number) and insurance."[cxvi]

Privacy: "the right to be free from intrusion and interruption. It is linked with other fundamental rights such as freedom and personal autonomy. In relation to information, privacy involves the right of individuals to determine when, how, and to what extent they share information about themselves with others".[cxvii]

Use: "the application of information for a specific purpose by the person or organization that collected the information".[cxviii]

References

i. Waddell, C.; Shepherd, C.; Schwartz, C.; & Barican, J. (2014). "Child and youth mental disorders: Prevalence and evidence-based interventions." Children's Health Policy Centre, Simon Fraser University.

ii. Government of British Columbia, Ministry of Health Services, & Ministry of Children and Family Development. (2010). *Healthy minds, healthy people: A ten-year plan to address mental health and substance use in British Columbia*. Victoria, BC.

iii. University of Texas Health Centre at San Antonio. (May 2009). "Do you know the difference between "Privacy" and "Confidentiality"? Retrieved from http://research.uthscsa.edu/ocr/Privacy%20and%20Confidentiality%20in%20Human%20Research.pdf

iv. Morris, J. (2013). "What Would a Family-Centered Mental Health and Substance Use Care System Look Like?" Visions: BC's Mental Health and Addictions Journal, 8(3), 7-9. Retrieved from www.heretohelp.bc.ca/sites/default/files/visions-families-vol8.pdf

v. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

vi. Queensland Health. (2011). "Information sharing between mental health workers, consumers, carers, family and significant others." Retrieved from www.health.qld.gov.au/mentalhealth

vii. Ibid.

viii. Ontario Ministry of Children and Youth Services (2010). "Ontario's Policy Framework for Child and Youth Mental Health." Retrieved from www.children.gov.on.ca/htdocs/English/topics/specialneeds/mentalhealth/shared_responsibility.aspx

ix. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

x. College of Physicians and Surgeons of Ontario. (2006). "Policy Statement #8-05: Confidentiality of personal health information." Retrieved from: www.cpso.on.ca

xi. Richardson, S. & Asthana, S. (2006). "Inter-agency information sharing in health and social care services: The role of professional culture." *British Journal of Social Work. 36,* 657-669. Doi:10.1093/bjsw/bch257

xii. Government of British Columbia, Ministry of Health Services, & Ministry of Children and Family Development. (2010). *Healthy minds, healthy people: A ten-year plan to address mental health and substance use in British Columbia.* Victoria, BC.

xiii. Ontario Ministry of Children and Youth Services (2010). "Ontario's Policy Framework for Child and Youth Mental Health." Retrieved from www.children.gov.on.ca/htdocs/English/topics/specialneeds/mentalhealth/shared_responsibility.aspx

xiv. Ibid.

xv. Mental Health Commission of Canada. (2013). "School-Based mental health in Canada: A final report." School-based Mental Health and Substance Use (SBMHSA) Consortium.

xvi. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

xvii. Ibid.

xviii. Royal College of Psychiatrists. (2010). *Carers and confidentiality in mental health.* Retrieved from www.rcpsych.ac.uk/healthadvice/partnersincarecampaign/carersandconfidentiality.aspx

xix. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

xx. Royal College of Psychiatrists. (2010). *Carers and confidentiality in mental health.* Retrieved from www.rcpsych.ac.uk/healthadvice/partnersincarecampaign/carersandconfidentiality.aspx

xxi. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

xxii. Slade, M.; Pinfold, V.; Rapaport, J.; Bellringer, S.; Banerjee, S.; Kuipers, E. & Huxley, P. (2007). "Best practice when service users do not consent to sharing information with carers: National multimethod study." *The British Journal of Psychiatry, 190,* 148-155. Doi: 10.1192/bjp.bp.106.024935

xxiii. Vancouver Coastal Health. (2013). "Family involvement in mental health and addictions services." Vancouver, BC.

xxiv. Ibid.

xxv. Richardson, S. & Asthana, S. (2006). "Inter-agency information sharing in health and social care services: The role of professional culture." *British Journal of Social Work. 36,* 657-669. Doi:10.1093/bjsw/bch257

xxvi. Alberta Government. (May 2013). "What we heard: Part two feedback summary on the information sharing strategy." Retrieved from http://humanservices.alberta.ca/department/14802.html

xxvii. Ibid.

xxviii. Ibid.

xxix. Ibid.

xxx. Ibid.

xxxi. Royal College of Psychiatrists. (2010). *Carers and confidentiality in mental health.* Retrieved from www.rcpsych.ac.uk/healthadvice/partnersincarecampaign/carersandconfidentiality.aspx

xxxii. Devon Partnership, NHS Trust. (2007). "Confidentiality and Carers Guidelines." Exeter, England. Retrieved from www.devonpartnership.nhs.uk/uploads/tx_mocarticles/Carers_Guidelines.pdf

xxxiii. Gray, B.; Robinson, C.; Seddon, D. & Roberts, A. (2013). "Confidentiality smokescreens' and carers for people with mental health problems: The perspectives of professionals." *Health & Social Care in the Community, 16*(4), 378-87.

