Records management guidelines:

Protecting privacy for victims/survivors of violence

ENDING VIOLENCE Association of BC

Fourth Edition | 2022

Please note:

If you are viewing the electronic version of these *Records Management Guidelines*, all the headings in the Table of Contents are hyperlinked to the listed page. The bookmarks tab (on the left hand panel in Adobe Acrobat reader) can also help you navigate through the document. Website URLs and email addresses in the document are also hyperlinked if you hover over the text.

Disclaimer:

This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization.

For more information about the Ending Violence Association of BC, visit **www.endingviolence.org**.

ENDING VIOLENCE
Association of BC

Acknowledgements

These guidelines update the 2006 *Records Management Guidelines*. The Fourth Edition (2022) was revised by Rachel Barsky, B. Journ., J.D., with assistance from Kristi Yuris, Kate Rossiter, and Laura Woods at the Ending Violence Association of BC (EVA BC). We are grateful to Madeline Neufeld (Limestone Learning Inc.) for copy editing and Chantal Lancaster (blacmao) for assistance with layout and design.

A number of experts from various sectors contributed to the original guidebook and to revised editions developed by the Ending Violence Association of BC (formerly BC Association of Specialized Victim Assistance and Counselling Programs) and the BC Society of Transition Houses (formerly BC/Yukon Society of Transition Houses). We gratefully acknowledge these sources for their expert assistance and wish to specifically recognize Gisela Ruebsaat and Tracy Porteous for their significant contributions to the first three editions of these guidelines.

Earlier editions of the *Records Management Guidelines* (1995/1996, 1998, and 2006) were developed with funding from BC's Ministry of Women's Equality, Ministry of Public Safety and Solicitor General, and Ministry of Community Services. The *Records Management Guidelines* (herein "*Guidelines*") were updated in 2022 with a Recruitment and Retention Training grant from BC's Ministry of Social Development and Poverty Reduction.

Table of contents

I. Introduction

What are records management guidelines?

Records management guidelines are a series of principles and suggested approaches. They serve as a guide for creating, updating, storing, releasing, and destroying client records.

Who are these guidelines designed to assist?

These guidelines are for staff and board members of agencies funded by the Ministry of Public Safety and Solicitor General (MPSSG) and operating under funding contracts in the following areas under the Ending Violence Association of BC (EVA BC) provincial umbrella:

- Community-Based Victim Services programs
- Stopping the Violence Counselling programs
- Stopping the Violence and Multicultural Outreach programs

If you work in a multipurpose agency, your agency may deliver additional programs not listed above. These guidelines were not specifically designed to assist in managing records for other programs. However, the *Guidelines* could be adapted for that purpose, subject to contract requirements. If you have questions regarding record-keeping requirements for a program not listed above, contact the Director/Manager of Information and Privacy for the funding ministry.

BC Society of Transition Houses (BCSTH) member programs, including transition houses, second- and third-stage houses, safe homes, and Prevention, Education, Advocacy, Counselling and *Empowerment (PEACE) programs, are encouraged to review the BCSTH Legal Toolkit: General Information about Legal Issues and Court Matters in British Columbia* (BC Society of Transition Houses, 2016).

How should I use these guidelines?

The *Guidelines* are organized or grouped according to frequently asked questions related to privacy protection.

Your agency or program can use these *Guidelines* as a component of your in-house privacy policy or as a template to develop your in-house policy. The background information included in this document can also be used as a sourcebook for best practices and further information.

Why are records management guidelines needed?

Agencies that work with victims/survivors are often privy to highly personal information about their clients. These agencies also deal with cases in which the chances of criminal or civil litigation are fairly high. In the past, in prosecutions involving charges of sexual assault or violence in intimate partner relationships, the victim's/survivor's personal history was often the focus of the case. The *Canadian Charter of Rights and Freedoms*, the *Criminal Code*, and provincial privacy laws all include provisions designed to protect privacy rights. These *Guidelines* help to ensure legal rights are respected by those working with victims/survivors and by those who administer laws.

Agencies also respond to high-risk situations. A complex web of laws and standards must be considered to help protect these agencies against legal liability. These include:

- The introduction of the provincial *Personal Information Protection Act* in January 2004.
- Amendments to BC's Freedom of *Information and Protection of Privacy Act*.
- Amendments to Part 5 of the *Child, Family and Community Service Act* that deal with freedom of information and protection of privacy.
- Amendments to the *Criminal Code* restricting access to records regarding victims/survivors in sexual offence cases.
- The requirement by some funding ministries that programs or agencies adhere to American accreditation standards, including standards related to record keeping.
- The requirement by some funding ministries that program or agency practices be audited by American accreditation bodies.
- Privacy advocates' concerns that Canadian private sector privacy laws are not strong enough to withstand the American *Patriot Act*, which gives the U.S. government broad powers to access personal information.
- The removal of the limitation period in civil cases for legal claims related to sexual assaults.
- The increased reporting of historical sexual abuse cases to police.
- The increased number and complexity of sexual and spousal assault cases being handled by community-based agencies.
- Defence counsel allegations of "false memory" in sexual assault/abuse cases.
- Requests for community-based agencies to disclose confidential client files or records in civil and criminal sexual assault cases.
- Requests for community-based agencies to disclose confidential client files or records in family law cases.

- Requests for community-based agencies to give evidence to help establish victims'/survivors' claims for damages in civil sexual assault cases.
- Requests for community-based agencies to verify their actions or interventions in cases where former clients have committed suicide or harmed someone else—for example, where there has been a Coroner's Inquest or a negligence lawsuit filed by grieving friends or relatives.
- High-profile cases, such as *R. v. Carosella* (1997), where agency record-keeping practices and the shredding of client records have been reviewed by the courts.
- High-profile cases where agency staff have successfully claimed that client records should be privileged or kept confidential.
- The need, indicated by many service providers, to encourage consistent record-keeping practices across the province.

How can record keeping help community-based agencies?

Records management guidelines can help agencies and service providers to handle and process information in a way that respects the client's confidentiality and acknowledges the organization's need to document the services it provides. Appropriate record keeping can help community-based agencies to document that they have obtained informed consent from their clients and protected the confidentiality of their clients' records.

Appropriate record keeping also helps agencies to document their actions, maintain consistent services among staff members, protect staff members against claims of improper behaviour, document that staff have satisfied legal or statutory reporting requirements, and determine appropriate retention periods for client records, among other things.

The Ministry of Public Safety and Solicitor General funds legal representation for any victim/survivor whose records are subject to an application for production in sexual offence proceedings under the Criminal Code. To apply, victims/survivors can contact Legal Aid BC.

If you or your agency are faced with a lawsuit related to your handling of a client's case, or you are asked to appear as a witness or provide evidence in a criminal or civil case, consult with a lawyer. If cost is a concern, consult with Legal Aid BC or your contracting ministry, or request that a private lawyer volunteer time for your agency or give a discounted rate.

What other sources of information should I consult?

Laws and policies

Legal and policy frameworks in this area are evolving rapidly. Agency staff responsible for policy must update themselves, their co-workers, and their board members regularly, particularly with regard to the following legislation and standards:

- BC's P*ersonal Information Protection Act* [provides privacy protections that apply to most businesses and non-profit organizations]
- BC's *Freedom of Information and Protection of Privacy Act* [deals with access and privacy issues related to records under the custody or control of public bodies]

- Canada's *Privacy Act* [contains privacy protections that apply to the RCMP and federally regulated businesses such as banks, railroads, and telecommunications firms]
- BC's *Child, Family and Community Service Act* [Part 3 establishes reporting requirements for suspected child abuse; Part 5 deals with access and privacy issues related to records governed by the *Act*]
- BC's *Infants Act* [Part 2 deals with a minor's consent to healthcare]
- Canada's *Criminal Code* [sections 278.1–278.9 deal with the production of records in sexual offence proceedings]
- Supreme Court of Canada decisions interpreting criminal and civil law privacy protections: *R. v. Grant* (2015), *R. v. Quesnelle* (2014), *R. v. Shearing* (2002), *R. v. Mills* (1999), M(A.) *v. Ryan* (1997)
- Supreme Court of Canada decisions setting limits on cross-examination of sexual assault complainants: *R. v. R.V.* (2019), *R. v. Lyttle* (2004), *R. v. Osolin* (1993), and *R. v. Seaboyer*, (1991)
- Records management guidelines developed by other ministries that fund your agency
- The B.C. *Handbook for Action on Child Abuse and Neglect* [2017 edition is available on the Ministry of Children and Family Development website]
- Ministry of Children and Family Development Best Practice Approaches: *Child Protection and Violence Against Women* (May 2014) [deals with best practices for child protection social workers; available on the Ministry of Children and Family Development website]

The Personal Information Protection Act

In January 2004, the *Personal Information Protection Act* (PIPA) came into force in BC. It is a provincial law that establishes rules about the collection, use, and disclosure of personal information. Under PIPA, "personal information" means information about an identifiable individual. PIPA contains safeguards designed to protect the privacy of the personal information that is collected by private businesses and non-profit organizations.

Which agencies or programs must follow PIPA rules?

PIPA applies to all private sector organizations in BC, including non- profit organizations. PIPA does not apply to agencies or programs already covered by BC's *Freedom of Information and Protection of Privacy Act* (FIPPA).

Whether your program is covered by FIPPA or PIPA will depend on the wording of your contract with the funding ministry. If the wording of the contract suggests that your records are under your agency's or program's "custody or control," then PIPA rules apply. If you are uncertain about this, see below for further information, including an overview of the factors affecting who has "custody or control." You may also wish to contact the contract manager at your funding ministry.

To date, the wording of the Community-Based Victim Services program and Stopping the Violence Counselling program contracts has been interpreted in the field to indicate that these programs have "custody or control." This means the programs are governed by PIPA. As contract wording can change from year to year, we recommend that you review

the contract terms again each fiscal year. Under FIPPA, it is the wording of the funding contract in force when the records were created that determines whether that act applies.

If your agency runs more than one program, some records may be governed by PIPA and others by FIPPA. Each individual contract should be reviewed to determine who has "custody or control" of the records.

Consent requirements under PIPA

If covered by PIPA, your agency must obtain consent before collecting, using, or disclosing personal information. There are limited instances in which your agency may collect information about an individual without consent, set out in section 12 of PIPA. These include situations where:

- Collecting the information is clearly in the individual's best interests and there is no timely way to obtain their consent.
- The information is needed for the individual's medical treatment and the individual cannot give consent.
- It is reasonable to expect that consent would compromise the availability or accuracy of the information, and it is reasonable to collect the information for an investigation or proceeding.
- The information is being collected at a public sporting event, a performance, or a similar event where the individual appears voluntarily (in which case consent is not required).
- The payment of a debt to a credit reporting agency is involved.
- Your agency is assisting the agency/organization that obtained consent with its work.
- Other circumstances outlined in section 12 of PIPA apply.

The Freedom of Information and Protection of Privacy Act

This *Act* applies to public bodies, including government ministries, and to some of the records held by community-based agencies contracted by government.

The Child, Family and Community Service Act

Part 3 of the *Child, Family and Community Service Act* (CFCSA) requires any person who has reason to believe that a child needs protection to report to a director of the Ministry of Children and Family Development (MCFD), or to a designated representative if the child is Indigenous (i.e., a local Delegated Aboriginal Agency). For Indigenous children (e.g., First Nation, Nisga'a, Treaty First Nation, Métis, Inuit), the director will contact the appropriate representative.

Part 5 of the CFCSA deals with information and privacy issues. If your agency is or was once funded by MCFD, Part 5 of the CFCSA may apply to records you have created to serve clients, such as counselling records or other ongoing service records. Review your contract language for clarification. Amendments to CFCSA Part 5 came into force in January 2006. The result is that there is now greater consistency between information sharing practices under the CFCSA and FIPPA.

Does FIPPA apply to your agency's records?

The following factors may be considered to determine whether your records are under the ministry's custody or control:

- Is there anything in your agency's funding contract that specifies that the records are under the ministry's control?
- Does the ministry have a right under the funding contract to review the records which relate to the services being provided?
- Does the ministry have a contractual right to have a say in the content, use or disposition of the records?
- Were the records created by the ministry?

Accreditation standards

A number of agencies, particularly those who receive funding from MCFD, are considering accreditation or have already been accredited based on their implementation of specific standards. Adherence to these standards is monitored by external accreditation bodies—namely, the Council on Accreditation (COA) and CARF International (CARF). The COA's and CARF's standards include a number of references to records management and confidentiality.

In many cases, an agency's guidelines will already be consistent with basic accreditation requirements. In other cases, the guidelines may be worded somewhat differently to take account of Canadian laws and recommended approaches based on long-established local practices.

Professional standards or codes of ethics

If you are a member of a professional association, such as the BC Association of Clinical Counsellors or the Canadian Art Therapy Association, you may be ethically required to follow certain guidelines regarding client confidentiality and records management.

Your contract with the provincial government or other funders

Your contract should also be consulted. It may require specific documentation practices or the maintenance of certain client records.

If you need more information about either PIPA or FIPPA, contact the Privacy Helpline by phone at 250-356-1851 or by email at privacy.helpline@gov.bc.ca.

II. Basic records management requirements and privacy principles

Obtain consent

Consent should be obtained for the collection, use, and disclosure of an individual's personal information. There are exceptions to this requirement, including employee personal information and information needed in an emergency. The *Personal Information Protection Act* (PIPA) considers consent to be given when a person, knowing the purpose of the collection of their information, provides that information willingly. You should therefore tell the person from whom the information is being collected, either verbally or in writing, before or at the time of collection, why this personal information is needed, how it will be used, and the limits to confidentiality e.g., information may need to be shared with other staff or board members, or there may be a legal obligation in certain circumstances to release it without client consent).

Decide whether consent will be oral or written

Consent should be in a form appropriate for the type of personal information involved. Express written consent is often desirable. Consider what is reasonable for the individual, the circumstances of collection, your proposed uses or disclosures of the information, the sensitivity of the information, and whether you may need to prove that the person consented. These *Guidelines* recommend that written consent be included as part of an intake form.

Determine the scope of information you need

Personal information should be collected only for reasonable purposes, and only the information that is reasonable for those purposes should be collected. Collect information directly from the individual, unless PIPA permits otherwise or the person agrees to someone else giving the information to you. Programs using these *Guidelines* will already meet this requirement.

Set limits on the use of the information you have collected

Use and disclose information only for the purpose for which it was collected, unless the person consents or PIPA permits release without consent.

Allow individuals to access information that pertains to them

On request, provide an individual with information about the existence, use, and disclosure of the personal information you have collected about them. If you receive such a request, respond within 30 days. Provide the individual with access to the requested information, unless PIPA excuses you from doing so. For example, you can refuse access where release of the information would harm an investigation or where disclosure would harm someone else or result in the disclosure someone else's personal information. On request, correct information that is inaccurate or incomplete. Access to personal information by the person who provided it is also addressed in these *Guidelines*.

Keep records secure

Ensure that the personal information you have is secure. Refer to the recommendations contained in these *Guidelines*.

Be able to justify the length of time for which you keep the information

PIPA requires that records be kept for a *minimum* of one year. After that, keep the information only for as long as is reasonable for business or legal purposes. If you are using the retention period recommended in these *Guidelines*, you won't need to change your policy. Use care in disposing of or destroying information.

Develop a personal information or confidentiality policy, and designate someone as a Privacy Officer

Designate someone in your organization who will be responsible for ensuring your organization complies with PIPA. That person will be responsible for developing and implementing a privacy policy and making sure it is working effectively, as well as responding to inquiries and complaints regarding information management. Make the details of how your organization manages of personal information available on request.

Respond to concerns

If someone makes a complaint about how your organization handles personal information, try to resolve the complaint quickly and fairly.

III. Goals of the records management guidelines

1. **To build trust between clients and service providers** by outlining record-keeping practices that ensure clients are informed of the practical and legal limits to privacy.
2. **To help service providers understand the practical and legal limits to privacy** so that they can inform clients of these limits before a crisis develops.
3. **To assist community-based agencies** if their staff are required to disclose client records in the context of a civil or criminal prosecution.
4. **To ensure that client confidentiality is protected to the greatest extent possible** in instances where client records are disclosed pursuant to legal requirements.
5. **To assist agency staff in maintaining credibility and refreshing their memories** if they are required to appear as trial witnesses and be cross-examined by defence lawyers in the context of a prosecution some time after agency service was provided.
6. **To help ensure that agency and staff record-keeping practices are consistent** with legal, professional, and ethical requirements.
7. **To reduce an agency's risk** of legal liability.
8. **To assist agency staff and board members** in the development of their own internal record-keeping policies.

IV. The records management guidelines

The intake process

1. How can I protect the identity of a prospective client?

Background

The very act of seeking help from a Community-Based Victim Services program, or other program, may put a victim/survivor in jeopardy if this information is inadvertently disclosed.

- If personal information is mailed with an agency logo on the envelope, and the recipient lives with the offender, the offender may open the mail and review private material. This could include sensitive information that the offender might otherwise need a court order to access. This information might be used to attack the victim's/survivor's credibility in court.
- If the victim/survivor once stayed at a transition house and is later involved in a custody dispute, the fact that they lived at the house with their children may be used to suggest they are not a capable parent.
- Where the situation involves a violent offender, and the offender finds out the victim/survivor is receiving support services, agency staff and the victim/survivor may be at increased risk of harassment or violence.

Guidelines

- → The agency should not disclose the identities of clients who have requested agency services, except where a client has consented or the agency is legally required to do so.
- → The principle of non-disclosure applies to board members and all staff, including supervisory (employed or contracted) and administrative support personnel, as well as volunteers.
- → The requirements of confidentiality extend to all records created or maintained by an agency, including intake records and forms filled out by prospective clients.

- → The obligation to maintain confidentiality remains indefinitely, even when the agency no longer has contact with the client and/or the file is closed.
- → The obligation to maintain confidentiality remains indefinitely, even after a staff member, volunteer, or consultant ceases to be connected to the agency.

Effective documentation practices

- Establish confidentiality policies that clearly spell out who does and does not have access to different kinds of information, as well as why each kind of information is needed. For example, an in-house policy could set out safeguards regarding access to client information by clinical supervisors and the rare circumstances under which a board member would have access to client information.
- When staff or volunteers are first hired or taken on by your agency, provide them with formal orientation on the principles of confidentiality and related policies, and document the fact that you have provided this training.
- Obtain oral consent from each prospective client before mailing, emailing, or faxing intake forms to them or contacting them at home, and document the fact that you have obtained this consent.

2. Who prepares the intake record?

Guidelines

- → Whenever possible, intake records should be prepared by staff who have received training or orientation on the principles of confidentiality.
- → Whenever possible, paid agency staff should review records prepared by volunteers.

3. What client information should I include in the intake record?

Background

Agencies provide a variety of services, including justice system information and practical support, court and witness preparation, emotional support, counselling, and emergency shelter. At the intake stage, the type of client information collected and the process followed will vary depending upon the specific service being requested. Intake will generally include some type of screening to ensure that a client is safe and to determine whether they are eligible for assistance.

Agencies seeking accreditation may be asked to conduct “intake assessments” in order to satisfy accreditation standards. For example, Standard 4 of the COA’s Domestic Violence Service Standards (2021/Canadian organizations) requires an organization to conduct a full assessment with each client, including:

Screening and informing the client about the compatibility of their request with the organization's services, as well as what services will be available and when.

- Gathering information about the client to identify critical service needs and determine whether there is an urgent or emergency situation, and—if the organization cannot provide the necessary services—referring the client to the appropriate resources.
- Assessing the client's needs in terms of medical and dental care, legal assistance, clothing, shelter, and food, as well as the safety and risk factors for them, their children (if applicable), and other family members.
- Engaging in safety planning to develop a comprehensive plan that is regularly re-evaluated to ensure it meets the client's needs.

General standards sometimes recommend that detailed information be gathered as part of this type of intake process—for instance, a medical and/or psychosocial history of the prospective client. This type of information may not be applicable to the initial intake if the client is only requesting court accompaniment or information about the justice system.

Whether an agency is striving to satisfy standards set by an external accreditation body or developing its own in-house policy regarding intake, certain basic principles apply. Only information necessary for the provision of the requested services should be collected. Additionally, each prospective client's consent should be obtained before any information is gathered and before it is used or released.

If the agency is in the process of accreditation, it may need to negotiate with the accreditation body to ensure that intake forms are tailored to meet the information and service needs of the specific program and the privacy needs of the specific client group.

Guidelines

- → Agency staff should only collect information that is necessary to determine the appropriate service and to deliver the specific service being requested.
- → Collection of information should occur at the time it is needed to deliver the service. Some multi-service agencies use both a generic and a secondary intake form for this reason. The generic form requests only basic information necessary to determine which service a client requires; then, once the client is referred to that service, the secondary intake form is used to collect the information needed to effectively deliver that service.
- → Agency staff must obtain the prospective client's written consent before collecting any personal information about them.
- → Agency staff should explain how they intend to use the personal information being collected and then obtain the client's written consent to use the information in that way.
- → Agency staff should create a written timeline outlining approximately how long it will take to complete intake/assessment and deliver services.
- → If the prospective client is eligible for specific services, agency staff should obtain their written consent to receive those services and inform them if delivery of services will be delayed because of a waitlist.

- If the prospective client is not eligible for services, agency staff should document any referrals made and/or information provided regarding other suitable agencies or programs.
- The agency must designate someone responsible for privacy compliance. This person's title and contact information should be provided to the client either at intake or upon request.
- In general, the person receiving service—or their legal guardian—should be the primary source for the information being collected. In some circumstances, agency staff might consider using collateral sources of information. For example, if immediate safety concerns are an issue, agency staff should consider whether coordinating with other involved agencies is necessary to develop an effective safety plan. In such instances:
  - Police or court services may have critical information about the existence of protection orders with conditions restricting an offender's access to a victim/survivor or use of firearms.
  - Corrections may have information about the offender's pending release from custody.
  - MCFD personnel may have information about measures in place to protect any children involved.
  - In cases of high-risk domestic violence, it may be appropriate to share information with other service providers to review and manage risk as part of an Interagency Case Assessment Team (ICAT).

  Coordinating with other agencies can aid in identifying risk factors and finding ways to minimize them.
- In general, any information sharing with other agencies should be done with the client's consent.
- The agency should document any actions taken in response to identified safety concerns.

Effective documentation practices

- At the intake stage, document:
  - any immediate safety concerns
  - information necessary to determine eligibility for service
  - any referrals made
  - the immediate information and practical support provided
  - the intended plan of action (including an immediate safety plan, if necessary)
- If the prospective client is involved in a violent relationship, has been sexually assaulted, or otherwise fears for their safety, collect and document any information necessary to develop an immediate safety plan. Questions like the following should be asked:
  - Where does the offender live?
  - Does the offender have access to the victim/survivor?
  - Does the offender know that the victim/survivor is seeking services such as counselling?

/ Continued on next page

  - What is the offender's history of violence? Has it included strangulation? Sexual assault?
  - Has a protection order been issued?
  - Has the offender made threats?
  - Does the offender have a history of coercive controlling behaviour?
  - Are children at risk?
  - Does the offender have mental health concerns? Have they expressed suicidal ideation?
  - Does the offender own or have access to firearms/other weapons?
  - Is it safe to contact the victim/survivor at home? By cell phone? By email?
- If the prospective client is eligible for service, obtain their written consent for service.
- If the client is a child (aged 18 or under), determine who has the legal right to enter into the contract of service and obtain the written consent of that person. (See Part V of these *Guidelines* for information on consent issues related to child clients.)
- If the client or their representative has difficulty understanding a written consent form, obtain oral consent and document the fact that you have done so.
- On intake forms, ask specific "yes/no" questions wherever possible. Avoid the use of open-ended questions. Consider having agency staff fill out these forms rather than asking clients to do so themselves.
- Use discretion when gathering and recording information related to:
  - family, medical, or psychiatric history
  - drug or alcohol use

  Some agencies use a checklist. The checklist indicates whether certain issues have been addressed—for example, the need for a referral—but does not include detailed psychological information about the client.
- Have the intake record specify which type of service the client is requesting and has consented to—for example, criminal justice system information and practical support, witness preparation, emotional support, crisis counselling, individual counselling, or group counselling.
- Have the intake record indicate whether the client has reported the assault or abuse to police, and/or whether they are involved with any pending legal proceedings related to the violence they have suffered.
- Have the intake record outline, in writing, the limits to client confidentiality. (See Part IV of these *Guidelines* for more information on the intake process, including how and when to advise clients about the limits to confidentiality.)
- Have the intake record dated and signed by the client—or read it out loud and have them summarize its contents, then document the fact that you have done so.
- Have the intake record include an agency waiver of liability developed in consultation with a lawyer.

Coordinating the information flow in high-risk cases

System-based agencies such as police and Crown have limits on what information they can share with a victim/survivor.

Exceptions generally apply in high-risk cases.

To avoid confusion in a crisis, consider developing local protocols with other agencies to guide information sharing and safety planning. This is what occurs via Interagency Case Assessment Teams (ICATs). An ICAT is a partnership of local agencies, including police, child welfare, health, social services, victim services, and other agencies. ICATs respond to referrals of suspected highest risk cases of domestic violence with a goal of increasing safety.

ICATs are not investigative bodies, but they do review and manage risk in high-risk cases. ICATs complement local domestic violence coordination committees, Highest Risk Domestic Violence Teams (HRDVs), and Domestic Violence Units (DVUs) in strengthening the local domestic violence response.

Details about these groups, how they work together, how they can share information, the local protocol for reviewing highest risk domestic violence cases, and more are set out in EVA BC's publication "Interagency Case Assessment Teams Best Practices: Working Together to Reduce the Risk of Domestic Violence" (2017), which is the second edition of the ICAT Best Practices Manual. To request a copy of this manual, please contact EVA BC's Community Coordination for Women's Safety (CCWS) program at **ccws@endingviolence.org**.

4. How should consent to services be documented where the prospective client does not read or speak English?

Guidelines

- → If the prospective client has difficulty understanding a written consent form because English is not their first language, the service provider should obtain oral consent and document the fact that they have done so.
- → If the prospective client does not understand enough English to be able to provide oral consent, the service provider should involve an interpreter. The interpreter must sign a confidentiality agreement, and the service provider must document the role the interpreter has played.

Effective documentation practices

- Consider translating agency intake forms to reflect the makeup of the community being served.
- Consider providing training on the need for safety and confidentiality to those you intend to use as interpreters.

5. How should consent to services be documented where the prospective client does not have the mental capacity to make decisions about their care?

Background

In this situation, your prospective client will likely have someone who is empowered to act as their legal representative. This is the person who should sign any agency consent forms. The legal representative could be:

- a committee appointed under the *Patients Property Act*
- a representative authorized to make decisions, pursuant to a representation agreement made under the *Representation Agreement Act*

The recommendations in Part IV of these *Guidelines* apply in situations where the prospective client is an adult. If the prospective client is 18 or under, refer to Part V of these *Guidelines* for records management issues related to clients who are children.

Guidelines

- → If the prospective client lacks the capacity to consent to services, the service provider should determine who has the legal authority to enter into the contract of service.
- → The service provider should request copies of the documents authorizing the legal representative to make decisions on behalf of the prospective client.
- → The written consent of the legal representative must be obtained.
- → If the service provider is concerned about the prospective client's legal capacity and they have not identified a legal representative (i.e., a lawyer or committee), the agency should take action only to the extent necessary to protect the person until a legal representative can be appointed.

6. How can an intake form be used to address the needs of clients who face particular discrimination?

Background

This is a sensitive area. Collecting information about someone's unique personal characteristics (such as their racial or cultural background) can help agency staff to design an appropriate service plan. It can also help to ensure that the person seeking service is referred to a program that is designed to meet their specific needs. It may be important for a service provider to be aware of particular physical or health-related needs during the intake process for a client with a physical or mental disability.

On the other hand, collecting this type of information can be very problematic. It can have the unintended consequence of stigmatizing the person seeking service or putting them at greater risk, particularly if the information must later be released to unsympathetic third parties.

In the justice system context, it is also important to consider historic and ongoing concerns about racial profiling and systemic bias and discrimination. Based on their own past

experiences, certain groups may justifiably assume that information about their personal characteristics will be used inappropriately by service providers to fit them into a predetermined category rooted in stereotype. For instance, Canada has a long history of systemic racism against Indigenous persons (Truth and Reconciliation Commission of Canada, 2015), which is reflected in the disproportionate rates of Indigenous children in care and the overrepresentation of Indigenous peoples in custody.

The needs of funders and accreditation bodies must also be considered. Funders may want to know the makeup of a service provider's clientele, as this information may indicate a need for additional funding to serve a particular group. Some accreditation bodies have specific standards that apply to intake or assessment of people with special needs. For example, the COA standards on intake, assessment, and service planning require that:

Victims/survivors participate in an individualized, culturally and linguistically responsive assessment that is:

- Completed within established timeframes;
- Updated as needed based on the needs of persons served; and
- Focused on information pertinent for meeting service requests and objectives. (Council on Accreditation, 2021, CA-DV 4.05, https://coanet.org/standard/ca-dv/4/)

Guidelines

- → General guidelines regarding intake apply.
- → The service provider should ensure the prospective client knows the agency's policy regarding confidentiality and release of information to third parties before collecting any information about their personal characteristics.
- → The prospective client should be invited to inform the service provider of any special needs they have that might be pertinent to the service being providing and that they feel the agency should know about. This step should be documented.
- → If the prospective client identifies any special needs, or such needs are otherwise identified through the intake process, the service provider should document any referrals made or other actions taken to address those needs.
- → With respect to prospective clients who may have physical or mental disabilities, the service provider should identify and document health and safety issues relevant to the services being requested, and document the possible need for additional support or reasonable measures to achieve accommodation.
- → Agency staff should consider working with community leaders representing the groups involved to design an intake process that balances the need for safety- and health-related information with the need to respect the dignity and privacy of the prospective client.

7. How and when should I advise agency clients about the limits to confidentiality?

Guidelines

- → Agency staff should advise clients about the limits to confidentiality at the time when services are first being requested.
- → If more than one type of service is being provided within the same agency—for example, emergency shelter in a transition house, and then individual or group counselling—the limits to confidentiality should be reinforced by agency staff at each stage (in this case, at intake and again during the first counselling interview or session).

Effective documentation practices

- Include in your agency's application for service, or other intake forms, a statement that client information will be kept confidential, subject to three exceptions:
  - Cases where a child is in need of protection, as set out in section 13 of the CFCSA.
  - Cases where a client indicates that they are likely to be a danger to themself or others.
  - Cases where agency staff are compelled by court order to release client information. (See Part IV of these *Guidelines* for information on practices associated with sharing client information and the release of client records.)
- Have the prospective client sign a confidentiality agreement before the rest of the intake forms are filled out.
- Have the prospective client sign a statement that says they have been informed of the exceptions to the basic principle of confidentiality. If the prospective client cannot read the written statement, or otherwise has difficulty understanding its contents, read it out loud and explain it, and document the fact that you have done so. If the prospective client has difficulty understanding English, use an interpreter.
- If a client receives ongoing services, have the service provider remind them during the first face-to-face meeting of the limits to confidentiality that were outlined at intake. Give the client a written handout that summarizes the exceptions and outlines the actions the service provider would take in those situations.

8. When should I open a client file?

Guideline

- → A client file should generally be opened when:
  - The client has requested a specific service,
  - Their request has been documented as part of the intake record,
  - They are no longer on a waiting list, and
  - They have begun to receive the services requested;

or when:

- Legal proceedings involving the client are underway or expected, or
- There is a greater-than-usual risk of agency liability in relation to the client.

Effective documentation practices

- Open a file immediately if the intake record indicates a potential need to disclose client information—for example, where the client appears to be suicidal or a danger to others, or where a child is in need of protection.
- Open a file immediately if the intake record indicates that the client is already involved in or may soon be involved in legal proceedings related to the violence they have suffered.
- Establish a system that allows for retrieval of the file and for the link-up or merging of the intake record and the service record if the client later receives counselling from your agency.

9. What information should I include in the service plan?

Background

Service plans are an important part of the documentation process. Generally, a plan is developed with the full participation of the client. A service plan can help the client better understand:

- The benefits and risks of different service options.
- How the agency can support the achievement of desired outcomes.

Some accreditation bodies, such as the COA, require the development of written service plans.

Guidelines

→ The agency should develop a written service plan for each person or group served.

→ The service plan should be based on the findings of the intake/assessment process and should include:

- Information about the services being provided, including who is providing them.
- Service goals.
- Desired outcomes.
- Proposed strategies to address specific needs.
- Approximate timeframes, with urgent or crisis cases identified for immediate attention.

→ The service plan should be signed by the client and/or their legal guardian at the start of service and any time a significant change is made to the plan.

Documenting the services provided to clients

1. Which records should be included in client files?

Guidelines

- Generally, records created or produced by agency staff belong to the agency. It is the agency's responsibility to maintain and manage these records. (In certain cases, an agency's funding contract may require that the funding ministry have custody or control over the records. If so, the FIPPA or the CFCSA may apply. If staff or board members are unclear as to which *Act*—if any—applies, the funding ministry's Director/Manager of Information and Privacy should be consulted.)
- Generally, materials or products created or produced by the client—such as diaries or artwork—are not the property or responsibility of the agency and should not be kept in the agency's client file. If they were to be kept in the agency's file, they could be subject to discovery in court and potentially used against the client.
- Written statements made to police are generally prepared by the client. It is recommended that such statements not be included in the agency's client file. Maintaining and managing these documents is not the responsibility of the agency.
  - Be aware that information in the agency's client files could be discoverable and could ultimately be disclosed to an offender or a third party. For this reason, it is advisable to collect the minimum amount of information needed by the agency to provide services. Not all details (such as observations about the client's mental wellness or substance use) or subjective assessments need to be included in the client's file.