xxxiv. Alberta Government. (May 2013). "What we heard: Part two feedback summary on the information sharing strategy." Retrieved from http://humanservices.alberta.ca/department/14802.html

xxxv. Alberta Government. (May 2013). "What we heard: Part two feedback summary on the information sharing strategy." Retrieved from http://humanservices.alberta.ca/department/14802.html

xxxvi. Zulman, D.; Nazl, K.; Turvey, C.; Wagner, T.; Woods, S. & An, L. (2011). "Patient interest in sharing personal health record information." *Annals of Internal Medicine, 155,* 805-810.

xxxvii. Slade, M.; Pinfold, V.; Rapaport, J.; Bellringer, S.; Banerjee, S.; Kuipers, E. & Huxley, P. (2007). "Best practice when service users do not consent to sharing information with carers: National multimethod study." *The British Journal of Psychiatry, 190,* 148-155. Doi: 10.1192/bjp.bp.106.024935

xxxviii. Whiddett, R.; Hunter, I.; Engelbrecht, J. & Handy, J. (2006). "Patients' attitudes towards sharing their health information." (2006). *International Journal of Medical Informatics, 75,* 530-541.

xxxix. Ibid.

xl. US Department of Health and Human Services. (2014). (2014). *Your Medical Records.* Retrieved from www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/medicalrecords.html

xli. Queensland Health. (2011). "Information sharing between mental health workers, consumers, carers, family and significant others." Retrieved from www.health.qld.gov.au/mentalhealth

xlii. Denham, E. Information and Privacy Commissioner for BC. (2013). Investigation report F13-05: Public body disclosure of information under section 25 of the Freedom of Information and Protection of Privacy Act. 2013 BCIPC No. 33.

xliii. Slade, M.; Pinfold, V.; Rapaport, J.; Bellringer, S.; Banerjee, S.; Kuipers, E. & Huxley, P. (2007). "Best practice when service users do not consent to sharing information with carers: National multimethod study." *The British Journal of Psychiatry, 190,* 148-155. Doi: 10.1192/bjp.bp.106.024935 xliv. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

xlv. Ontario and B.C. Privacy Commissioners issue joint message: personal health information can be disclosed in emergencies and other urgent circumstances. (2008). CNW Newswire. Retrieved from www.newswire.ca/en/story/276007/ontario-and-b-c-privacy-commissioners-issue-joint-message-personal-health-information-can-be-disclosed-in-emergencies-and-other-urgent-circumstances

xlvi. Digital Information Policy, DH Informatics Directorate (2010). *The Caldicott Guardian Manual.* Leeds, England. Retrieved from www.dh.gov.uk/policyandguidance

xlvii. National Mental Health Consumer & Carer Forum. (2011). *Privacy, Confidentiality and Information Sharing—Consumers, Carers and Clinicians.* Canberra, Australia. Retrieved from www.nmhccf.org.au

xlviii. Ibid.

xlix. Health and Social Information Centre. (2013). "A guide to confidentiality in health and social care: Treating confidential information with respect. Leeds, England. Retrieved from www.hscic.gov.uk

l. Digital Information Policy, DH Informatics Directorate (2010). *The Caldicott Guardian Manual.* Leeds, England. Retrieved from www.dh.gov.uk/policyandguidance

li. Devon Partnership, NHS Trust. (2007). "Confidentiality and Carers Guidelines." Exeter, England. Retrieved from http://www.devonpartnership.nhs.uk/uploads/tx_mocarticles/Carers_Guidelines.pdf

lii. Health and Social Information Centre. (2013). "A guide to confidentiality in health and social care: Treating confidential information with respect. Leeds, England. Retrieved from www.hscic.gov.uk

liii. Digital Information Policy, DH Informatics Directorate (2010). *The Caldicott Guardian Manual.* Leeds, England. Available from www.dh.gov.uk/policyandguidance

liv. British Columbia Medial Association, Office of the Information & Privacy Commissioner for British Columbia, and British Columbia College of Physicians and Surgeons. (2009). *BC Physician Privacy Toolkit.* Available from www.doctorsofbc.ca

lv. Digital Information Policy, DH Informatics Directorate (2010). *The Caldicott Guardian Manual.* Leeds, England. Available from www.dh.gov.uk/policyandguidance

lvi. Health and Social Information Centre. (2013). "A guide to confidentiality in health and social care: Treating confidential information with respect. Leeds, England. Retrieved from www.hscic.gov.uk

lvii. British Columbia Medial Association, Office of the Information & Privacy Commissioner for British Columbia, and British Columbia College of Physicians and Surgeons. (2009). *BC Physician Privacy Toolkit.* Available from www.doctorsofbc.ca

lviii. Health and Social Information Centre. (2013). "A guide to confidentiality in health and social care: Treating confidential information with respect. Leeds, England. Retrieved from www.hscic.gov.uk

lix. Queensland Health. (2011). "Information sharing between mental health workers, consumers, carers, family and significant others." Retrieved from www.health.qld.gov.au/mentalhealth

lx. Ibid.

lxi. Ibid.

lxii. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

lxiii. National Mental Health Consumer & Carer Forum. (2011). *Privacy, Confidentiality and Information Sharing—Consumers, Carers and Clinicians.* Canberra, Australia. Retrieved from www.nmhccf.org.au/

lxiv. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

lxv. Infants Act. R.S.B.C. 1996, C17.