Effective documentation practices

- Retain in the client file all records produced or maintained by agency staff. This might include:
  - intake records, such as applications for service, intake forms or checklists, Release of Information agreements, or consent forms
  - safety plans
  - service plans
  - Crime Victim Assistance Program application forms
  - completed Victim Impact Statements
  - completed Statement on Restitution forms
  - letters of advocacy written on behalf of the client
  - progress or case notes on individual sessions
  - reviews of progress made during sessions
  - completed assessments
  - miscellaneous reports
  - documentation of referrals made
  - documentation of interventions, in cases where there are legal reporting requirements (e.g., suspected child abuse; client indicates they are a danger to themself or others)
  - termination summary notes

/ Continued on next page

- Strongly encourage clients to retain personal materials they have created, such as diaries, letters, or artwork. These items should only be included in the agency's client file where necessary for effective service delivery.

2. Are there situations where client records should be kept in more than one file or separated out within a file?

Background

Different types of service require the collection of different types of information. For example, information about court dates, appointments with police and Crown, or case status might be collected in order to provide justice-related information or practical support. On the other hand, more detailed information about a client's personal history might be collected in order to provide emotional support or counselling. Information related to any immediate health concerns or current medications might be required to safely provide emergency housing.

If the client's file makes no distinction between information collected for the purposes of assisting with a court case and information collected for other purposes, such as providing counselling, then a court reviewing this file may interpret *all* the information as relevant to the legal process and may release it all to defence counsel. This may not be in the best interests of the client.

Guideline

→ Whenever possible, client files should be set up in such a way that information related to one type of service is clearly stored in a separate part of the file from information related to another type of service (e.g., the justice-related information should be kept separate from the counselling or service delivery information). Electronic records on agency computers should also be stored separately based upon the type of service provided.

Effective documentation practice

- If your client's records span the life of two or more funding contracts that contain different language regarding custody or control of client records, consider storing the records that are subject to FIPPA in a separate file or in a separate part of the same file from those that are not. Label the two (or more) files or parts of the file accordingly.

3. What information should be included in the service record?

Background

The main purpose of the service record is to enable staff to do their jobs. The record can also help verify actions taken by staff or agencies in cases where questions are raised about their actions. Circumstances may arise in which service records such as case notes, or the complete contents of a case file, must be released to a third party whose interests may conflict with the client's or the agency's. Given this possibility, every service record should be written so as to protect client confidentiality to the greatest extent possible. In preparing any part of the service record, be aware that documents cannot be edited or destroyed once they have been subpoenaed. Also be aware that certain aspects of the file—for instance, documentation of issues related to the client's memory—will be the subject of particular scrutiny if the file is disclosed in the context of a court case.

Some of the effective documentation practices listed below refer to "case or session notes." However, many of these practices are equally relevant to other documents included in the service record or counselling file, such as assessments or termination summary notes.

These *Guidelines* recommend that service providers use discretion when gathering and recording sensitive information about a client's psychiatric and/or medical history and consider using a checklist approach, as opposed to asking open-ended questions (see Part IV of these *Guidelines* for information on the intake process and what client information should be included in the intake record). It is also recommended that case notes be brief and succinct (see below). This approach is taken mainly because:

- Canadian privacy laws discourage the collection and/or recording of sensitive personal information unless it is absolutely necessary to provide a particular service.
- Litigation is fairly common in gender-based violence cases, and agency records can sometimes be inappropriately used to discredit a victim/survivor. This can be very traumatic for agency clients.

Agencies can negotiate with accreditation bodies to ensure that standards are applied and interpreted in a way that balances the need for information with the need for privacy.

Guidelines

- → The service provider should ensure that all recorded information is necessary to the delivery of the service.
- → Entries should be relevant to the needs of the client.
- → The client's full name should not be recorded in call/crisis logs, and the identity of the client should not be disclosed in email messages, even between staff.
- → Case notes should be brief. The service provider should note major topic areas discussed in the session—for example, "discussed feelings towards partner/spouse." Details of any specific symptoms should be kept brief—for example, "client is experiencing flashbacks or nightmares."
- → Generally, service providers should avoid documenting verbatim accounts of a session or putting quotation marks around a file note summarizing what a client said. If there is even a minor discrepancy between the quoted portion and what the client later reports to police or says in court, this can be used to challenge their credibility.

- → The service provider should document the methodology used and should record observations they have made, being careful not to be subjective. Their case notes should not attempt to document historical or legal truth.
- → Wherever possible, language used in case notes should reflect the client's experience. Service providers should avoid terms which suggest moral judgment, keeping in mind the ways case notes might be interpreted by uninformed or unsympathetic third parties.
- → Case supervision should be documented, and if a case file review has been done, it should include the supervisor's signature.
- → Agency policy should provide for regular screening of the service record for transitory documents such as post-its, reminders to staff, or general impressions. Provided there is a complete and accurate record of the service provided somewhere in the file, it is not necessary to keep every record that was created during the period of service. Rather, unnecessary documents—including electronic documents—should be removed from the file. Computer hard drives must be wiped clean or made unreadable. Paper records that are removed should be shredded. (See Part IV of these *Guidelines* for information on retention of client records.)
- → Once a particular set of records or a file is subject to subpoena, no material of any kind should be removed from it.

Effective documentation practices

Regarding the formatting of case notes:

- Keep case notes on a session-by-session basis.
- Write the case notes soon after each session.
- If handwritten case notes are later transcribed, the handwritten draft can then be expunged from the file.
- If the case notes were written during the session, this should be clearly indicated.
- Record the date of each session in the case note, sign and date it, and indicate who wrote it.
- Develop a common format for case notes and ensure that all agency counsellors use it.
- Develop a list of acceptable abbreviations used within the agency.
- Where information contained in the case file has been provided by a third party, indicate this in some way.
- Document or record on a need-to-know basis.
- Consider flagging or marking entries that may have legal significance.
- Write legibly and in ink.
- Prepare progress notes or summaries on a quarterly basis.

Regarding the content of case notes:

- Be brief. Note the major topic areas discussed in the session—for example, "discussed feelings towards partner/spouse." Be brief about the details of flashbacks.

/ Continued on next page

- Generally, avoid documenting verbatim accounts of a session.
- Document the methodology used.
- Avoid the use of guided imagery techniques or other interpretive techniques when working with someone who does not have complete memory.
- Avoid including your own subjective comments regarding a client's behaviour or emotions.
- Avoid including information about third parties.
- Do not use the case notes to make speculations about the client.
- Do not use the case notes to debrief or record your own emotional responses to the client or the case.
- Document the conclusion of services on a termination form.

4. What special confidentiality concerns arise in group counselling sessions?

Background

It is more difficult to maintain individual client confidentiality in a group setting. Also, it has been suggested by some—though, not proven—that a client's recollection of past abuse might be influenced by the flow of information or images coming from other group members. For these reasons, special considerations arise in the management of documentation for group counselling.

Guideline

→ Agency staff should obtain verbal or written agreement from those participating in group counselling that all matters discussed in the group will be kept confidential.

Effective documentation practices

- Advise group members that aspects of their private lives may be revealed in the group and that there are no absolute guarantees of confidentiality in this situation.
- Consider keeping separate sets of case notes for the group and for each individual member. The group record should not include information that could identify individual members of the group.

Physical security of client records

1. What steps can I take to protect the physical security of client records?

Guideline

→ Client records, including computerized records, should be protected from unauthorized access, duplication, or theft.

Effective storage practices

- Lock filing cabinets and limit access to areas where records are stored. Case records should not be left in a public area. When not in use, files should be returned to a secure area. Store paper records in locked and fireproof or fire-resistant cabinets.
- Avoid travelling with records. If it is essential to do so, take the fewest records possible based on what is needed, and be sure to obtain the necessary approval before removing the records from the office. If there are too many records to carry, send them to the destination via courier. Send only copies of the documents, rather than the originals.
- Maintain control over the storage, availability, and use of all computer storage media. Do not leave laptops or other mobile devices unattended. If this is not possible, store devices in a secure location such as a locked filing cabinet, room, or desk drawer. Avoid viewing records in public or at home—but if you must do so, ensure that your screens are not visible to others in public or to those in your home environment.
- Limit access to computer systems or networks that contain client records. Log off or shut down your device, lock its screen, and enable password protection, encryption, and other security measures discussed in Part IV of these *Guidelines* regarding the use of information technology to store or transmit client records and/or personal information.

Using information technology to store or transmit client records and/or personal information

1. How can I protect personal information that is stored electronically?

Background

Many agencies now store client files electronically. Others may be making this change to satisfy accreditation requirements. It is important to keep in mind that accreditation bodies may recommend or require the use of particular databases for storing records. They will also require security features, such as the use of passwords, firewalls, and up-to-date anti-virus protection.

Guidelines

- → Access to client personal information contained in computer databases should be password controlled. Only staff who must access to that information to perform their day-to-day duties should be granted their own password to do so. Limit password attempts. An “erase after X failed password attempts” capability can be added to devices, but a strategy for regular back-ups must be put in place first.
- → For staff working remotely, client personal information should be stored on a storage device such as a USB flash drive or portable hard drive rather than the hard drive of a laptop or home desktop computer. All portable storage devices should be password protected and encrypted.

Clients and their mobile devices

Some clients (especially in remote communities) may have limited access to high-speed Internet and mobile devices, and you should offer them low-tech options such as the use of a telephone. However, these days, more and more clients may use electronic devices to communicate. In these cases, ensure that the client understands that they are responsible for the security of their own device, even when communicating with your staff. Let them know about the potential risks associated with using their device in their home environment or using a shared device. Discuss with them where they could get help identifying signs that an abuser might be using spyware to monitor or control their social media accounts, text messages, or GPS location. The Peace Geeks Blog is a resource that includes steps the client can take if they think their device is being monitored (**https://peacegeeks.org/**).

- Staff should log off or shut down their devices when they are not using them. Devices should not be shared with other individuals.
- All computers should have up-to-date anti-virus protection and firewall protection. Screens should be locked, and devices encrypted. Electronic records containing sensitive personal information should be encrypted when they are taken out of the office, and location information should be limited. This means activating GPS only when needed, and disabling Bluetooth, Wi-Fi, and Near Field Communication (NFC) when not in use. Agencies should devise a list of apps that can be installed and how they should be installed, updated, and removed. Staff should receive guidance on how to mitigate risk by not clicking on suspicious links or spam messages and how to recognize suspicious sites. End-to-end encryption of communications is the gold standard.
- With large, multipurpose databases, software should be designed such that different staff members only have access to the parts of the database that relate to their duties. For example, administrators should not have access to counselling files or client intake records containing personal information.
- The agency should have a system for regular backup of digital records. Electronic backup should be maintained off premises. Where possible, databases that allow for the creation of audit trails should be used. Audit trails make it possible for authorized personnel to check the system to find out who has updated a particular file and when.
- Where possible, thin client computers should be considered as an alternative to typical PCs. Thin client computers use resources housed inside a central server rather than on a hard drive. A thin client computer connects to a server-based environment which hosts the applications, memory, and sensitive information the user needs. This type of computer offers increased security—because someone who steals the computer will have access to the computer hardware but no access to data. If someone accidentally tries to save data that is corrupted with malicious code, they won't be able to do so on a thin client computer, because that code would have to be saved onto the server. (Since the server is protected by a firewall, it won't become infected—and it therefore prevents the computer itself from becoming infected by the malicious code.)

As well, thin client computers are less expensive, and they can connect to servers based in the cloud.

- The agency should be familiar with cloud computing services. Cloud computing means storing and accessing data and programs over the Internet instead of through computers' own hard drives. Google Drive, Apple iCloud, Dropbox, and Slack are examples of cloud computing services.
- The agency should have a disaster recovery strategy for personal information that is lost or damaged. For example, a computer virus, a hacking incident, the theft of a computer, or physical damage to the office environment (such as fire or flood) could result in computerized data and/or privacy being compromised.
- The agency should refer to the checklist for network security measures located within the document *Securing personal information: A self-assessment for public bodies and organizations*, published in 2020 by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner for British Columbia.

Know the risks associated with texting and Instant Messaging (IM)

Clients should be aware that:

- They or other individuals could be impersonated via text or IM.
- Texts/IMs can be intercepted.
- Personal information can be recorded, stored, and sold through these platforms.
- SMS texts cannot be encrypted.

Tips to mitigate risk:

- Inform clients that web chat is more secure and can be encrypted.
- Delete the history of the communication.
- Staff should not save clients' names in their contacts.
- Use agency devices and accounts whenever possible.
- Turn off default settings if they allow chat messages to be saved, recorded, or copied.
- Do not automatically back up text chats to cloud accounts in Google Drive or in a shared calendar, as they may then be accessible to others.

For additional guidance, see the BC Association of Clinical Counsellors (2011) Standards for the Use of Technology in Counselling, and the BC Society of Transition Houses (2013) *Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children*.

More tips for using technological tools securely while working remotely

- When using technological tools with clients, make sure they understand how their personal information will be collected, used, and sometimes disclosed by your agency. Keep detailed notes of what you have done and why.
- Before starting a remote connection, get the client's consent and document it—you may want to go over the consent form with the client orally.
- If you are using video technology with a client, make sure the application has end-to-end encryption and that interviews are not recorded. Use the waiting room setting so that only you can let people into virtual meetings.
- Warn the client that some video platforms share personal information with social media sign-ins such as Google and Facebook. Advise them not to sign in through their social media account or Google account because this gives both vendors access to the information on the other platform.
- Transfer digital files to your agency's databases and then delete any digital records from devices you used in your home office.

2. How can I protect personal information when using voicemail?

Background

Voicemail is a useful tool for sending and receiving detailed phone messages. With appropriate safeguards in place, the confidentiality of voice messages, and the privacy of those whose personal information is sent by voicemail, can be protected.

Guideline

- → Agencies should pursue technological methods of protecting voicemail privacy, such as the use of password-controlled voicemail boxes.

3. How can I protect personal information when using emails and faxes?

Background

It is all too common for emails or faxes to be sent to the wrong person. All it takes is the pressing of a single button or key. Managing the flow of personal information by email and fax remains a challenge for both large, well-financed organizations like banks and smaller agencies like doctors' offices.

In BC, both PIPA and FIPPA require that steps be taken to reduce the risks associated with emailing or faxing personal information.

Guidelines

- → Agencies should avoid emailing or faxing sensitive personal information, such as health or financial information or information about someone's psychosocial history. This type of information should only be emailed or faxed when it is absolutely necessary to send it at once and emailing or faxing is the only timely way to do so. Otherwise, such information should be sent by hand.
- → If it is necessary to email or fax a client's sensitive personal information, agency staff should consider phoning first to:
  - Confirm that the intended recipient is actually the right person to receive the email or fax.
  - Confirm that the intended recipient will be there to receive it (if sending by fax).
  - Confirm the intended recipient's email address and/or fax number.
  - Ask the intended recipient to call to confirm receipt of the email or fax.
- → When emailing or faxing clients' sensitive personal information, agencies should consider using unique identifiers or codes made up of numbers or letters in place of names to protect the identities of the individuals involved.
- → Agency staff should avoid emailing or faxing client personal information from public locations.

Effective transmission practices: Emails and faxes

- Set rules about the types of information that can be emailed or faxed to and from your organization. Check regularly to make sure your employees are following the rules.
- Where possible, make one person responsible for sending and receiving personal information, especially faxes. Train that person on proper procedures and ensure they're aware of their legal duty to protect personal information.
- Do not make or keep more copies of emailed or faxed material than you truly need. Securely destroy extra copies.
- If someone asks you to email or fax their personal information to them, explain how emailing or faxing creates a risk of personal information being accidentally disclosed or deliberately intercepted by other people, and get their consent before proceeding.
- If personal information is mistakenly emailed or faxed to the wrong person, or is otherwise compromised through emailing or faxing in a way that cannot be undone, notify your supervisor and the person responsible for privacy compliance in your organization, as well as the BC Office of the Information and Privacy Commissioner. Promptly notify the individual(s) whose personal information has been compromised, telling them the kind of information that has been compromised and the steps that are being taken.

Emails:

- Never use email distribution lists to email personal information.
- Remember, sending an email is like sending a postcard; the content of an email can be read during its transmission. Most email is not encrypted, so it can be easily intercepted. As well, emails may be synced across multiple devices. When emailing personal information—especially sensitive information, such as health information—you should encrypt it so only the intended recipient can read it. Free or low-cost encryption software is readily available on the Internet and through retailers.
- Another way to safeguard email is to password-protect documents and share passwords separately (e.g., over the phone).
- For each email account used to send or receive personal information, establish a secure password known only by the employee authorized to access that mailbox. For a shared mailbox, only provide the password to authorized employees.
- Delete emails from your computer after they have been successfully sent, and retain only paper copies. Clear emails out of the trash folder regularly, and encourage clients to do the same.
- As part of your email signature, include a statement that the information in any email sent by your account is private and for the intended recipient only, and that any email that goes to the wrong recipient should be deleted.

/ Continued on next page

Faxes:

- Place the fax machine in a location that prevents unauthorized persons from seeing faxed personal information.
- Always use a fax cover sheet. It should clearly identify the sender (including call-back particulars) and the intended recipient, and should specify the total number of pages being sent. The cover sheet should also contain a confidentiality clause stating that the faxed material is confidential, is intended only for the named recipient, and is not to be disclosed to or used by anyone else. The confidentiality clause should ask anyone who receives the fax in error to immediately notify the sender and then return or securely destroy the personal information, as the sender requests.
- Before faxing personal information, confirm that the agency you are sending it to has precautions in place to protect the personal information when they receive it. Confirm you have the correct fax number for your intended recipient.
- Follow up right away to be sure the fax went to the right place. Also check the number of pages actually transmitted and received.
- If you've designated one person to send and receive faxes, have that person check each day's fax history report for errors or unauthorized faxing. Keep fax confirmation sheets and fax history reports long enough to be able to do this.
- Retrieve the material you are sending by fax from the fax machine as soon as it has been processed for sending. When you're faxing a client's sensitive personal information, stay by the machine at all times during faxing.
- If you receive a fax in error, promptly notify the sender and return or destroy the information, as requested by the sender.
- If your fax machine has a feature that can require the recipient to enter a password before their machine will print your fax, use that feature when sending a client's sensitive personal information (and in other circumstances, as applicable).
- If you regularly fax sensitive personal information, consider obtaining a secure fax machine that employs encryption or other security measures that limit access to the stored information.
- If you use computers for sending, receiving, or storing faxes, create appropriate computer directories and passwords so that faxes can only be sent, received, and accessed by designated users with the use of confidential passwords. Before faxing personal information through your computer, check that the recipient's computer is protected in the same way.

For more information on best practices and important considerations for keeping electronic records and communicating electronically with clients, visit the BCSTH Technology Safety Project webpage.

Practices associated with the sharing of client information and the release of client records

Release of personal information to third parties under PIPA

Defendants or offenders sometimes request records or personal information about a victim/survivor from a victim-serving agency. They make their request on the grounds that the record also includes information about them or their child, and that they are therefore entitled to see it. In other cases, the offender simply wants to harass or intimidate the victim/survivor to discourage them from participating in legal proceedings.

These *Guidelines* provide that, subject to certain limited exceptions set out in section 18 of PIPA, personal information should not be released to a third party without the client's consent. PIPA also requires consent for information to be so released. In addition, section 23 of PIPA sets out specific situations in which personal information must not be disclosed to anyone. These include situations where:

- Disclosure would reveal information about another individual. (For example, if personal information in the victim's/survivor's file includes information they provided about the offender, then releasing this to the offender would have the prohibited effect of also revealing to the offender information about the victim/survivor.)
- Disclosure could reasonably be expected to threaten the health or safety of an individual, even if they are the person who made the request. (For example, releasing information about what the victim/survivor said to service providers might incite the offender to commit further acts of violence against them. This situation would involve some assessment of the degree of risk involved.)
- Disclosure would reveal the identity of someone who has provided personal information about another individual, and the individual providing the personal information does not consent to disclosure of their identity. (For example, the victim's/survivor's sister has provided information about the offender, which is included in the victim's/survivor's file, and the sister does not wish to have her identity revealed.)

In addition to the restrictions on disclosure already set out in these *Guidelines*, agencies/programs should not release personal information in the above situations.

PIPA and legal proceedings

These *Guidelines* deal with a number of situations in which legal proceedings are underway and third parties are seeking access to information contained in records as part of the proceedings. PIPA does not limit the information available by law to a party to a proceeding, nor does it override the *Criminal Code* or other federal legislation.

1. What if the client indicates they may be a danger to themself or others, or there is evidence of child abuse?

Background

There is no legal requirement to report a potential suicide. However, in cases where a client indicates they may be suicidal, and they then go on to die by suicide, the failure to take appropriate steps to intervene may leave you and your agency open to civil liability. Aggrieved relatives, for example, may sue. They could claim that agency staff did not respond appropriately to indications of suicidal ideation or that the counselling process triggered the act.

The public safety exception to the law of solicitor-client privilege can offer some guidance. Of course, agency staff who are not lawyers do not owe clients such a duty of privilege. However, even for lawyers—who owe their clients the highest level of protection and confidentiality—there are circumstances in which danger to the public can provide an exception to the principle of solicitor-client privilege. The three factors to be considered in determining whether a breach of solicitor-client privilege is appropriate are:

1) whether there is a clear risk to an identifiable person or group of persons
2) whether the risk is one of serious bodily harm or death
3) whether the risk is imminent

The weight given to these three factors will be different depending on the circumstances of each case.

Disclosure obligations when a client may pose a physical danger to themself or others. Content warning: Violence against sex workers

The leading legal case that deals with this issue remains Smith v. Jones, 1 S.C.R. 455, a decision of the Supreme Court of Canada. In this case, a lawyer referred his client, Mr. Jones (who was accused of sexually assaulting a sex worker) to a psychiatrist, Dr. Smith, for an assessment relating to an upcoming sentencing hearing. The accused shared with the psychiatrist a detailed plan of how he was going to kill a sex worker in a specific area of Vancouver. The psychiatrist advised the lawyer that the accused was a dangerous person, but the lawyer told the psychiatrist that he was not planning to raise the psychiatrist's concerns in the sentencing hearing.

While on bail awaiting sentencing, the accused ultimately did not carry out his plan to kill a sex worker. The psychiatrist brought an action for a declaration that he be allowed to disclose the information the accused shared about his plan, in the interests of public safety.

The psychiatrist's communications with the accused fell under solicitor-client privilege because the psychiatrist was acting as an expert for the lawyer. The Supreme Court determined that it was appropriate for solicitor-client privilege to be set aside with regard to the psychiatrist's report. The psychiatrist was able to warn the relevant authorities that the accused posed a threat to sex workers in the Vancouver area. However, the disclosure of information was limited to include only the information necessary to protect the public.

If you, as a member of an agency, have reason to believe that your client will physically harm another adult, there is no positive legal duty to report or warn others; however, you have the *ability* to do so in the appropriate circumstances. If you make a decision *not* to disclose the danger, you may be leaving yourself or your agency open to a civil suit claiming negligence or a failure to exercise due care.

PIPA and FIPPA allow information to be shared when compelling circumstances exist that affect the health or safety of any person. This means that if you do share information about a risk to health or safety, you will not be in breach of your legal privacy obligations.

Ethical guidelines or standards might also come into play in these situations. If you are a member of a professional body, you may be subject to ethical practice codes which address potential suicide or dangerousness (CCPA, 2015). For agencies seeking accreditation, there are specific standards to consider. The COA Standards on Crisis Intervention Services, for example, require that the agency develop written procedures for treatment and referral in cases where a person being served is threatening suicide. The COA Standards require that agencies have clearly stated procedures governing disclosure of client information. These would apply in cases where a person may be dangerous to themself or others.

In cases where a child is in need of protection, the requirements are different. Everyone has a legal duty to report suspected child abuse to the MCFD. (See Part V of these *Guidelines* for more detailed information regarding reporting requirements and other steps to take in cases of suspected child abuse.)

The guidelines below are confined to issues of confidentiality and record keeping. They do not attempt to describe appropriate counselling strategies or interventions in cases involving clients who may be suicidal or a danger to others. In addition to the guidelines below, your agency may want to develop an in-house policy to address these complex issues.

Consider staff training on risk/lethality assessment and appropriate intervention strategies for potential suicide cases. The following agencies can be contacted for further information and assistance:

- Canadian Mental Health Association – BC Division
- Crisis Intervention and Suicide Prevention Centre of BC
- Living Through Loss Counselling Society of BC
- Suicide Attempt Follow-up, Education & Research (S.A.F.E.R.)

Guidelines

→ The duty to protect client confidentiality and not disclose client information to third parties without the client's consent is not absolute. It is subject to legal reporting requirements contained in the CFCSA and other reporting obligations which may be set by agency policy to protect the safety of clients or others. See the B.C. Handbook for Action on Child Abuse and Neglect for further information.

→ In cases where a service provider is made aware of circumstances that indicate that a child is in need of protection, the service provider should:

- Report the suspected abuse to a director/child protection social worker at the MCFD, or to their local Delegated Aboriginal Agency if the child is Indigenous. For Indigenous children (e.g., First Nation, Nisga'a, Treaty First Nation, Métis, Inuit), the director will contact the designated representative.
- Document the response from MCFD or the Delegated Aboriginal Agency.
- Document carefully any steps taken by their agency.
- Advise the client of any agency interventions, unless informing them would impede the due process of law or put the child at further risk of physical or emotional harm.
- Make note that the client has been advised of or consented to the disclosure of information to third parties, if applicable, and include this information in the service record. (See Part V of these *Guidelines* for more detailed information regarding reporting requirements and other steps to take in cases of suspected child abuse.)

2. What if the client is an adult survivor of childhood sexual abuse?

Guideline

→ If an adult client (aged 18 or over) indicates that they were sexually abused as a child, the CFCSA requirement to report does not apply. If, however, there is reason to believe that other children are at risk from the same abuser, the service provider must report this to a child protection worker.

Effective documentation practice

- If you report the abuse, follow the same steps you would take when made aware of circumstances that indicate a child is in need of protection.

Consulting with MCFD

Section 13 of the CFCSA lists circumstances which indicate a child needs protection.

If uncertain as to whether you are required to report to MCFD, contact a worker.

Inform them that you are not making a report but are requesting guidance and consultation. Document the results of the consultation in your service record.

In cases where the client or prospective client indicates they are likely to be a danger to themself or another adult, agency staff should:

- Adopt and consistently use a recognized risk or lethality assessment tool and attach this to your in-house policy on records management. (To obtain additional information on risk identification and assessment tools currently in use, contact EVA BC).
- Consult with another professional whenever possible to obtain their opinion as to whether the circumstances are sufficiently compelling to warrant disclosing the client's personal information.

- Make appropriate referrals.
- Seriously consider notifying the psychiatric or mental health unit, the client's physician, the intended target, or the police, as appropriate. Under PIPA and FIPPA, if compelling circumstances affecting anyone's health or safety exist, the agency may disclose the necessary personal information about the client.
- Provided it will not put the client or anyone else at further risk, discuss any privacy breach with the client beforehand and get their consent if possible; otherwise, notify the client afterwards, provided there is no risk involved.
- Make note that the client has been advised of or consented to the disclosure of information to third parties, if applicable, and include this information in the service record.
- Document the notifications and include them in the service record.
- Document any other steps taken by the agency. Note the date and time when specific procedures were carried out, as well as any individuals contacted, and include this information in the service record.

3. What if I believe that a client is at risk of harm by another person?

If you, as a member of an agency, have reason to believe that your client is at risk of serious bodily harm or death, there is no positive legal duty to report to the authorities; however, you have the ability to do so under privacy legislation in the appropriate circumstances. If you make a decision not to disclose the danger, you may be leaving yourself or your agency open to a civil suit claiming negligence or a failure to exercise due care.

PIPA and FIPPA allow information to be shared when compelling circumstances exist that affect the health or safety of any person. This means that if you do share information about the risk to health or safety, you will not be in breach of your legal privacy obligations. Section 33 (3)(b) of FIPPA also permits employees of public bodies to disclose information for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur.

It may be appropriate to refer a highest risk case to the local ICAT for further information sharing about risk, risk review, and risk management planning. For more information about ICATs and how to connect with your local team, contact Community Coordination for Women's Safety at ccws@endingviolence.org.

4. What if the client wants to see their intake or service record?

Guidelines

- → Unless the funding contract states otherwise, records created or produced by agency staff are owned by and are the responsibility of the agency, and there is no obligation to allow the client physical possession of file contents. A copy of the paper file can be provided, or, if the client's information is in an electronic format, they can choose to receive a copy electronically instead.
- → Generally, the client has a right of access to the information contained in their file (*McInerey v. MacDonald* (1992)). As summarized in A Guide to B.C.'s *Personal Information Protection Act for Businesses and Organizations*, if a client makes a

written request for access to their own personal information and PIPA enables or requires the organization to provide them access, the organization must—pursuant to section 23 of PIPA—give the client:

- Access to their information.
- Information on how the organization has used or is using their information.
- The names of the people and agencies that the organization has provided the client's information to and in which situations the organization did so.

→ Under section 29 of PIPA, the organization normally has 30 days in which to disclose the client's information to them; however, there are certain exemptions (s. 31(1)) which enable the organization to take an additional 30 days. These exemptions include, for instance, situations where the organization has to consult with another agency or government body to determine whether access can be granted; where the client did not provide enough information to lead the organization to the requested information or material; or where a large amount of information needs to be searched and meeting the 30-day deadline would interfere with the organization's operations.

→ If more time is needed to complete the request, the organization must explain to the client why they are taking extra time and when the client should expect a response. The client must also be informed that they can make a complaint to the Privacy Commissioner if they wish to. Further summaries of the sections of PIPA that relate to this issue are set out in B.C.'s *Personal Information Protection Act for Businesses and Organizations*.

→ The client's access to the information in their file should not include access to information regarding third parties that was not provided by the client. Specific situations in which organizations are to deny access are set out in section 23 of PIPA. If some information can be provided but some must be denied, the agency can redact the portion of the information that cannot be disclosed.

→ If the record is, by virtue of the contract, under the custody or control of the funding ministry, the organization must contact the Director/Manager of Information and Privacy. The request will be treated as a request under FIPPA.

→ If the record is under the agency's control, PIPA applies and the request should be handled by the agency's Privacy Officer.

If, after reviewing their records, the client believes there are inaccuracies, they can ask the organization to correct their personal information (s. 24(1), PIPA). If the agency disagrees that there is an error, they should annotate the client's information with their requested correction. The client can ask the Privacy Commissioner to review the issue if they desire. If corrections are made as requested by the client, these corrections must also be disclosed to any other agencies to whom the incorrect information was given within the year prior. The other agencies must then correct the information in their records.

5. What if the client does not have the mental capacity to make decisions about the release of their records?

In this situation, your client—or the courts—will likely have granted someone the authority to act as their representative.

Under PIPA regulations, this representative could be:

- a committee under the *Patients Property Act*
- a lawyer acting under an enduring power of attorney
- a litigation guardian
- a representative under the *Representation Agreement Act*

Under PIPA, this representative has the right to:

- Access a record.
- Request correction of the personal information contained in the record.
- Give or refuse consent to the collection, use, and/or disclosure of personal information on behalf of an adult who is incapable of exercising these rights themself.

Under FIPPA, the committee under the *Patients Property Act* is authorized to make these decisions. Most agencies will be governed by PIPA regulations.

Guidelines

- → If the client lacks the capacity to consent to the release of their personal information, the agency should determine who has the legal authority to act on their behalf.
- → The agency should request copies of the documents authorizing the representative to make decisions on behalf of the client.
- → The written consent of the client's representative should be obtained.

6. What if the client is deceased and family members want access to their records?

Background

Under PIPA regulations, if someone has died, their personal representative can exercise that person's rights to access information and make corrections to that information. If there is no personal representative, the person's nearest relative can act on their behalf.

Guideline

- → The agency should develop an in-house policy governing the release of records after a client's death. The policy should be based on PIPA regulations.

7. What if there is a need to disclose client information for other reasons—for example, to consult or obtain supervision, or to respond to a request from the client's lawyer?

Guidelines

- Unless agency staff are legally required to disclose it, client information should not be released to third parties outside the agency without the informed consent of the client. Even where the client consents, restrictions should be established regarding what client information can be shared, and clear policies should be developed restricting the dissemination of client records. To satisfy the requirement of informed consent, the client needs to know exactly what information is being shared, with whom, and for what purpose.
- If the service provider needs to disclose client information for consultation purposes or otherwise, where there is no legal requirement to release it, the client's written consent to disclose should be obtained. If the client cannot read a written consent form, it should be read out loud and explained to them. If the client cannot understand English, an interpreter should be used.
- The client should be provided with a copy of their signed consent form. The original should be kept in the case file for the recommended retention period.
- The client should be informed at the start of the service relationship of some of the situations that could come up in which confidentiality would be limited, and how these situations would be handled. Examples might include:
  - Presenting the victim's/survivor's case (without identifying information) for training or supervision purposes.
  - A situation in which the client needs to obtain support from the Crime Victim Assistance Program and the service provider must therefore submit reports on counselling progress to Crime Victim Assistance personnel.

Effective documentation practices

- It is not generally advisable to transfer information or client records to a professional outside your agency, including your client's lawyer. Do so only when the client has consented and it is deemed essential. Take steps to ensure that appropriate confidentiality policies are in place in the receiving office. You may, for example, wish to advise the consulting professional that the consent is time-limited and request that any transferred records be destroyed after the expiry date.
- Consider establishing guidelines for your agency restricting the use of mail, faxes, and email to transmit client information outside the agency for any reason.

8. What if police informally request information about clients?

Normally, under PIPA, consent would be required before any of the client's personal information could be shared with third parties, including police. But there are exceptions to this rule.