lxvi. Queensland Health. (2011). "Information sharing between mental health workers, consumers, carers, family and significant others." Retrieved from www.health.qld.gov.au/mentalhealth

lxvii. Ibid.

lxviii. College of Physicians and Surgeons of Ontario. (2006). "Policy Statement #8-05: Confidentiality of Personal Health Information." (2006). Toronto, Ontario.

lxix. National Mental Health Consumer & Carer Forum. (2011). *Privacy, Confidentiality and Information Sharing—Consumers, Carers and Clinicians.* Canberra, Australia. Retrieved from www.nmhccf.org.au

lxx. British Columbia Medial Association, Office of the Information & Privacy Commissioner for British Columbia, and British Columbia College of Physicians and Surgeons. (2009). *BC Physician Privacy Toolkit.* Available from www.doctorsofbc.ca

lxxi. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

lxxii. National Mental Health Consumer & Carer Forum. (2011). *Privacy, Confidentiality and Information Sharing—Consumers, Carers and Clinicians.* Canberra, Australia. Retrieved from www.nmhccf.org.au

lxxiii. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

lxxiv. Slade, M.; Pinfold, V.; Rapaport, J.; Bellringer, S.; Banerjee, S.; Kuipers, E. & Huxley, P. (2007). "Best practice when service users do not consent to sharing information with carers: National multimethod study." *The British Journal of Psychiatry, 190*, 148-155. Doi: 10.1192/bjp.bp.106.024935

lxxv. Victoria Government Department of Health. (2010). "Information sharing between area mental health services and psychiatric disability rehabilitation and support services: Chief psychiatrist's guideline." Retrieved from www.health.vic.gov.au/mentalhealth/cpg/information_sharing.pdf

lxxvi. Ibid.

lxxvii. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

lxxviii. Bogart, T. & Soloman, P. (1999). "Procedures to share treatment information among mental health providers, consumers, and families." *Psychiatric Services, 50*(10), 1321-25.

lxxix. Gray, B.; Robinson, C.; Seddon, D. & Roberts, A. (2013). "Confidentiality smokescreens' and carers for people with mental health problems: The perspectives of professionals." *Health & Social Care in the Community, 16*(4), 378-87.

lxxx. National Mental Health Consumer & Carer Forum. (2011). *Privacy, Confidentiality and Information Sharing—Consumers, Carers and Clinicians.* Canberra, Australia. Retrieved from www.nmhccf.org.au

lxxxi. Ibid.

lxxxii. Ibid.

lxxxiii. Ibid.

lxxxiv. Gray, B.; Robinson, C.; Seddon, D. & Roberts, A. (2013). "Confidentiality smokescreens' and carers for people with mental health problems: The perspectives of professionals." *Health & Social Care in the Community, 16*(4), 378-87.

lxxxv. Wenger, E.; McDermott, R. & Snyder, W. (2002). Cultivating Communities of Practice. Harvard Business School Press: Boston, MA. As cited by Centres for Disease Control and Prevention, "Introduction to CoPs" Retrieved from www.cdc.gov/phcommunities/resourcekit/intro/index.html

lxxxvi. Ibid.

lxxxvii. Ibid.

lxxxviii. Ibid.

lxxxix. Wenger, E.; Taryner, B. & De Laat, M. (2011). "Promoting and assessing value creation in communities and networks: A conceptual framework." Tuud de Moor Centrum. Retrieved from http://wenger-trayner.com

xc. Wenger, E.; McDermott, R. & Snyder, W. (2002). Cultivating Communities of Practice. Harvard Business School Press: Boston, MA. As cited by Centres for Disease Control and Prevention, "Introduction to CoPs" Retrieved from www.cdc.gov/phcommunities/resourcekit/intro/index.html

xci. Brown, J. & Duguid, P. (1991). "Organizational Learning and Communities-of-Practice: Toward a unified view of working, learning, and innovation." *Organization Science, 2*(1), Special Issue: Organizational Learning: Papers in Honor of (and by) James G. March. 40-57.

xcii. Rock, F. (2005). "'I've picked some up from a colleague': Language, sharing and communities of practice in an institutional setting." 77-104 in *Beyond communities of practice: Language, power and social context.* Eds David Barton and Karin Tusting.

xciii. Cambridge, D.; Kaplan, S. & Suter, V. (2005). "Community of Practice design guide: A step-by-step guide for designing and cultivating communities of practice in higher education." Retrieved from http://net.educause.edu/ir/library/pdf/nli0531.pdf

xciv. Cox, A. (2005). "What are communities of practice? A comparative review of four seminal works." *Journal of Information Science, 31*(6), 527–540 DOI: 10.1177/0165551505057016

xcv. Probst, G. & Borzillo, S. (2008). "Why communities of practice succeed and why they fail." *European Management Journal, 26,* 335– 347 DOI:10.1016/j.emj.2008.05.003

xcvi. Education Development Centre, Inc. (2013). *PromotePrevent: Information Sharing.* Retrieved from http://informationsharing.promoteprevent.org

xcvii. Education Development Centre, Inc. (2013). *Frequently Asked Questions.* Retrieved from http://informationsharing.promoteprevent.org

xcviii. Education Development Center. (2013). "Sharing Information to Help Youth Involved in Multiple Systems" Retrieved from http://informationsharing.promoteprevent.org

xcix. Loukidelis, D. & Cavoukian, A. (2008). Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions. Toronto, Ontario. Retrieved from www.ipc.on.ca

c. British Columbia Medial Association, Office of the Information & Privacy Commissioner for British Columbia, and British Columbia College of Physicians and Surgeons. (2009). *BC Physician Privacy Toolkit.* Available from www.doctorsofbc.ca

ci. Ibid.