Under PIPA section 18(1)(j), your agency may disclose without consent to a law enforcement agency, such as police, under certain circumstances. You may disclose to assist police with an investigation, or to assist them in making a decision to start an investigation.

Section 18 applies before a charge is laid. It permits you to share personal information with law enforcement agencies but does not require you to do so. Each situation will need to be assessed on its own merits.

To satisfy the requirements of informed consent, a written consent should:

- Set out the nature of the information to be shared, the recipient(s) of the information, and the purpose for which it is being shared.
- Indicate whether it applies only to information that has already been gathered, or also to information that may be obtained in the future.
- Be signed by the client and dated.
- Be time-limited.
- Include a statement to the effect that the client may withdraw their consent.

PIPA does not apply to documents related to a prosecution if proceedings, including possible appeals, are still pending. This means that after a charge has been laid, and until all appeals have been exhausted, regular criminal law rules regarding disclosure and evidence gathering will apply rather than PIPA. Under these circumstances, you are not generally required to release information without a court order. It may well be against your client's interests to do so.

Most but not all agencies and programs will be covered by PIPA. For those that are not, reference should be made to equivalent provisions in FIPPA. (See Part I of these *Guidelines* for general information about these Acts.)

The release of personal information can have significant implications for your client. As a matter of law with few exceptions, all relevant documents that police or Crown counsel review in the context of a criminal case must be disclosed to defence counsel (*R. v. Stinchcombe* (1991), *R. v. McNeil* (2009)). The use of this material for cross-examination of the victim/survivor could result in re-traumatization. However, there may also be cases where information contained in the records will assist the victim/survivor. It might corroborate their complaint or provide aggravating details. An in-house policy at your agency should outline what criteria might be considered by your agency's staff in deciding what to release.

Guideline

→ The agency should develop an in-house policy that applies in cases where a request for information is made by police without a court order.

Effective documentation practices

Consider adapting the following clauses for inclusion in your in-house policy:

- The client should be informed at intake, or soon after, of the agency's policy regarding release of records to third parties, including police.
  - Client records should not be released to police (or any third parties) without the client's consent, unless the agency is legally required to release them—for example, where a court orders the release of client records, where agency staff are subpoenaed and then required to give evidence in court, or where there is a statutory or common law obligation to disclose, as there is under the CFCSA—or there is reason to believe the client is a danger to themself or others.
- If agency policy is to release to police, Crown, or third parties (where not legally required) with the client's consent, the following precautions should be taken:
  - Inform the client that there are legal implications to the release of the records.
  - Recommend that they obtain independent legal advice prior to the release of the records to discuss these legal implications.
  - Have the client sign a written consent.
  - Document that the above precautions have been taken (e.g., the written consent could confirm that precautionary steps have been taken).

9. What if client records are the subject of a search warrant?

Background

A search warrant is a court order issued by a judge under the *Criminal Code*. It overrides any requirements not to release information under PIPA. The warrant authorizes a named person, usually the police, to enter a specified place to search for and seize specified property which will provide evidence of the commission of a crime. The warrant must contain sufficient description of the objects of the search (e.g., the type or category of objects and their relation to the offence).

The warrant may be issued early in a criminal investigation, before charges have been laid. It is possible that client records may be the subject of a search warrant. For example, if the client was a transition house resident who resumed living with their partner and was later murdered, police might execute a search warrant to obtain transition house records regarding the client. Police may believe that the records will provide important evidence that is relevant to an issue in the murder case.

Guideline

→ When an agency is served with a search warrant, the applicable agency staff should read the warrant and provide police with the objects described in the warrant. If staff have concerns about the warrant or how it is being executed—for example, if they believe the warrant does not describe the objects in enough detail or does not link them to an issue in the case—they must nonetheless comply with the terms of the warrant, but they should contact a lawyer at the earliest opportunity. The lawyer may make an application to quash the warrant.

10. What if client records are subpoenaed in the context of a criminal prosecution for a sexual offence?

Background

Criminal law applies here, rather than PIPA. (PIPA does not override the *Criminal Code* or other federal laws.)

There are two main ways through which your client's records or files may become involved in court proceedings in a criminal case:

- Your agency's records about the client are subpoenaed.
- You and/or other agency *staff* are subpoenaed to appear as witnesses in court and bring relevant documents with you.

The guidelines below deal with the subpoenaing of records. (See Part IV of these *Guidelines* for practices associated with the sharing of client information and the release of client records and guidelines related to a subpoena to appear as a witness.)

Offences covered by *Criminal Code* sections 278.1 to 278.91

If the accused is charged with one or more of the offences below, their access to the victim's/survivor's private records will be restricted by *Criminal Code* sections 278.1 to 278.91:

Section 151 Sexual Interference
Section 152 Invitation to Sexual Touching
Section 153 Sexual Exploitation
Section 155 Incest
Section 160 Bestiality
Section 170 Parent or Guardian Procuring Sexual Activity
Section 171 Householder Permitting Sexual Activity
Section 172 Corrupting Children
Section 173 Indecent Acts
Section 213 Offence in Relation to
Section 271 Sexual Assault
Section 272 Sexual Assault with a Weapon
Section 273 Aggravated Sexual Assault

A subpoena of records is often described as making an application for "production." You will be served with a Notice of Motion and Subpoena. A hearing (separate from the trial) will be held on the application to have the records released or "produced." If the court orders the records released, this does not mean they are automatically admissible as evidence during the trial. However, information contained in the records may be used by defence counsel to help develop questions for cross-examination or as a way to find out about other evidence they could potentially use in the defence's case.

If a sexual offence is involved, the procedure that defence counsel will follow to apply for access to your client's records is governed by *Criminal Code* sections 278.1 to 278.91.

A record is defined in these sections (particularly s. 278.1) as any form of record that contains personal information for which there is a reasonable expectation of privacy. This includes medical, psychiatric, therapeutic, counselling, education, employment, child protection, adoption, and social services records, personal diaries, and more. The sections apply whether the record is held by a third party—such as a Community-Based Victim Services program—or by the Crown prosecutor.

Sections 278.1 to 278.91 restrict the accused's access to private records regarding the victim/survivor. They were added to the *Criminal Code* in 1997 in response to the Supreme Court of Canada (SCC) case of *R. v. O'Connor* (1995) and the lobbying of former Justice Minister Allan Rock by women-serving organizations across the country. The *O'Connor* ruling required record holders—including community-based agencies—to release a victim's/survivor's personal records subject to a test for relevance.

The SCC built upon its ruling in O'Connor in the cases of *R. v. Mills* (1999), *R. v. Quesnelle* (2014), and *R. v. Grant* (2015). The "*Mills* regime" applies if a record contains personal information for which there is a "reasonable expectation of privacy" (s. 278.3). When the Crown prosecutor receives a record that is subject to the *Mills* regime, they must notify the accused and indicate whether or not it is likely to be relevant and why. Then, the accused can apply for the records to be produced by the third party.

To decide whether or not to order the third party to produce the records, the judge must consider eight factors, which are listed in s. 278.5(2) of the *Criminal Code*. If the judge orders the records to be produced, they will then review the records in a private hearing.

The judge will weigh the accused's right to make a full answer and defence against the complainant's/witness's right to privacy, personal security, and equality. In order to release some or all of the records to the accused, the judge must determine that they are "likely relevant" and their disclosure necessary in the "interests of justice."

In *Quesnelle*, the SCC held that police occurrence reports that relate to complainants or witnesses in sexual offence cases but that do not directly relate to charges an accused person is facing are still subject to the *Mills* regime. In *Grant*, the SCC affirmed its decision in *Quesnelle*, as well as the Parliamentary amendments to the *Mills* regime.

Guidelines

- The service provider should advise the client of the situation and the steps they intend to take.
- The service provider should advise the client to get independent legal advice by referring them to Legal Aid BC. Complainants/witnesses have the right to counsel and to be informed of that right (s. 278.4(2)(1)).
  - Crown counsel acts on behalf of the state's interests and does not represent the agency or the victim/survivor.
  - The agency may not have the same legal interests as the client, so it is not appropriate for both to have the same lawyer.
- The agency should consider seeking legal advice. This may be important to protect the reputation of the program as a confidential service.
- If it is determined that the agency will not comply with the request to hand the records over, the agency's lawyer can file a motion to set aside the subpoena, and a hearing will be scheduled.

The Ministry of Public Safety and Solicitor General provides legal representation for:

- Any victim/survivor whose records are subject to an application for release under *Criminal Code* sections 278.1 to 278.91.
- Victims/survivors of prescribed criminal offences (as per Schedule 1, Crime Victim Assistance (General) Regulation) who require representation independent from that of Crown counsel in response to a disclosure application relating to their personal history.
- Witnesses of crimes subject to disclosure applications other than s. 278.3 disclosure applications.

This funding is based in part on s. 3 of the *Victims of Crime Act*, which requires the Ministry of Attorney General to take measures to ensure legal representation for victims/survivors in certain situations.

For further information, contact Legal Aid BC.

→ The agency should inform Crown counsel that they have been served with a production order, as well as the position they intend to take. While Crown counsel does not represent the victim/survivor or the agency, they may have a role to play in ensuring the correct procedure has been followed by defence, especially if the victim/survivor has not yet retained a lawyer. Crown may object to insufficiency or lack of notice. For example, if the records relate to group counselling and other group members who are not the target of the production application were not served with the Notice of Motion, the Crown might object.

If the agency retains a lawyer to handle the application for production, the lawyer may ask:

- Has the defence lawyer provided any evidence that the type of information they are looking for is likely to be in the records they are demanding?
- Is it logical to infer from the surrounding circumstances that the records do contain such information?
- If the information is in the records, does it relate to an issue in the case?
- How important is client confidentiality to your agency's work?
- Do you have evidence to support the view that assurances of confidentiality assist survivors to come forward to seek help?

→ The agency and/or its lawyer must appear in court on the date set out in the Notice of Motion. There is no requirement to release the records in question until the court orders the release (at the hearing).

→ Agency staff should consider adopting an in-house policy that provides that client records not be released to police or Crown counsel without a court order. Under the Criminal Code, if Crown has the records, Crown must notify defence of their existence (without revealing the contents).

- Agency staff should consider adopting an in-house policy that provides that client records not be released to any third parties unless the client consents or there is a legal requirement to do so (e.g., the court orders the release of client records, agency staff are subpoenaed to appear as witnesses and then required to give evidence in court, or there is a statutory obligation to disclose—for example, under the CFCSA).
- There may be cases where the client *will* consent to the release of records or wish them released without a court order or other legal requirement. Information contained in the records may corroborate their complaint or provide aggravating details. Whatever approach the agency takes in sch cases, the client should be informed of it—preferably at intake or soon after. If agency policy is to release to police, Crown, or third parties (where not legally required) with the client's consent, the following precautions should be taken:
  - The client should be informed that there are legal implications to the release of the records.
  - The service provider should recommend that the client obtain independent legal advice prior to the release of the records to discuss these legal implications.
  - The client should sign a written consent.
  - The service provider should document that the above precautions have been taken (e.g., the written consent could confirm that precautionary steps have been taken).
- If the agency has been served with an application for production of records (the Notice of Motion and Subpoena), and agency staff are bringing documents to court, they should include both an original and a copy of the records specified in the subpoena. An additional copy should be retained in the case file at the agency. All documents should be sealed. If the records are ordered released, the agency will want a copy for reference. If the records are not released, the file will be kept by the court in case later evidence results in another application for production. When all levels of appeal are exhausted, the records will be returned to the agency. This may take months or years.
- If the judge orders the records released, the agency or its lawyer can argue that any one or more of the following conditions should be attached:
  - Only relevant parts of the record should be released.
  - Only a limited number of copies should be made.
  - Records should only be viewed in court.
  - For safety reasons, any identifying information regarding people named in the record should be redacted, along with other such information.

11. What if client records are subpoenaed in the context of criminal prosecution for a non-sexual offence, such as spousal assault?

Background

If an accused is charged with a non-sexual offence, such as simple assault, the principles set out by the SCC in the cases of *R. v. O'Connor*, *R. v. Mills*, *R. v. Quesnelle*, and *R. v. Grant* still apply to requests for release of third-party records. In 2015, Parliament made changes to the legislative regime governing third-party records when it enacted the *Victims Bill of Rights Act*. This *Act* included the *Canadian Victims Bill of Rights* (CVBR) and amended other *Acts*, such as the Criminal Code. Specifically, sections 278.4(2), 278.5(2), 278.7(2), and 278.7(3) of the *Criminal Code* were amended, collecting and restating the SCC's decisions and establishing the updated system of rules for third-party records.

Guideline

→ The service provider should apply the guidelines under Part V *(What if client records are subpoenaed in the context of a criminal prosecution for a sexual offence?)* with the necessary changes.

12. What if the accused already has the records?

Background

It is unlikely the accused would obtain records maintained by the agency. They might, however, get access to documents created by the client, such as their personal diary, which are kept at home. This might happen where the couple had been living together at some point.

If for some reason the accused already has the records in their possession, the courts treat this situation as a question of "admissibility of evidence" and not "production" (*R. v. Shearing* (2002)). In 2019, the *Criminal Code* was amended to include a procedure addressing whether the complainant's record can be admitted into evidence by the accused. As summarized by Alan Gold (2020), the record will be inadmissible unless the judge (following the procedures set out in sections 278.93 and 278.94 of the *Code*) determines:

(a) that evidence relating to earlier sexual activity by the complainant meets the conditions set out in s. 276, or

(b) in any other case, that the evidence is relevant to an issue at trial and has significant probative value that is not substantially outweighed by the danger of prejudice to the proper administration of justice.

To determine whether the evidence is admissible, there will be a hearing in which the judge will consider:

(c) The interests of justice, including the accused's right to make a full answer and defence.

(d) Society's interest in encouraging the reporting of sexual assault offences.

(e) Society's interest in encouraging complainants to obtain treatment.

(f) Whether there is a reasonable prospect that the evidence will help arrive at a just determination in the case.

(g) The need to remove any discriminatory belief or bias from the fact-finding process.
(h) The risk that the evidence may trigger feelings of sympathy, prejudice, or hostility among the jurors.
(i) The potential prejudice to the complainant's dignity and right to privacy.
(j) The complainant's right (and all peoples' right) to personal security and to the full protection and benefit of the law.
(k) Any other factor the court considers to be relevant.

Guidelines

- → The service provider should let the client know that if there is a trial:
  - They may be cross-examined on the contents of the records.
  - The records may be introduced as evidence if their contents are considered relevant to an issue in the case.
- → The agency should inform Crown counsel that the accused has the records.

13. What if I am subpoenaed to court to appear as a witness at the time of the preliminary inquiry or trial?

Background

This is a different process from the subpoenaing of records. It involves you appearing as a witness. You will be served with a subpoena, which means you will be required to attend court and give evidence. The subpoena may also include a clause requiring you to bring along anything in your possession that relates to the charge, including particular documents. This might happen where defence has already obtained a production order, has reviewed the records, and now wishes to introduce them as evidence at the trial.

Guidelines

- → It is necessary to follow the directions contained in the subpoena. Generally, this requires the service provider (the custodian of the records) to attend court at the time, place, and date of the trial. If the records have not yet been released in the case, the subpoena does not require the service provider to provide them until the court orders it.
- → The service provider should advise the client of the situation and the steps they intend to take.
- → The service provider should advise the client to get independent legal advice.
- → The agency should also obtain legal advice. Even if a production order (for release of the records) has already been made by the court before trial, the records are not automatically admissible as evidence in the case. The agency's lawyer may object to the records being admitted as evidence, for example, on the grounds that they are inherently unreliable as a source of "factual" information.

14. What if client records are subpoenaed in the context of a custody dispute or another civil case, or I am served with an application for an order for production and inspection of records?

Background

There are two major ways in which disclosure of client files may be formally requested in a civil court case:

1. When an application or Notice of Motion is made for the production and inspection of client records as part of the pre-trial discovery process.
2. When program staff and their client records are subpoenaed to appear in court at trial.

If pre-trial production of records is being requested, you will receive a Notice of Motion prior to trial advising you of the disclosure application. For example, the non-custodial parent may request release of your client's files in order to assist them in a custody dispute. The Notice of Motion does not contain the actual order for production of the files, nor does it require the service provider to produce the files. For example, where the agency has two types of records regarding a client—such as one set related to justice system information and support services, and another related to counselling services—and where likely relevance is based only on arguments related to information in one type of record, then the other records may not need to be released because they are irrelevant. This position is strengthened if the two types of records are kept in separate files or in separate sections of the same file.

Just because you receive a Notice of Motion to produce records does not automatically mean that the records you have must be released. Ethical or accreditation standards may require that you first consider the legal validity of a request for release of records before you complete the disclosure.