cii. Ibid.

ciii. Ibid.

civ. Ibid.

cv. Health Information Privacy in British Columbia. *Definitions.* Retrieved from www.healthinfoprivacybc.ca/home/definitions

cvi. British Columbia Medial Association, Office of the Information & Privacy Commissioner for British Columbia, and British Columbia College of Physicians and Surgeons. (2009). *BC Physician Privacy Toolkit.* Available from www.doctorsofbc.ca

cvii. Ibid.

cviii. Health Information Privacy in British Columbia. *Definitions.* Retrieved from www.healthinfoprivacybc.ca/home/definitions

cix. Ibid.

cx. Ibid.

cxi. Ibid.

cxii. Ibid.

cxiii. Ibid.

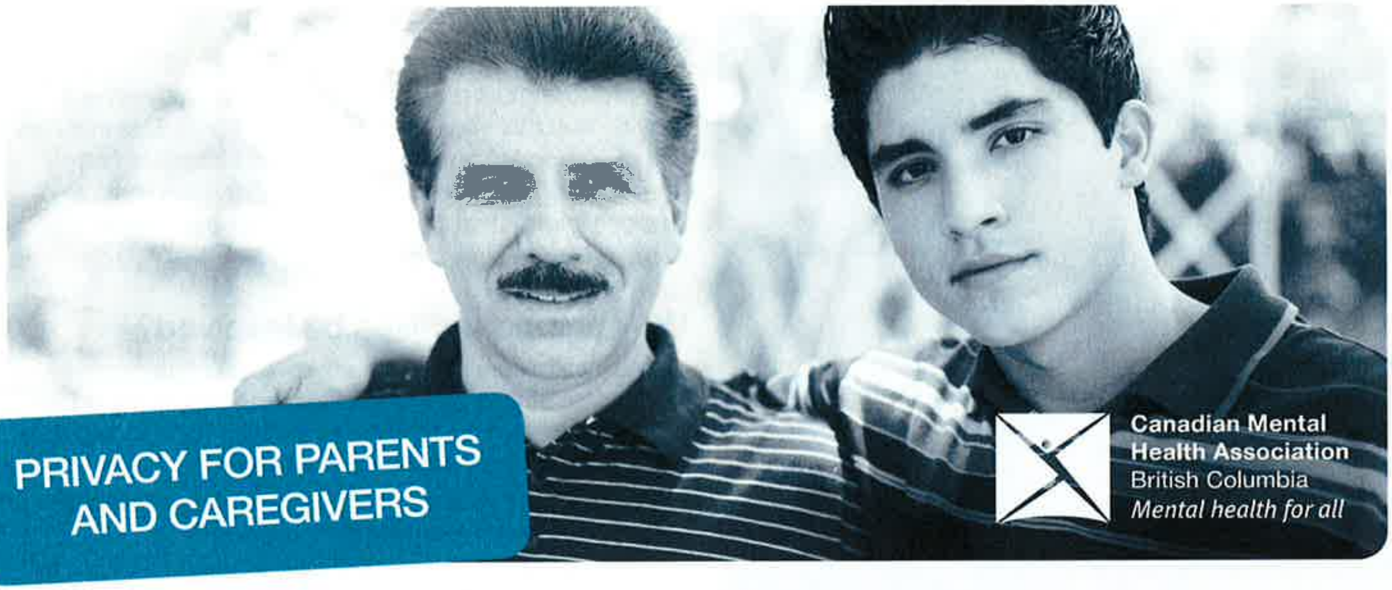
cxiv. Ibid.

cxv. Ibid.

cxvi. Health Information Privacy in British Columbia. *Definitions.* Retrieved from www.healthinfoprivacybc.ca/home/definitions

cxvii. Ibid.

cxviii. Ibid.


[redacted]

PRIVACY FOR PARENTS AND CAREGIVERS

Canadian Mental Health Association
British Columbia
Mental health for all

Many family members and caregivers are surprised to hear that doctors and other service providers can't share information about their child's health. It can be a frustrating situation for everyone, and it can really affect the support that family members can offer. With good planning, you, your child, and your child's service providers can work together to make sure that everyone is included in a helpful way.

When is my child old enough to give their own consent?

The age when a young person can give their own consent is a judgement call. Anyone 19 years of age or older is considered by the law to be an adult and can, in most cases, make their own decisions around consent. It's not quite as clear for people under the age of 19. While the law technically sees anyone under the age of 19 as an "infant", a young child and a young adult have different capabilities when it comes to managing their care. Young people under the age of 19 can make their own care decisions when providers feel that the individual understands what's required of them, understands their own responsibilities, the health care choices and the consequences. At this point, care providers follow the young person's wishes—parents or caregivers can't change or take away the right to give consent or make decisions.