In consultation with your agency's lawyer, you might challenge the request for records. For example, your lawyer could argue that the documents should be privileged or that their release be subject to strict conditions (*M.(A). v. Ryan* (1997)). At trial, it could be argued that the records are inadmissible as evidence—that the information contained in the records is of limited relevance to an issue in the case. The court makes decisions about privilege on a case-by-case basis. As summarized in the *BCSTH Legal Toolkit* (2016), the judge will consider whether:

- the information was provided in confidence
- the confidentiality is necessary to the relationship
- the confidentiality fosters a public good

If the judge finds that these three conditions are satisfactorily met, they will then decide whether the interest of privacy in protecting the records' confidentiality is more important than the interest of finding the truth in the context of the civil case. Just because records may be produced in a criminal case does not mean that records will be produced in a civil case. If the judge does order the records to be produced, your organization can request that the records be disclosed on a limited/redacted basis, as described in the guidelines for criminal cases.

If a subpoena is issued, you will be served with it. As described in the guidelines for criminal cases, a subpoena is a court order compelling a person to attend court to give evidence and/

or produce client records at the hearing. For example, if you are an STV counsellor, you may be subpoenaed by the defendant in a civil sexual assault case to give evidence as to what the victim/survivor may have said to you at the time when they first disclosed the assault. The subpoena orders the custodian of the files to attend court with their records at the time, place, and date of the trial. If you do not attend, you may be arrested and charged with contempt or obstruction of justice.

There may be other cases where your client's lawyer asks you by phone or letter to provide information to support your client's civil action. In the absence of a court order or subpoena requiring you to release records, you will need to get your client's consent before releasing any information. (See Part IV of these *Guidelines* for further information on practices associated with the sharing of client information and the release of client records, and the need to disclose client information.) When making decisions about release in this situation, it is important to consider the research that suggests that third-party records are generally used to discredit, rather than support, a victim's/survivor's claim (Cory, Ruebsaat, Hankivsky & Dechief, 2003).

Guidelines

- → If client records are subpoenaed or the service provider is served with an application or Notice of Motion advising them that an order for production and inspection of client records is being sought, the service provider should:
  - Contact a lawyer.
  - Consult with any applicable provincial umbrella agencies, licensing bodies, or professional associations regarding ethical requirements.
  - Carefully review the records in question to identify any parts that could arguably be retained on the grounds of privilege or irrelevance.
  - As appropriate, assist their lawyer by providing information on why all or some of the information is privileged or irrelevant.
  - As appropriate, inform their lawyer that:
    - It was expected that the communications with the client would be kept confidential.
    - This confidentiality is essential to the agency/client relationship.
    - Supporting this type of agency/client relationship is in the public good.
    - The interests served by protecting the communications from disclosure outweigh the interest of pursuing the truth and preventing an unjust verdict (*M.(A.) v. Ryan* (1997)).
  - Assist the lawyer by formulating possible conditions or limits that can be attached to production, along with reasons for these restrictions.
  - Advise the client of the situation and the steps they intend to take.
  - Advise the client to obtain independent legal advice.
  - Make copies of all the records in the client's file and keep them at the agency in a separate file for the recommended retention period (see Part IV of these *Guidelines* for further information on retention of client records). It may be advisable to have the copies of the client's records certified by a lawyer or notary; this way, they can be used for other legal purposes while the originals remain with the court.

- Even if the agency has been served with a Notice of Motion, the service provider is not legally required to produce client records immediately. The service provider should attend court at the date and time specified in the Notice of Motion; at that time, the court will hear arguments about the relevance of the documents in question. If the service provider or agency has been served with a subpoena, they should attend court with the records at the date and time requested.
- If the service provider is asked to produce their files when they are called to the stand, they should first state any concerns regarding the protection of their client's confidentiality and then wait to hear what the judge directs. The service provider must proceed as directed by the judge.
- If the service provider believes that the safety of their client or any person is threatened by the release of the records, this should be stated at the hearing.
- If the court issues an order for production and inspection of client documents, the terms set out in the order must be complied with. The service provider should only release the documents ordered by the court.
- The service provider or their lawyer should request that the wording of any court order that is made be precise regarding which documents must be released.
- If the court orders the production of the files, the service provider or their lawyer should request that the court impose terms in order to limit any invasion of privacy. This would include, for example, a request that non-relevant sensitive portions of the record be edited (by the judge) prior to release, that no photocopies be made, and/or that the party seeking access to the records only be permitted to view them in the presence of the agency's lawyer.

15. What if there is a question about whether privacy rules were followed?

Background

PIPA provides that anyone who feels that the *Act* was not followed can contact the Privacy Officer of the organization. Information about the Privacy Officer should be made available either at intake or upon request.

PIPA requires organizations to designate at least one person to be responsible for privacy compliance. This person is responsible for managing and implementing your agency's privacy policy. You must designate at least one person within your agency as the Privacy Officer and must list their identity and contact information on your intake forms.

If there is a complaint, the Privacy Officer should make every effort to deal with the matter quickly and fairly. While different personnel may be called upon to help investigate, the Privacy Officer is, logically, the one responsible for receiving all complaints and making sure they are dealt with in a timely manner. If the Privacy Officer is uncertain as to how to address a complaint, they can call the Privacy and Access Helpline at 250-356-1851 or email privacy.helpline@gov.bc.ca.

Guidelines

- The organization should designate someone who will be responsible for ensuring compliance with PIPA. That person will be responsible for developing and implementing a privacy policy and making sure it is working effectively.
- Agency staff should respond to concerns. If someone makes a complaint about how the organization handles personal information, agency staff should try to resolve the complaint quickly and fairly.
- If the complaint cannot be resolved directly with the organization, the client should be advised that they may ask the Office of the Information & Privacy Commissioner for British Columbia to review the matter. The Commission website can be found at https://www.oipc.bc.ca.

16. Do the same rules apply to information about agency employees?

Guideline

- Under PIPA, the agency may collect, use, and disclose employee information without consent if it is reasonable for starting, managing, or ending the employment relationship. If the agency collects, uses, or discloses employee information without consent, however, it must notify the employee.

17. What about information provided to individuals doing contract work for the agency?

Background

PIPA rules also apply to personal information that your organization has transferred to a contractor for processing and to information the contractor may have collected on your organization's behalf.

Guideline

- Agency contracts should clearly state what requirements must be met to comply with applicable privacy legislation and any policies the organization has developed to manage personal information.

Retention of client records

1. For how long should client files be kept?

Background

PIPA requires that personal information be kept for *at least* one year. After that, the retention period should be based on legal or business requirements. The guidelines below recommend that, in general, adult client records be kept for a minimum of seven years, while the records of a child client should be kept for seven additional years after they reach age 19. The seven-year minimum is based on the agency's potential need for protection from legal liability and the client's potential need to access such records in the context of a civil suit for sexual assault. The guidelines below go on to suggest that some agencies consider whether client

records might be kept indefinitely, subject to financial and physical capacity. These guidelines apply even if the client has relocated to another jurisdiction.

The seven-year minimum retention period is consistent with current practice in related fields (e.g., social workers, psychologists) and with the legal and business needs of most community-based programs. Further, it is consistent with BC's *Document Disposal Act*, which governs ministries, branches, and institutions of the provincial government. As well, COA Standards provide that, as a general rule, the organization must maintain case records for at least seven years after termination of services unless otherwise mandated by law.

In making decisions about retention periods, agencies should also refer to their funding contracts. These may require that client records be kept for a certain period of time.

Some service providers believe it is best not to keep notes or records at all. This is because of the possibility of client records having to be disclosed to unsympathetic third parties in a court case. There is a real need to protect client privacy and a real concern that private information will be used inappropriately or in an adversarial way. Despite these concerns, a decision not to keep records may not be in the client's or the agency's best interests. Records provide an important source of information for both the client and the service provider.

Conscientious record keeping can help the service provider to develop and implement an appropriate plan of service, review their work as a whole, and self-monitor more carefully. Also, if the client decides to pursue a civil claim for damages for pain and suffering resulting from a sexual or physical assault, counselling records might verify the extent of the psychological trauma suffered. If they submit an application for Crime Victim Assistance, their records can assist in establishing the need for compensation.

It is not easy to predict what type of legal process your client might become involved with, or when. There is a 12-month limitation period for summary conviction offences under the *Criminal Code* and no limitation period for indictable (more serious) offences. The latter would include more serious physical and sexual assaults.

In civil cases, there are various limitation periods. Under the 2012 *Limitation Act*, most claims have to be filed within two years of the date of discovery (except for debts owed to the government, for which the limit is six years, and for the enforcement of civil judgments, for which 10 years is allotted). The longest limitation period under the *Act* is 15 years from the act or omission; though, some civil claims, such as actions relating to sexual assault and arrears of child and spousal support, are exempt and have no limitation period. Because some actions have no limitation period, the possibility exists that a criminal or civil action related to your client may be initiated at any time in the future, even if no legal process is planned or underway at the time services are requested or delivered.

In addition to possibly establishing your client's claim, client records can help support you or your agency if you are sued for negligence or malpractice. A client, former client, or aggrieved third party could launch a civil suit against you or your agency years after a supposed incident. If records were not kept or were destroyed within the applicable period before the commencement of the lawsuit, it may be difficult to verify actions taken or interventions made by your agency on behalf of the client.

The legal concept of "discoverability" is also important to consider. Discovery rules are set out in Part 2 of the *Limitation Act*. There are situations in which limitation periods may be suspended—for instance, if the client becomes a person under disability. In criminal prosecutions, the destruction of client records may also have a significant impact on the client or agency. If your client is a victim/survivor or witness in a criminal case, and agency records were destroyed prior to the trial, there is a chance the case will be stayed if their counselling records are requested by defence and are no longer available (*R. v. Carosella* (1997), *R. v. Bero* (2000), *R. v. Neidig* (2015)).

Some professional associations recommend or require members to keep client records. The code of ethics of the Canadian Psychological Association, the British Columbia College of Social Workers, the British Columbia Art Therapy Association, and the BC Association of Clinical Counsellors, for example, all identify the need to maintain session notes.

Please note that the guidelines and documentation practices set out below apply only to operational records and not to administrative records (see the Glossary at the end of these *Guidelines*).

Guidelines

- Some agencies may choose to keep all client records indefinitely. For many, this may not be possible, given financial or physical capacity; though, the ability to retain records electronically assists in this regard. The documentation practice tips below recommend that operational records be kept for a minimum of seven years for adults and seven years past the age of majority for those who obtained service as minors. After this period, critical information from each record can be transferred into a file summary or database and maintained indefinitely, while the rest can be shredded.
- Client records must not be destroyed if they have been subpoenaed or if legal proceedings are underway or expected.
- The agency should develop a written policy on file retention and inform agency clients (preferably at intake) of this policy.

Write your retention policy as if it were a public document, and be able to justify its contents. Base the policy on the service requirements or needs of your agency. If your agency has a policy of shredding after a certain number of years, this policy might be strengthened by including a rationale for that approach. For example:

- Space and financial limitations do not allow files to be kept indefinitely.
- The retention period is based on accepted practices within the field.
- The client has been advised of and has agreed to the retention period.

Effective documentation practices for operational records

- Unless otherwise required by law or contract, keep records for a minimum of seven years. (It is recognized that this may not be possible for all agencies, given current funding levels.)
- At the end of the seven-year period, transfer critical information from the record into a file summary or database, and then shred the complete record. File the summary and keep it indefinitely.

Sample file summary

Client number:

Name:

Date of birth:

Address:

Telephone:

Presenting issue (particulars of complaint or reason for seeking service):

Dates of contact:

Date record destroyed:

For operational records involving a client who is a minor (aged 18 or under)

- Unless otherwise required by law or contract, keep records for a minimum of seven additional years after the client reaches the age of majority (age 19).
- At the end of the seven-year period, follow the documentation practices described above for operational records.

2. What about old or existing files that have been kept in their entirety?

Guideline

→ If resources are available, agency staff should consider transferring information contained in these files into a file summary or electronic database according to the procedure set out above in Part IV of these *Guidelines* on retention of client records (For how long should client files be kept?), then shredding the remaining file contents.

Destruction of client records

1. How should client records be destroyed?

Guidelines

- → Paper copies of client records should be shredded at the end of the retention period adopted by the agency.
- → Computer records should be wiped clean or rendered unreadable through the use of an appropriate mechanical, physical, or electronic process at the end of the retention period.

2. What if the client wishes to have their records destroyed before the recommended retention period is over?

Guidelines

- → Unless the agency's funding contract states otherwise, the agency is responsible for the records it creates and has no legal obligation to destroy them at the request of the client.
- → In situations where agency staff or board members are concerned about possible legal liability, it will not be in the interests of the agency to destroy the records before the end of the recommended retention period. Records must not be destroyed to avoid a subpoena.

Effective documentation practices

- If your client asks you to destroy their records, inform them that there are legal implications. If you are considering destroying the records before the end of your agency's recommended retention period, recommend that your client obtain independent legal advice first. If your agency has an internal policy regarding file retention, consult it first.
- In exceptional circumstances where your agency decides to destroy the records:
  - Basic file information should be recorded in a file summary or database. (See Part IV of these *Guidelines* for more information on retention of client records.)
  - The client should sign a written consent stating that they requested and agreed to this action, and that they have been referred to a lawyer to discuss the implications.
  - The consent should be referred to in the file summary or database and should be filed and retained indefinitely by the agency.

Closure of the agency

1. What should be done with client records if the agency dissolves or shuts down?

Guidelines

- The agency's contract with the provincial government should be referred to in order to determine how it deals with this situation. If the contract specifies that client intake and service records are owned by the funding ministry, then these records should be sealed and forwarded to the ministry.
- If the contract does not address this situation, or does not state that intake and service records are government property, then the funding ministry should be advised of the closure of the agency. Records for which the retention period has not expired should be sealed so as to preserve confidentiality and stored at an independent storage facility, possibly with the assistance of government funding. If applicable, the sealed records could be forwarded to the community agency that receives the contract to continue the service.

If your agency does not have a shredder, commercial shredding services should be used where resources permit. Client records should not be recycled or placed with regular garbage.

V. Records management issues related to clients who are children

The intake process

1. What is the process for documenting that a child client has consented to receive services?

Background

It is often said that "consent is a process, not a form." This is especially true where a service provider is determining whether a child is able to consent. While a signed consent form is necessary to establish that valid consent was given, no one consent form can address all the situations that can arise.

These guidelines deal with records management issues. They do not attempt to outline appropriate counselling practice.

- Service providers working with children who witness abuse can refer to BCSTH's PEACE Program Policy Template & Guide (2018) for further information in this area.
- Those working with youth victims/survivors of gender-based violence can refer to EVA BC's Sexual Assault Support Worker Handbook (2016) and the ICAT Best Practices Guide, 2nd Edition (2017). EVA BC resources are available on the EVA BC website.

In order to consent to services/counselling, clients must have legal capacity. The *Age of Majority Act* provides that, by age 19, individuals can make decisions affecting their welfare, including healthcare decisions. According to the *Infants Act* and case law, anyone under 19 is also capable of consenting to healthcare, as long as the service provider:

- Is satisfied that the infant understands the nature and consequences, as well as the benefits and risks, of a particular plan of care.
- Has made reasonable efforts to determine and has concluded that the healthcare is in the infant's best interests.

The service provider should also ensure that the consent is voluntary and not the result of undue pressure.

Technically, anyone under 19—even someone as young as 10 years of age—can consent to treatment or healthcare (including support services or counselling), provided they understand the nature and consequences of treatment, as well as the associated benefits and risks, and provided the care is in their best interests.

In *practice*, 12 years of age is often used by public agencies and service providers as a benchmark to help determine whether a child has the legal capacity to consent. In its policy and procedure manual, for example, the BC Children's Hospital has determined that patients 12 years of age and older are usually competent individuals. This means that, generally, they can give consent for any plan of care without the need to consult with their parents or guardians.

In addition to the child's age, the following general factors are often considered by service providers in deciding whether young clients are capable of consenting:

- The child's developmental level and maturity.
- The nature, complexity, and duration of the plan of care (e.g., if the service or intervention is long-term or very involved, more maturity may be required for a child to understand the nature, consequences, and associated risks and benefits).
- The child's ability to agree voluntarily (e.g., does the family situation interfere with the child's ability to make independent decisions? Is the child expected to go along with their parents' wishes in order to receive emotional or financial support?).

If the basic criteria for capacity to consent have been met, the service provider must then take steps to ensure the child makes an informed decision about the services they are to receive. This involves:

- Providing the child with information that a reasonable person would require to understand the services being offered and to make a decision.
- Providing information about the nature and purpose of the services and any risks and benefits associated with them that a reasonable person would want to know about.
- Discussing alternatives to the services being offered.
- Responding to questions about the services.
  (Bryce, 2013; Bryce, 2015)

While it is possible to provide services to a "mature minor" without their parents' or guardians' consent or knowledge, it may be appropriate to involve a non-abusive parent in some way. This will depend upon the circumstances and the type of service being provided.

It is important to note that, apart from consent issues, other aspects and information involved in the intake process for adults apply equally for clients who are children. For example, there may be a need for safety planning or risk assessment related to both parent and child when services are being provided to the child. (See Part IV of these *Guidelines* for further information on the intake process.)