In some situations, people may not be able to give consent regardless of age. People are incapable of giving consent if it's believed that they don't understand what's happening or make sound decisions. For example, someone who is actively experiencing an episode of psychosis may not be able to provide their own consent to treatment.

A note on our words

When we say "**child**," we mean any young person that you care for.

When we say "**family,**" we mean the person or people who care for a young person. This includes biological family, a legal guardian, foster parents, or any other adult that helps out.

When we say "**service provider**," we mean any person, organization, or agency that provides health care. This includes doctors, psychiatrists, psychologists, nurses, school counsellors, therapists, social workers, mental health teams, and more.

Who needs my child's information and what will they do with it?

Different service providers may share information related to your child's care. For example, your child's counsellor may share relevant information with your child's doctor. Even though this information can be shared without your consent in some situations, organizations usually have ethical guidelines around what kind of information they can disclose. Ideally, they should ask for permission whether it's legally required or not or explain their procedures before they begin sharing information.

Your child's service provider may share information with family members if the service provider believes it's in the best interest of the child's care. However, service providers may only share information that's relevant to care, such

Definitions

Personal information—information about an individual person. It includes your name and address, information about your health, information about your education, your cultural background, your religious beliefs, and more. Some information isn't very sensitive, like your name or birthday. Other information is sensitive, like your mental health history and the treatments you use.

Privacy—the right to decide who can access your personal information.

Confidentiality— the responsibility to protect someone else's personal information.

Consent—means that you agree to something. In this factsheet, consent means that the child or youth receiving care agrees to let service providers share information with family members.

Disclosure—another way of saying 'sharing.' When you disclose information, you're sharing information.

as information about a treatment and what your child needs at home. This can be a gray area for many people. It's true that family support is a very important part of recovery, but sharing information in a way that doesn't respect your child's wishes can really damage trust between your child and the service provider. Many service providers, organizations, and agencies have formal or informal policies that say they should have a conversation around consent to this kind of information sharing, even though it's not required by law.

Some information may be used without consent or notification, such as information for researchers and information for statistics or other data. In these cases, the information received will be stripped of anything that might identify an individual. In the very rare case that personal information needs to be collected for these purposes, they must seek written permission first. The individual has the right to refuse sharing.

Any provider must disclose information to authorities if they believe that your child is at risk of harm. This includes risk of suicide (ending your life) as well as acts of harm from someone else, such as abuse. Providers must also disclose information if they believe that your child may harm someone else.

Why should families be involved?

Mental health care is a team effort. Your child's team includes all of their service providers as well as important support people—like families. In addition to providing care and support, family members may also:

- Help a child monitor symptoms of illnesses and help them seek extra help when it's needed
- Help a child follow their treatment plan and monitor for side effects or other problems
- Act as advocates, explain challenges, and explain what care has been provided—this can be very helpful for service providers when the child who is ill has a hard time talking about their experiences or when they're seeing a new provider
- Give their perspectives of the illness, which can give service providers a better idea of what's happening

Families should feel supported and informed. Unfortunately, lack of information, confusion, or lack of communication can get in the way. But by including families as equal members of the team, families are informed and capable of providing the care and support that's needed. When a child begins to take charge of their own health and care, many family members find the transition challenging—they're no longer on the front line of their child's care, and many say that they feel like they're kept in the dark. The laws around sharing information with family members are not clear, and family members may not know what to ask for or what they're allowed to ask for. The best way to make sure that everyone is working together is to have a conversation with your child and their service providers.

What do the laws say? What does it mean for me and my family?

There are two main Acts or laws that say how information is protected and shared. One Act covers information that a private orgnization collects, like a private therapist you pay to see. Another Act covers information collected by a public body, like a hospital, health authority, or government ministry. There are some differences between the two, but they follow many of the same guidelines when it comes to the kind of information sharing we are covering in this factsheet. Here are examples of how these laws work:

Some personal information must be shared if:

- Someone believes that your child is in serious danger (such as immediate risk or suicide) or believes that your child may harm someone else.

Some personal information may be shared if:

- Your child works with more than one service provider, and they need to share information about your child's care. For example, your child's doctor may tell your child's counsellor about a new medication. Service providers can only share necessary information that's relevant to your child's care.
- Your child's service provider believes that family members need information about a child's care. Again, they can only share information that's necessary.
- Your child consents to share information with you or another person. Whoever gives consent can also say what information can be shared. For example, they may consent to share relevant treatment information with family, but keep other details private.
- Your child is sick or injured in a hospital on their own.
- A service provider believe that information sharing is critical to care, but can't obtain necessary consent. This may come up in emergency situations when people have to make decisions very quickly.

Personal information may not be shared if:

- Someone asks for more information than they need to care for your child.
- Someone who isn't providing care asks for your information.
- Your child doesn't allow one person to share their information with another person (they don't give consent)
- The reason for sharing information has changed, even if your child originally gave consent.

Learn more about laws

- Read the Guide to the Personal Information Protection Act at www.cio.gov.bc.ca/local/cio/priv_leg/documents/pipa/guidepipaview.pdf
- Read the Guide to the Freedom of Information and Protection of Privacy Act at www.cio.gov.bc.ca/cio/priv_leg/foippa/foippa_guide.page

When might family not have access to information?

Service providers can refuse to share information with family members, even if someone has given consent. This can happen when:

- A service provider believes that consent was not given freely (for example, someone was tricked or forced to give consent)A service provider believes that providing that information may harm their client or another person
- The information includes other people's personal information
- Information was provided by someone other than your child

How can I start the conversation with my child's health team? What can I ask for?

First, it's important to know that consent is an on-going process, not a one-time conversation. You can start the conversation at any time. Ideally, conversations around sharing information should start during intake or when someone begins to receive services. However, the conversation can (and should) come up regularly. It's important to pick up the conversation if you or your child are no longer happy or comfortable with the current situation or whenever your child's situation changes, such as changes in diagnosis, treatment, care team members, or family situations.

Service providers understand that family involvement is an important part of a child's care. In most cases, service providers are happy to help you and your child find an agreement that works for everyone.

- Ask about confidentiality and information sharing policies and procedures. Some providers may share information based on verbal consent, but most will ask your child to sign a form or agreement.
- Laws around information sharing are not always clear, so you and your child may have a lot of questions or concerns. Don't be afraid to ask questions to clarify any points you don't understand.
- Regularly check in with your child to make sure that they know what's happening and feel good about the current situation.

When your child lets a service provider share information with you or any other family member, it's important to remember that you have a responsibility to protect that information. Sharing health information takes a lot of trust, and it's important to respect your child's privacy. In addition, the stigma of mental illnesses mean that there may be consequences for your child if information is made public without their knowledge or consent.

What if my child doesn't want to share information with family members?

Understandably, many people would rather keep some information private between themselves and their care providers.

Information-sharing doesn't have to be all-or-nothing. A young person who is receiving treatment may feel more comfortable sharing information if they can set their own limits. For example, a young person may let a service provider share their diagnosis and information related to treatment with family members, but keep other information private. This kind of flexibility gives people control over their information but still keeps family members informed of what they need to know.

What about the *Mental Health Act*?

The *Mental Health Act* is a law that lets a service provider assess a person who is believed to be at risk of harming themselves or others due to a mental illness and admit them to a hospital, if needed. This assessment or hospitalization can happen voluntarily (with their consent) or involuntarily (against their wishes). The *Mental Health Act* can be complicated on its own, but there are a few important things to know about information sharing when someone is hospitalized under the Act:

- For the *Mental Health Act*, a person is considered an adult at the age of 16. As with other situations, a person can give their own consent when service providers feel that they understand what's happening, even if they're younger than 16.
- People who are admitted under the *Mental Health Act* have to give consent in writing by filling out a form.
- People can't give consent if providers feel that they are incapable of providing consent, regardless of age. People are also incapable of giving consent if they're believed to be intoxicated.
- The hospital must tell a family member in writing when someone is admitted under the *Mental Health Act*, when they apply for a Review Panel Hearing, and when they're discharged from the hospital. The person admitted can choose who the hospital notifies.
- Ideally, the hospital providing care should try to get consent to share an individual's information with family members. If this can't happen, service providers can still share relevant information about your child's ongoing care without their consent.

For more on the *Mental Health Act*, see the *Guide to the Mental Health Act* resource at www.health.gov.bc.ca/library/publications/year/2005/MentalHealthGuide.pdf

How do you request medical records?

If you want records from a doctor or someone that you see privately, you just need to ask for your records.

If you would like records from a hospital (like during time in hospital or an outpatient program), you usually make a request in writing, with a specific form. Look up the hospital's Privacy Officer for more information about the hospital's specific requirements. If you aren't sure what to do, check if the hospital has a patient advocate, patient navigator, or ombudsperson—they can help connect you with the right department.

How can I make a complaint?

If you have a complaint against a doctor's office, you can make a complaint to the College of Physicians and Surgeons of British Columbia. You'll find their website at www.cpsbc.ca. If you have a complaint about a hospital, you can contact the Patient Care Quality Office for your health authority. You'll find a list of health authorities at www.health.gov.bc.ca/socsec.

You can also make any privacy complaint to the Office of the Information and Privacy Commissioner. You'll find their website at www.oipc.bc.ca.

Where can I go for help?

The Office of the Information and Privacy Commissioner of British Columbia makes sure that everyone follows privacy laws. The 'For the Public' section of their website has a lot of information on your rights, how to make a complaint, and where to go for more help. Visit www.oipc.bc.ca

The People's Law School offers education and information on many different legal concerns. They can also refer you to other resources that can help. Visit www.publiclegaled.bc.ca

This project has been initiated and funded by the Province of British Columbia

BRITISH COLUMBIA

INFORMATION SHARING FOR YOUNG PEOPLE

Canadian Mental Health Association
British Columbia
Mental health for all

Health information—like your diagnoses and treatments—can feel very private. In some situations, though, it's helpful to share this information with other people. It's important to know who needs your information and what they can do with it. This can help you make good decisions about your private information based on your own situation.

In this factsheet, we are going to look at sharing your health information. Health information includes details like your diagnosis, past and current treatments, and personal situations that affect your health.