If a child refuses to consent to treatment, child protection authorities can override their decision pursuant to s. 29 of the CFCSA. This *Act* enables the child protection agency to commence a court action if they believe the child requires specific healthcare. In order for the agency to bring the action, two medical practitioners need to sign on with their support, indicating that the treatment is necessary to preserve the child's life or to prevent serious or permanent impairment to the child's health (BCSTH, 2016; CFSA, s. 29).

Guidelines

- If a child is consenting to services/counselling on their own behalf, the service provider should document steps taken to determine the client's capacity to consent. This documentation should be kept in the client's file for the recommended retention period. (See Part IV of these *Guidelines* for more information on retention of client records.)
- If the child is not capable of consenting and the referring parent/guardian has sole custody, but guardianship of the child is joint, the service provider may obtain consent from the custodial parent/guardian unless the guardianship order requires that the other parent/guardian also be consulted (section 41, *Family Law Act*).
- If the child is not capable of consenting and the referring parent/guardian shares joint custody, the service provider should make every effort to obtain consent from both custodial parents/guardians. If this is not possible, the service provider may proceed with the consent of one custodial parent/guardian, pursuant to the *Family Law Act* (Bryce, 2013; *BCSTH Legal Toolki*t, 2016). The reasons for not getting consent from both custodial parents/guardians should be documented in the file.
- If consent is obtained from the child's parent(s)/guardian(s), the service provider should document steps taken to verify the custody or guardianship of the child.
- Once the service provider has determined that the child has capacity to consent, or consent to services/counselling has been obtained from the child's parent(s)/guardian(s) on behalf of the child, the consent to services/counselling should be confirmed in writing. The consent should outline the nature of the proposed services/counselling or intervention and should indicate that the child understands the associated benefits and/or risks/consequences. The consent should be signed by the client or their representative and be kept in the client's file for the recommended retention period.
- If the child or parent/guardian has difficulty reading a written consent due to language difficulties, a low level of literacy, or a disability, then the service provider should document the fact that oral consent has been obtained. This documentation should be kept in the client's file for the recommended retention period.
- If the child or parent/guardian cannot understand English, or has other difficulties communicating, an interpreter should be used to assist with an assessment of whether the child has the capacity to consent and to establish that the child (or their parent/guardian) has, in fact, consented.

Strategies to help decide whether a child is able to consent to services/ counselling

- Explain the process, intervention, or procedure to the child, along with the associated benefits and risks. Ask them to outline in their own words what you have just said.
- With input from children or youth, develop a handout that summarizes the process and what it can do or what may happen as a result. Give the handout to the child client at the beginning of the service/counselling relationship and discuss it with them.
- If you are unsure of the child's ability to consent, involve another service provider if possible. Do you both agree that the child is mature enough to make the decision on their own?

2. If the child client is not capable of consenting to receive services/ counselling, what documents are considered acceptable evidence of the referring adult's custody or guardianship?

Background

The provincial *Family Law Act* (FLA) and the federal *Divorce Act* regulate child custody and support in BC. *The Divorce Act* now refers to custody as "decision-making responsibility" and "parenting time." The FLA refers to custody and access as "parenting time." Guardianship is referred to as "parental responsibilities." A person does not have to be the parent of the child to claim parenting time and/or parental responsibility in BC. For instance, step-parents and grandparents may seek contact rights. There is no limit to how many guardians a child can have.

Parental responsibilities mean making major life decisions for a child—i.e., about the child's religious upbringing, educational programs, athletics, recreational activities, and healthcare. Parenting time means the responsibility to care for a child, including day-to-day decision making. After the breakdown of a marriage, both parents typically have parenting time, unless the court orders differently based on the child's best interests. If only one parent is the child's guardian, they will have the decision-making authority for the child, whereas the other parent could have access rights but no authority to make major decisions.

If the parents of a child client live together with the child, each parent has equal rights in terms of parental responsibility. In this case, therefore, if the client is not capable of consenting to receive services, both parents or either one may legally act on behalf of the child in decisions related to a plan for their healthcare.

If the client's parents have separated, the situation is more complex. If no formal agreement regarding parental responsibility has been reached, nor has the court ruled on the matter, then the person who has day-to-day care and control—or the person with whom the child usually lives—is generally considered to have the decision-making power. If day-to-day care and control of the child are shared, then decision-making powers are also shared.

If the question of guardianship has been decided by court order or an agreement exists between the parents, then the guardian of the child has decision-making powers.

If both parents are guardians, then both parents have equal parental responsibility. In this situation, the service provider may rely on the consent of only one parent (Bryce, 2013). Although this is permitted, in general, it is best to make every effort to obtain the consent of both parents. This may not be possible in abusive family situations. If dual consent is not pursued, the service provider should document the reasons for this course of action.

In some cases, one parent (the guardian) may have full parental responsibilities, while both parents have parenting time. In this situation, the guardian is the one who makes day-to-day decisions for the child, including healthcare decisions.

It is important to remember that agreements or court orders may change during the course of service delivery if the family is still involved in legal proceedings. It will be important to revisit some of the above issues periodically.

In cases where a child who is not competent has been found to be in need of protection and has been removed by child protection workers, the director authorized under the CFCSA—or a caregiver authorized by the director—may be entitled by agreement or court order to act as the guardian of the child.

In the absence of a formal agreement or court order, foster parents are not generally considered the guardians of a child. They are not, therefore, entitled to consent on behalf of the child. In this situation, a child protection worker should be consulted for guidance.

Guidelines

- If the referring adult is the child client's parent, the service provider should find out whether there is an agreement or court order in place establishing guardianship of the child. All efforts made by the service provider to determine whether such an agreement or order exists should be documented and kept in the client's file for the recommended retention period. (See Part IV of these *Guidelines* for recommendations related to retention of client records.)
- If the service provider believes an agreement or court order exists regarding guardianship of the child, then the service provider should request a copy from the referring adult or agency. Depending on the circumstances, one or more of the following documents can provide evidence of guardianship:
  - a court order
  - a separation agreement or other agreement regarding care of the child
  - an adoption order

  The service provider should carefully review the court order or other document establishing guardianship.

  The document should be checked to ensure it is up to date. In some cases, parental responsibilities may change during the course of the service relationship with the client. A partner with access rights, for example, may later be granted parental responsibilities. If the service provider is unsure, they can ask the guardian to obtain a current copy from the court registry. A signature from the appropriate court official confirms that the document is still in effect.
- Any documents obtained to verify guardianship should be kept in the client's file for the recommended retention period.

- If it is not possible to obtain a copy of such legal documents, then that fact, along with the information provided orally by the referring adult, should be documented and kept in the client's file for the recommended retention period.
- Consider including in the agency intake form a clause which provides that responsibility for notifying the agency of a change in guardianship arrangements lies with the guardian.
- If the referring adult is the client's parent, and there is no agreement or court order in place regarding guardianship of the child client, the service provider should request that the adult demonstrate that the child lives with them. Any evidence presented by the referring parent should be documented and kept in the client's file for the recommended retention period.
- If the client is referred by MCFD or a Delegated Aboriginal Agency, or by a foster parent, then the service provider should request that the responsible social worker or foster parent provide a copy of the court order establishing who has guardianship of the child.

3. What if the child client provides information that indicates that they need protection?

Background

In some cases, either at intake or later in the service relationship, circumstances may arise which suggest that a child client is in danger. If there is reason to believe a child needs protection, the service provider has a legal duty to promptly report the matter to a child protection worker, under section 14 of the CFCSA. Section 13 of this *Act* describes the circumstances under which it is reasonable to believe a child may need protection. This duty overrides the duty to protect the client's confidentiality. Failure to report is an offence under the *Act*.

If the matter is reported to MCFD or a Delegated Aboriginal Agency, the CFCSA provides that the identity of the person making the report—e.g., the service provider—cannot be disclosed to the child's parent/guardian by the ministry without the reporter's consent.

In collaboration with EVA BC and the BCSTH, as well as other provincial service providers, MCFD has developed best practice approaches for child protection workers in cases involving gender-based violence (Ministry of Children and Family Development, 2014). These MCFD best practice guidelines reiterate that the safety and well-being of children are of paramount concern. They also clarify that, in situations involving gender-based violence, a report to child protection is not automatically required. Each case must be decided in relation to the section 13 criteria.

In addition to laws and policies, accreditation standards also need to be considered. The COA Standards, for example, call for written procedures that outline legal reporting requirements. They also require that service providers be oriented on laws governing suspected abuse and their agencies' disclosure policies.

When is it reasonable to believe a child may be in need of protection?

Section 13 (1) of the CFCSA states that:

A child needs protection in the following circumstances:

a) if the child has been, or is likely to be, physically harmed by the child's parent;

b) if the child has been, or is likely to be, sexually abused or exploited by the child's parent;

c) if the child has been, or is likely to be, physically harmed, sexually abused or sexually exploited by another person and if the child's parent is unwilling or unable to protect the child;

d) if the child has been, or is likely to be, physically harmed because of neglect by the child's parent;

e) if the child is emotionally harmed by the parent's conduct;

f) if the child is deprived of necessary health care;

g) if the child's development is likely to be seriously impaired by a treatable condition and the child's parent refuses to provide or consent to treatment;

h) if the child's parent is unable or unwilling to care for the child and has not made adequate provision for the child's care;

i) if the child is or has been absent from home in circumstances that endanger the child's safety or well-being; made for the child's care;

j) if the child's parent is dead and adequate provision has not been made for the child's care;

k) if the child has been abandoned and adequate provision has not been made for the child's care;

l) if the child is in the care of a director or another person by agreement and the child's parent is unwilling or unable to resume care when the agreement is no longer in force.

(1.1) For the purpose of subsection 1(b) and (c) but without limiting the meaning of "sexually abused" or "sexually exploited," a child has been or is likely to be sexually abused or sexually exploited if the child has been, or is likely to be,
(a) encouraged or helped to engage in prostitution, or
(b) coerced or inveigled into engaging in prostitution.

(1.2) For the purpose of subsection (1)(a) and (c) but without limiting the circumstances that may increase the likelihood of physical harm to a child, the likelihood of physical harm to a child increases when the child is living in a situation where there is domestic violence by or towards a person with whom the child resides.

(2) For the purpose of subsection (1)(e), a child is emotionally harmed if the child demonstrates severe (a) anxiety, (b) depression, (c) withdrawal, or (d) self-destructive or aggressive behaviour.

If a report to MCFD is made and a child protection investigation is started, the ministry may request release of agency records about the client. (See below for practices associated with the release of child client records to parents, guardians, or other third parties to address this situation.)

Guidelines

- If the service provider has reason to believe that a child needs protection, as set out in section 13 of the CFCSA, they have a legal duty to report the matter. Note that with regards to s. 13(1.2), the service provider is not legally required to report to a child protection worker if the only issue is that the child is living in a situation where domestic violence is occurring. However, if the service provider also believes the child is being emotionally or physically harmed, or is likely to be physically harmed, then the service provider does need to report the information to a child protection worker. The service provider should report to a child protection social worker in either an MCFD office or a Delegated Aboriginal Agency.
- If the service provider receives a disclosure of child abuse from a child client, they should provide acknowledgment and support but should not interview the child. If questions are asked by the service provider, they should be short and open-ended, using words that are part of the child's vocabulary. The service provider should record what the child has said using the child's own words.
- The service provider should record carefully any interventions made or actions taken in response to evidence that the child client is in need of protection. This would include recording the report made to MCFD or a Delegated Aboriginal Agency, along with the ministry's response. If, for example, MCFD or the Delegated Aboriginal Agency decides not to take action, this should be noted in the client's file. Any documentation should be kept in the client's file for the recommended retention period.
- The service provider should advise the child client of any agency interventions, unless informing them would impede the due process of law or put the child at further risk of physical or emotional harm.
- If the child client was advised of or consented to the disclosure of information to any third parties, make a note of this fact and include this information in the service record.

How to report

If the child is in immediate danger or a criminal offence has been or will likely be committed against them, call 9-1-1.

Otherwise, call 1-800-663-9122 at any time, day or night.

If the child would like to speak to someone, call the Helpline for Children at 310-1234 (no area code required).

Practices associated with the release of child client records to parents, guardians, or other third parties

1. What if the client's parent/guardian wants access to information from their child's file?

Background

Many of the considerations outlined above regarding a child client's capacity to consent to services/counselling also apply here.

In determining whether your child client is capable of exercising the right to access their record or consent to its release to someone else, consider the following questions:

- Is your client able to understand their rights to confidentiality?
- Is your client able to understand the consequences of disclosure or non-disclosure of information?

For agencies seeking accreditation, it is also important to consider that standards may require the involvement of family members in the delivery of care to the child and the sharing of information with family members.

Whatever standards are applied, they must be interpreted so as to be consistent with legal requirements here in BC. An overview of the applicable laws is outlined below.

The *Personal Information Protection Act* (PIPA) and parents' access to records

Most non-profit agencies will be governed by information sharing rules contained in this *Act* (see Part I of these *Guidelines* for additional information). In addition to its general requirements, PIPA's regulations include rules about parents or guardians getting access to their children's records.

Under PIPA regulations, the right to access a record and the right to request correction of personal information contained in the record may generally be exercised by a parent/guardian on behalf of someone who is under 19 if:

- The child is incapable of exercising those rights themself.

Similar regulations under FIPPA have been interpreted as also requiring that:

- The parent/guardian be seeking access to the child's information to protect or advance the interests of the child and not trying to obtain information for their own use.

As with the process for deciding whether a child is capable of consenting to services, the child's age and individual level of development are considered to determine whether they are capable of making a decision about access to their records. Depending on the circumstances, the maturity of the child, and the type of personal information involved, a child under 19 may or may not be capable of exercising their rights under PIPA regulations.

In particular, children under 12 may not be fully capable of exercising their rights under the *Act*. In practice, 12 years of age is often used by public agencies and service providers as the benchmark for capacity to consent in the healthcare context.

The *Freedom of Information and Protection of Privacy Act* (FIPPA) and parents' access to records

Depending on the wording of their funding contract, some agencies will be covered by this *Act* (see Part I of these *Guidelines* for additional information). FIPPA also has regulations dealing with access to children's records. These rules are substantially similar to those under PIPA. If you are uncertain which *Act* applies, contact your funding ministry's Director/Manager of Information and Privacy.

The *Child, Family and Community Service Act* (CFCSA) and parents' access to records

While everyone is subject to the CFCSA's reporting requirement, most agencies will not be subject to Part 5 of this *Act*. If you have a question or concern in this area, contact your funding ministry's Director/Manager of Information and Privacy for further information.

Questions which help determine whether Part 5 of the CFCSA applies to your agency's records

Is your service currently funded by MCFD, or was it once funded by them?

If yes, were the records in question created on or after January 29, 1996?

If yes, do the records relate to matters or services covered by the CFCSA? Does your contract contain language suggesting the ministry owns the records?

If yes to all of the above, CFCSA Part 5 may apply.

Guidelines

If the records are governed by the CFCSA

- If the child is under 12, the CFCSA provides that the parent or person who has legal care of the child can exercise the child's rights under FIPPA. The parent or legal guardian can:
  - be given access to the child's records
  - consent to disclosure of the information in the record
  - request correction of the record
- If the child is aged 12 or older, the CFCSA provides that the parent or person who has legal care of the child may exercise the child's rights under FIPPA if the child is incapable of exercising those rights themself. In this situation, follow guidelines in Part V related to the intake process *(What is the process for documenting that a child client has consented to receive services?)* with the necessary changes.

If the records are not governed by the CFCSA

- If the client is under 19, the service provider should document steps they have taken to determine whether the client has the capacity to consent to the release of personal information contained in their records. The documentation should be kept in the client's file for the recommended retention period.
- If the service provider determines that the client is not capable of consenting to the release of personal information, then the client's parent/guardian can

consent to the release of information on their behalf. In these cases, the service provider should obtain the necessary documents to verify guardianship and keep these documents in the client's file for the recommended retention period.

- If the service provider believes that the parent/guardian is not acting in the best interests of the child, and access to records is denied on this basis, the reasons for this denial should be well documented—for example, the service provider may want to note in the file that, based on what the child has told them, they believe that releasing the records would put the child or another person at risk of serious emotional or physical harm.
- If the client is not capable of consenting and the referring adult has sole parental responsibility for the child but parenting time is shared, the service provider may obtain consent from the parent who has parental responsibility for the child.
- Once the client's capacity to consent to the release of personal information has been determined, or the child's parent/guardian has consented to the release of this information, written consent should be obtained. The consent should set out the nature of the information to be shared, the recipients of the information, and the purpose for which the information is being shared. The written consent should indicate whether it applies only to information that has already been gathered, or also to information that may be obtained in the future. The written consent should be signed by the client or the parent/guardian and dated. The written consent should be time-limited.
- If the client or parent/guardian has difficulty reading a written consent because of language difficulties, a low level of literacy, or a disability, the service provider should document the fact that oral consent has been obtained. The oral consent should be subject to the same limitations as any written consent and should be kept in the client's file for the recommended retention period.
- If the adult requesting access to client files or information is the client's parent, and there is no court order or parenting/guardianship agreement in place regarding parental responsibility or parenting time with regards to the client, the service provider should request that the parent demonstrate that the client lives with them. For example, the counsellor could request to see a letter addressed to the child or any child identification indicating their address—such as a child safety identification card—and compare this with the address of the referring parent. Any evidence presented by the adult requesting access should be documented and kept in the client's file for the recommended retention period.
- If the client does not have the capacity to consent to the release of information, then the service provider should advise them that information about the counselling process, and possibly about them, may be shared with a parent/guardian if requested.
- If the client has the capacity to consent to the release of information, and the service provider feels it would be beneficial for a parent/guardian to be made aware of aspects of the counselling process or other service being provided, the client should be encouraged to inform these individuals themself. If the service provider intends to provide the information to the parent/guardian directly, then consent for the release of this information should also be obtained from the client prior to the information being released.