What is personal information?

Personal information is information about an individual person. It includes your name and address, information about your health, information about your education, your cultural background, your religious beliefs, and more. Some information isn't very sensitive, like your name or birthday. You probably wouldn't worry if other people knew your name and age. Other information is sensitive, like your mental health history and the treatments you use. You may not want everybody to have all of this information.

What does it mean to share information?

Sharing information means that one person shares some of your personal information with another person—usually so that they can provide health care to you. In many cases, others have to ask for your permission or consent before they can share your information. But there are situations when they don't have to ask first.

Before we start ...

Here are some **key terms** we use throughout this factsheet and what they mean:

By **family**, we mean the person or people who care for you. This includes your biological parents, a legal guardian, foster parents, or any other adult that helps out.

Service providers are any person, organization, or agency that you see for your health. This includes doctors, psychiatrists, psychologists, nurses, school counsellors, therapists, social workers, mental health teams, or anyone else who gives you some kind of health care or support.

Your mental health care team is the group of people who are working together to help you live well. Your team may include your doctor, a specialist like a psychiatrist, a counsellor at school, a therapist, a social worker, or anyone else who helps you. Your team also includes people who give you support, like family members or other important adults

Privacy is the right to decide who can access your personal information.

Confidentiality is the responsibility to protect someone else's personal information.

Consent means that you agree to something. In this case, consent means that you agree to let your service provider share information with family members.

Disclosure is another way of saying 'sharing.' When you disclose information, you're sharing information.

Can I give my own consent?

In BC, anyone under the age of 19 is an "infant" according to the law. This technically means that your parents or legal guardians have control of many legal issues—like consent—until you turn 19. However, there's a big difference between a two-year-old and an 18-year-old! In most situations, people under the age of 19 can make decisions about their health care when a service provider believes that they understand what's happening, that they can make decisions on their own, and can understand the consequences. The exact age will be different for everyone as it is based on judgement.

There are a few specific situations when you can't give consent. For example, if you are actively experiencing certain symptoms like psychosis, you may not be able to give consent or change how you want information shared. That's why it's important to talk about information sharing with your service providers and family members and figure out a plan when you feel well. If you have a crisis or emergency plan with any of your service providers (a plan of what will happen in a crisis or emergency), think about including directions for how you would want your information shared.

Why does sharing information matter?

In order to work together, people on your team need information from other people on your team. Sharing information with your team can help them support you.

Sharing can improve your health care

Many people who are dealing with a health problem see more than one service provider. For example, you might see a family doctor, a psychologist, and a counsellor at school. When you make sure that one service provider is sharing information that other providers should know, everyone can give you better care. They know exactly what's going on, what's working for you, and what isn't working for you. Sometimes it's hard to keep track of your health information. Sharing information means that you don't have to remember everything on your own.

Sharing can make it easier to see new service providers

Sharing information means that you don't have to tell your story every time you see a new service provider, agency, or organization. Talking about difficult experiences can be really hard, especially when you're meeting a service provider for the first time. A lot of people feel uncomfortable or embarrassed when they have to talk about problems. Sharing information means that you only have to tell your story once.

Do researchers need my information?

Some information can be shared without asking first if it doesn't identify you. For example, researchers who are studying mental health may get information from a hospital. Some organizations or agencies might collect information for statistics, like the number of people they care for. In these cases, information can be collected without asking for your permission, but they share very specific details that doesn't tell anyone who you are. They can't give any information that would identify you, like your name, address, or phone number. In the very rare case that people do need information that identifies you, they must ask for your permission in writing. You have the right to say no if you don't feel comfortable with their request.

This is how information sharing can work. One service provider can share information about your care with another service provider. For example, your doctor can share information with your school counsellor. They can only share information about your care. This is called an information-sharing agreement.

A service provider can also share information with your family. It's often helpful if family members know about your diagnosis and treatment, but you can decide how much information a service provider shares with family member.

What does the law say? How does it work?

There are two main Acts or laws that say how your information is protected and shared. They are meant to protect your right to privacy, but they let people share specific information if you're in trouble or need help. Here are some examples of how the laws work:

Some of your personal information must be shared when:

- Someone believes that you are in serious danger. This can happen if they're worried about suicide (ending your life) or if someone else is harming you. They must also share information with authorities if they're worried that you might hurt someone else. They will only share relevant information with those who need to know.

Some of your personal information may be shared when:

- You see more than one service provider, and they need to share information about your care. For example, pretend that you see a doctor and a counsellor. Your doctor may tell your counsellor about your new medication. In this case, service providers can only share information that's necessary for your care. Even though some of this information can be shared without asking for your permission (consent), many service providers will ask you first.

- You allow (give consent to) a service provider to share information with someone else.
- Someone is concerned that you or someone else may be harmed without help.

Your personal information cannot be shared when:

- Someone asks for more information than they need to know to care for you.
- Someone who isn't providing care asks for your information.
- You don't allow one person to share your information with another person (you don't give consent)

Learn more about laws

If you want to learn more about the privacy laws in BC:

- Read the Guide to the Personal Information Protection Act at www.cio.gov.bc.ca/local/cio/priv_leg/documents/pipa/guidepipaview.pdf
- Read the Guide to the Freedom of Information and Protection of Privacy Act at www.cio.gov.bc.ca/cio/priv_leg/foippa/foippa_guide.page

What does my team need to know?