2. If the client is not capable of consenting to the release of information, what documents are considered acceptable evidence of the referring adult's custody or guardianship?

Guideline

- Apply the guidelines under Part V *(If the child client is not capable of consenting to receive services/counselling, what documents are considered acceptable evidence of the referring adult's custody or guardianship?)* with the necessary changes.

3. What if the referring parent/guardian, or their lawyer, requests access to client files in preparation for a family law dispute?

Guideline

- If the service provider receives a request—in the form of a letter, for example—from a client's parent or guardian or their lawyer, for access to client files or for information contained in the files, then the considerations and guidelines set out in Part V of these *Guidelines (What if the client's parent/guardian wants access to information from their child's file?)* apply. If the client is capable of consenting and the agency wishes to release the information, the client must consent to the release of information. If the client is not capable, then the parent/guardian can consent on their behalf.

4. What if the other parent/guardian, or their lawyer, requests access to client files in preparation for a family law dispute?

Guideline

- If the service provider receives a request—in the form of a letter, for example—from the other (non-referring) parent/guardian, or their lawyer, for access to client files or for information contained in the files, then the considerations and guidelines set out in Part V of these *Guidelines (What if the client's parent/guardian wants access to information from their child's file?)* apply. If the client is capable of doing so, they must consent to the release of information before the agency proceeds. If the client is not capable, and the agency does not have reason to argue against the release of information, then the referring parent/guardian can consent on their child's behalf. If the other parent shares equal parenting responsibility for the child but the service provider believes that releasing the client's files or information contained in the files could reasonably be expected to threaten the client's or anyone else's safety or mental or physical health, then access to the child's files can be denied. If access to records by a parent/guardian is denied, the reasons for denying access should be noted in the file (e.g., that the service provider believes, based on what the child has told them, that releasing the information would put the child at risk of emotional or physical harm). The reasons should be retained in the file for the recommended retention period.

5. What if a family justice counsellor, social worker, or other individual requests access to client records in the context of a family law dispute?

Background

Under the FLA, a court may order an assessment to be conducted for the purpose of a proceeding under Part 4 *(Care of and Time with Children)*. The court will designate a person to conduct the investigation to determine the needs and/or views of the child. This person will prepare a report (sometimes referred to as a "section 211 report") for the court on the results of the assessment. The assessment will be carried out by a family justice counsellor, a social worker, a psychologist, or another person approved by the court. The assessor should not have had any prior connection to the parties, unless the parties each consent.

Guidelines

- If a family justice counsellor, social worker, psychologist, or other individual requests client records for the purposes of conducting an assessment into family matters in the context of a family law dispute (under section 211 of the FLA), the service provider should—before releasing any records—request a copy of the court order directing that the assessment be conducted and designating that person as the assessor. The service provider should also request that the appointed individual provide copies of any consents they have obtained for the release of client information. If a broadly worded consent is provided, the service provider should insist that the producer of the consent form be specific about what records are needed.
- If a copy of the court order and the necessary consents are provided, then client records should be released to the person carrying out the assessment. The service provider may also consult orally with the assessor, if necessary. Copies of the court order and consents should be kept in the client file for the recommended retention period.

6. What other types of situations could arise in which the release of client records might be required?

Background

Section 65 of the CFCSA provides that, in the context of a child protection investigation, a director (a person designated by the minister under s. 91, CFCSA) may apply to the court for an order requiring a person or organization to produce a record to the director if there are reasonable grounds to believe the record contains information necessary to determine whether the child is in need of protection.

Generally, in the absence of a court order, a community-based agency is not legally required to release client records to a child protection worker. If, however, the agency's records are under the custody or control of a public body, as defined in FIPA, then the director has the right to access the records without a court order, provided the information is necessary to enable the director to perform their functions under the *Act* (s.96, CFCSA).

It is also possible that an abusive or non-custodial parent might try to bring a civil case against a service provider or their agency for failing to involve the parent in the child's

counselling or other service delivery process. The parent might, for example, claim professional negligence or some other civil cause of action. This process would be initiated by a Writ of Summons and a Statement of Claim. If the civil case goes forward, the child client's files might be reviewed as part of the discovery process.

Guidelines

- If the service provider receives a request from MCFD or a Delegated Aboriginal Agency to produce a child client's record for the purposes of determining whether the child is in need of protection under section 65 of the CFCSA, the service provider is not legally required to release the client records to the ministry unless there is a court order to this effect. The service provider should consider releasing the record voluntarily, however, unless compelling reasons exist for refusing to do so.
- If the service provider receives a request from MCFD or a Delegated Aboriginal Agency to produce a child client's record for the purposes of determining whether the child is in need of protection, the service provider should consider advising the client or their parent/guardian that the records have been requested, unless this would place the client at further risk of emotional or physical harm.
- If the agency's records are under the custody or control of a public body and the service provider receives a section 96 request to provide information in a client's file that is necessary for the director to perform their functions under the CFCSA, then the service provider should ask for the request in writing and for written confirmation of the ministry's designation of the person as a director under section 91 of the *Act*. (See Part I of these *Guidelines* on FIPPA for factors affecting whether or not the records are under the ministry's custody or control.)
- If the service provider or the agency is served with a Writ of Summons or Statement of Claim, they should consult with a lawyer.

References

British Columbia. (2014). Ministry of Children and Family Development. Best Practice Approaches: Child Protection and Violence Against Women.

British Columbia. (2015). *Report of the Special Committee to Review the Personal Information Protection Ac*t. Online, https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/3rd-session/pipa/reports/PDF/Rpt-PIPA-40-3-Report-2015-FEB-06.pdf

British Columbia. (2017). *The B.C. Handbook for Action on Child Abuse and Neglect*. Online, https://www2.gov.bc.ca/assets/gov/public-safety-and-emergency-services/public-safety/protecting-children/childabusepreventionhandbook_serviceprovider.pdf

British Columbia. (2021). "Reporting Child Abuse in BC." Online, https://www2.gov.bc.ca/gov/content/safety/public-safety/protecting-children/reporting-child-abuse

Bryce, G. (2013). *Consent to Counselling Therapy Services: What counsellors need to know about the law of consent before they provide counselling therapy services to their clients*. Online, https://bcacc.ca/wp-content/uploads/2015/10/130726-Commentary-re-Consent-to-Counselling.pdf

Bryce, G. (2015). *Consent of minors to counselling therapy and disclosure of their personal information*. Online, https://bcacc.ca/wp-content/uploads/2015/10/Practice-Summary-Consent-of-Minors-Update-June-25-2015.pdf

Canadian Counselling and Psychotherapy Association (April 2015). *Standards of Practice, 5th Edition*. Online, https://www.ccpa-accp.ca/wp-content/uploads/2015/07/StandardsOfPractice_en_June2015.pdf

CARF International. (2021). Online, http://www.carf.org/home/

Cory, J., Ruebsaat, G., Hankivsky, O., & Dechief, L. (2003). *Reasonable Doubt: The Use of Health Records in Criminal and Civil Cases of Violence Against Women in Relationships*. Vancouver, BC: BC Women's Hospital and Health Centre Woman Abuse Response Program. Online, https://www.bcifv.org/resources/healthrecordsbrochure02.pdf

Council on Accreditation. (2021). Online, https://coanet.org/

Ending Violence Association of BC. (June 2017). *Interagency Case Assessment Teams Best Practices: Working Together to Reduce the Risk of Domestic Violence*. Instructions as to how to obtain a copy are found online: https://endingviolence.org/prevention-programs/ccws-program/interagency-case-assessment-teams-icats/

Ending Violence Association of BC. (March 2019). *Third Party Reporting Guidebook 2.0: Increasing Reporting Options for Sexual Assault Survivors*. Online, https://endingviolence.org/publications/third-party-reporting-guidebook-increasing-reporting-options-for-sexual-assault-victims-november-2015/

Ending Violence Association of BC. (July 9, 2020). *Privacy Tips for Anti-Violence Advocates Working from Hom*e. Online, https://endingviolence.org/publications/privacy-tips-for-anti-violence-advocates-working-from-home/

Family Law Act, [SBC 2011] CHAPTER 25

Fortinet. (2021). "Thin Client." Online, https://www.fortinet.com/resources/cyberglossary/thin-client

Gold, Alan. (2020). HCR-231 *Production of personal records of complainants and witnesses*. Halsbury's Laws of Canada-Criminal Offences and Defences.

Government of Canada, Canadian Radio-television and Telecommunications Commission. (2021). *Canada's Anti-Spam Legislation*. Online, https://crtc.gc.ca/eng/internet/anti.htm

Jacuk, C. & Hassan, H.R. (2018). *Third Party Records: A Review of the Case Law from 2011–2017*. Department of Justice. Online, https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd11-rr11/p6.html

Law Society of British Columbia. (2021). Code of Professional Conduct for British Columbia: Chapter 3 – Relationship to Clients – annotated. Online, https://www.lawsociety.bc.ca/support-and-resources-for-lawyers/act-rules-and-code/code-of-professional-conduct-for-british-columbia/chapter-3-%E2%80%93-relationship-to-clients/

Limitation Act [SBC 2012] CHAPTER 13

M.(A.) v. Ryan, [1997] 1 SCR 157

McInerey v. MacDonald, (1992) 93 DLR (4d) 415 (SCC)

Ministry of Justice, Civil Policy and Legislation Office. (2012). *New Limitation Act Questions and Answers*. Online, https://www2.gov.bc.ca/assets/gov/law-crime-and-justice/about-bc-justice-system/legislation-policy/limitation-act/la_qas.pdf

Office of the Information and Privacy Commissioner for British Columbia. (February 2005). *Faxing and Emailing Personal Information*. Online, https://www.bchousing.org/publications/GD_Fax-Email.pdf

Office of the Information and Privacy Commissioner for British Columbia. (January 2015). *Protecting Personal Information Outside the Office*. Online, https://www.oipc.bc.ca/guidance-documents/1447

Office of the Information and Privacy Commissioner for British Columbia. (October 2015). *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*. Online, https://www.oipc.bc.ca/guidance-documents/1438

Office of the Information and Privacy Commissioner for British Columbia. (October 2016). *Mobile Devices: Tips for Security & Privacy*. Online, https://www.oipc.bc.ca/guidance-documents/1994

Office of the Information and Privacy Commissioner for British Columbia. (March 2019). *Developing a Privacy Policy Under PIPA*. Online, https://www.oipc.bc.ca/guidance-documents/2286

Office of the Information and Privacy Commissioner for British Columbia. (September 2019). *Disclosure of personal information of individuals in crisis*. Online, https://www.oipc.bc.ca/guidance-documents/2336

Office of the Information and Privacy Commissioner for Ontario. (March 1996). *Privacy Protection Principles for Voice Mail Systems*.

Office of the Information and Privacy Commissioner of Canada. (May 2018). *Obtaining Meaningful Consent*. Online, https://www.oipc.bc.ca/guidance-documents/2255

Office of the Privacy Commissioner of Canada. (2020). *Canada's anti-spam legislation*. Online, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/canadas-anti-spam-legislation/

Offices of the Privacy Commissioners of Canada, Alberta and British Columbia. (August 2015). *Contemplating a Bring Your Own Device (BYOD) program*? Online, https://www.oipc.bc.ca/guidance-documents/1828

Offices of the Privacy Commissioners of Canada, Alberta and British Columbia. (October 2020). *Securing person information: A self-assessment tool for public bodies and organizations*. Online, https://www.oipc.bc.ca/guidance-documents/1439

PCMag. (June 29, 2020). "What is Cloud Computing?" Online, https://www.pcmag.com/news/what-is-cloud-computing

Peace Geeks. (May 3, 2020). "COVID Blog #5: A Survivor's Resource Guide on Tech Safety and Support – Combating Domestic Violence During and Beyond COVID-19." Online, https://peacegeeks.org/news/covid-blog-5-survivor's-resource-guide-tech-safetyandsupport-––combating-domestic-violence

Truth and Reconciliation Commission of Canada. (2015). *Honouring the Truth, Reconciling for the Future*. Online, http://www.trc.ca/assets/pdf/Executive_Summary_English_Web.pdf

R. v. Bero, [2000] OJ No. 4199, 151 CCC (3d) 545

R. v. Carosella, [1997] 1 SCR 80

R. v. Grant, 2015 SCC 9, 1 SCR 475

R. v. Lyttle, 2004 SCC 5

R. v. McNeil, [2009] SCJ No. 3, [2009] 1 SCR 66

R. v. Mills, [1999] 3 SCR 668

R. v. Neidig, [2015] BCJ No. 2585, 332 CCC (3d) 370

R. v. O'Connor, [1995] 4 SCR 411

R. v. Osolin, (1994) 86 CCC (3d) 481 (SCC)

R. v. Quesnelle, 2014 SCC 46

R. v. R.V., 2019 SCC 41

R. v. Seaboyer, (1991) 66 CCC (3d) 321, (SCC)

R. v. Shearing, [2002] 3 SCR 33

R. v. Stinchcombe, (1991) 68 CCC (3d) 1 (SCC)

Glossary

Agency: Includes any community-based agency that receives funding and delivers services pursuant to the following programs:

1. Stopping the Violence Counselling
2. Stopping the Violence and Multicultural Outreach
3. Community-Based Victim Services

These funded programs are often housed in agencies which may also operate a variety of family service programs, including transition houses and Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) programs for children and youth experiencing violence.

Agency staff: Paid and unpaid support or administrative staff, counsellors, victim service workers, and outreach workers.

BCSTH: BC Society of Transition Houses.

CFCSA: *Child, Family and Community Service Act*.

Child: A person aged 18 years or under.

Clients: Adult and child victims/survivors of gender-based violence who are being provided with crisis intervention, information, and support regarding the justice system, or who are being provided with counselling services.

CARF: Commission on Accreditation of Rehabilitation Facilities. COA: Council on Accreditation for Children and Family Services.

EVA BC: Ending Violence Association of BC.

File: A folder, physical or digital, or other container in which records (such as notes) are arranged for reference or retrieval.

FIPPA: *Freedom of Information and Protection of Privacy Act*.

Limitation period: The period of time after which legal actions—related to an alleged civil or criminal assault or another wrongful act—can no longer be initiated.

MPSSG: Ministry of Public Safety and Solicitor General.

MCFD: Ministry of Children and Family Development.

Personal information: Information that would identify a particular person—for example, information such as their name, home address or phone number, medical information, marital status, or educational history. Personal information does not include contact information that enables someone to be contacted at a place of business for business purposes.

PIPA: *Personal Information Protection Act*.

Prospective clients: Individuals who have requested but have not yet received services. Prospective clients may be on a waitlist or may be in the process of filling out an agency intake record, such as an application for service.

Record: All recorded information, regardless of its physical format. A record might include:

- filled-out forms
- handwritten, typed, or computerized notes
- video or audio tapes or files
- photos

Server: A piece of equipment that stores information from computers on a network.

STV: Stopping the Violence.

Operational record: A record that relates to the operations or services provided by the agency according to its mandate. Operational records are distinct from administrative records, which relate to the management of the agency. Agencies will have a variety of specific forms or systems of documentation. The *Guidelines* deal primarily with operational records of two basic types:

1. **Intake record:** Refers to the record containing the details of the agency's first contact with a prospective client. It might include, for example, an application for service or an intake form. It might also include a record of hospital, police, or other system accompaniment by agency staff or volunteers.
2. **Service record:** Refers to the running record that documents the ongoing service the client is receiving from the agency. It might include, for example, documentation of justice system information and practical support provided by the agency. Such documentation might consist of letters of advocacy written on behalf of a client, Crime Victim Assistance forms, release or consent forms, or notes of upcoming court dates. The service record should also include documentation of the counselling service provided, if applicable. This might consist of assessment tools, progress or case notes made during the course of counselling, consent forms, or termination summary notes.

Service providers: Agency staff who are employees and who are delivering services as part of a contract between the agency and the provincial government.

ENDING VIOLENCE
Association of BC

CONTACT
510 – 1155 West Pender Street
Vancouver, BC V6E 2P4

PHONE
604-633-2506

ONLINE
endingviolence.org