Service providers can share information on a "need to know" basis. They share information that others need to give you good health care, but they don't share information that isn't about your care. Here's an example:

A service provider may need to know …

- Your diagnosis
- The medications you take and the treatments you receive (like therapy)
- Problems you've have with other medications or treatments, like bad side effects
- Challenges you experience at home or school because of a mental illness, plus things that help or don't help

But service providers usually don't need to share information like …

- Your religion or beliefs
- Your thoughts and opinions
- Information that doesn't have to do with your health and your care
- Information that is very sensitive, and you want to keep it private (such as past abuse or trauma)

What about my family?

Family members can be really helpful when you're managing a mental illness.

Family members can:

- Help you watch for symptoms of your illness
- Help you find service providers and figure out where to go next
- Help you with your treatment plan and watch for problems, like side effects from medications
- Help you talk to service providers and explain the care you've already received
- Share their experiences, which gives service providers a better idea of your challenges

Do I have to share *everything?*

Absolutely not. You can decide what information is shared with others and what information is private. For example, you can share your diagnosis and treatment without sharing certain details of your experiences.

How do I start sharing information with my team?

Service providers want to respect your privacy and they want to build a good, trusting relationship with you. In order to make sure that you and your service providers have the same idea of what you want, it's important to talk to everyone on your team. Then you know exactly what's happening and your service providers know exactly what you want. Remember that you can have these conversations at any time. Here are three steps to working with your team.

Step One: Let everyone know who is on your team

To make sure that everyone is included in the way that you want them included, it's important to be clear about your thoughts and wishes. Your service provider should have a conversation with you when you start to work with them. Ideally, it's a good idea to have this conversation early on. If this doesn't happen, you can start the conversation yourself at any time. Let them know who is on your team: for example, it may be your family doctor, your parents, a school counsellor, and a psychiatrist.

Step Two: Ask questions

Here are some important questions to ask when you talk with your service provider:

- Do you, your organization, or your agency have any policies (rules) around sharing information? Each service provider you see might have different rules, so it's a good idea to ask each one. Their rules will tell you how they share information and what they can do.
- What do I need to do if I want to share information with my team? Some service providers need you to sign a consent form (a form that tells someone else what you want).
- What will you tell my team? Remember that you don't have to share everything with everyone. If you don't want to share certain information with your family members, make sure you tell your service provider or write it on your consent form. For example: you can let your service provider talk to your family about your diagnosis and treatment without bringing up other things that you and your service provide talk about.
- What do I do if I no longer want to share information with someone on my team? You can take back your consent at any time, but your service provider may have a process to make it official, like a form.

Step Three: Bring it up as often as you want

- Don't be afraid to ask questions if you don't understand something or don't understand what a service provider needs. It's important to understand what's happening! Also, if you don't like how someone else is using your information, you have the "right to object." It means that you can speak up if you aren't happy with the way your information is being shared.

What if I don't want to include my family?

You don't have to share information with your family. In some situations, it might not be a good option for you. Remember that you can always start sharing information later on if the situation changes.

If you're worried about sharing information with your family, try talking with your service provider about your concerns. You may be able to come to an agreement that works for everyone.

You don't have to share all information with your family. You can decide what your service providers share with your family. You can let your service provider tell your family about your diagnosis and treatment but keep other details private. This is a good way to let your family help you while still protecting your privacy.

How can I manage my medical records?

Your service provider has to give you a copy of your records if you ask for them. If you don't agree with something in your records, you can ask the service provider to fix the problem. Rarely, service providers may charge a fee to make a copy of your records. In a few situations, service providers can't give you your records. This can happen if your records include personal information about another person or if they believe that give you your records may cause harm to you or someone else.

How can I request my records?

If you want records from a doctor or someone that you see privately, you just need to ask for your records.

If you would like records from a hospital (like during time in hospital or from a program you took at a hospital), you will likely have to fill out a form. Look up the hospital's Health Records Office or Privacy Officer for more information about the hospital's specific requirements. If you aren't sure what to do, check if the hospital has a patient advocate, patient navigator, or ombudsperson. They can help you figure out what to do next.

How can I make a complaint?

If you have a complaint against a doctor's office, you can make a complaint to the College of Physicians and Surgeons of British Columbia. You'll find their website at www.cpsbc.ca. If you have a complaint about a hospital, you can contact the Patient Care Quality Office for your health authority. You'll find a list of health authorities at www.health.gov.bc.ca/socsec.

You can also make any privacy complaint to the Office of the Information and Privacy Commissioner. You'll find their website at www.oipc.bc.ca.

Where can I go for help?

The Office of the Information and Privacy Commissioner of British Columbia makes sure that everyone follows privacy laws. The 'For the Public' section of their website has a lot of information on your rights, how to make a complaint, and where to go for more help. Visit www.oipc.bc.ca.

The People's Law School offers education and information on many different legal concerns. They can also refer you to other resources that can help. Visit www.publiclegaled.bc.ca.

This project has been initiated and funded by the Province of British Columbia

BRITISH COLUMBIA