MANITOBA OMBUDSMAN

Guidance for Public Bodies & Trustees

Permissible Disclosure of Personal Information to Reduce or Eliminate Intimate Partner Violence (IPV) Harm

This guidance outlines key points to keep in mind when deciding whether to share personal information to help reduce or prevent a serious risk to someone's health or safety related to intimate partner violence (IPV).

IPV is a pervasive problem in Canada, primarily harming women and gender-diverse individuals. In 2023, there were 123,319 victims (aged 12 years and older) of IPV reported to police.[1] Recognizing this issue, privacy authorities across Canada have jointly endorsed a resolution promoting responsible disclosure of personal information in cases of IPV.[2]

The timely and responsible disclosure of personal information is a critical component of IPV prevention to reduce or eliminate a serious health or safety concern for an at-risk individual(s). Consideration must be given to provide only the minimum amount of information necessary to an at-risk individual(s) or an entity that needs this information, to enable an informed decision and appropriate actions to eliminate or reduce a risk of serious harm.

Privacy should not present a barrier when an individual's health or safety is at risk.

Manitoba's Privacy Laws

Information sharing in Manitoba is governed by two key statutes: The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA), which set out the rules for collecting, using and disclosing personal and personal health information across public bodies and trustees.

Manitoba's privacy laws allow for the sharing of personal information in specific circumstances to prevent situations of risk to life, health or safety.[3][4] These circumstances may occur across a wide range of public sectors and programs including, but not limited to, justice, child and family services, education, and health care.

Who is this guidance intended for?

This guidance is intended for public body (defined under FIPPA) and trustee (defined under PHIA) employees who may be involved in assessing or responding to risks of serious harm while providing services to the public. It is especially relevant to those working in contexts where intimate partner violence, health and safety concerns, or cross-sector collaboration may require the sharing of personal information.

How should this guidance be used?

This guidance should be considered alongside any organizational guidelines, policies, procedures and training related to the sharing of personal information. It should be interpreted in conjunction with relevant legislation, internal protocols, regulatory obligations, and supplementary resources, including assessment frameworks to mitigate the risk of IPV. This document does not constitute legal advice and should not be relied upon as such. It also does not limit or predetermine the discretion of the Manitoba Ombudsman in deciding complaints submitted under FIPPA or PHIA.

Requirements under Manitoba law

Sharing to reduce serious harm

As permitted by section 44(1)(l) of FIPPA, public body employees may share personal information without consent if it is reasonably necessary to protect the mental or physical health or safety of any individual or group of individuals.

Under section 22(2)(b) of PHIA, personal information may be shared without consent if a trustee reasonably believes it is necessary to prevent or lessen a risk of harm to the health or safety of a minor, or a risk of serious harm to the health or safety of the individual the information is about or another individual, or to public health or public safety.

Assessing the risk of IPV requires consideration of current or past indicators of harm to decide if there is a reasonable basis to believe there is some potential threat or danger to an individual. Depending on the situation, indicators might include statements, actions, behaviours, a history of violence, or a criminal history. The following principles should be considered when assessing risk:

- Disclosure decisions which are based on a thoughtful review of the situation, available facts, and relevant legal rules are generally considered reasonable.
- A serious risk may warrant disclosure of personal information even if it's unclear whether the situation will escalate and cause harm. Uncertainty about the outcome does not invalidate the concern.

- Sharing personal information in good faith is not a breach simply because the expected harm didn't occur. Choosing not to share personal information is also acceptable if the decision is made responsibly, taking into account whether there is any basis for determining a potential threat, danger or harm exists.
- Organizations, service providers, and their staff are generally protected from liability under Manitoba's privacy laws if sharing personal information is generally reasonable in the circumstances and is done in good faith.

Justice sector example on assessing risk

Mark has a history of harassment charges involving violence toward his former partner, Claire. After receiving a suspended sentence, he's required to attend a violence prevention program and meet regularly with both his probation officer and a community counsellor.

During a session, Mark tells the counsellor that he's been "watching Claire's apartment" and feels he needs to "teach her a lesson." Concerned by the escalation in language and behaviour, the counsellor documents the statement and immediately contacts the probation officer. To assess the risk they:

- Review Mark's prior charges and history of stalking behaviour
- Note current warning signs: obsessive monitoring, threatening language, and emotional volatility
- Use a validated risk assessment tool to evaluate the likelihood of future harm
- Consider both static factors (e.g., prior convictions, breach history) and dynamic ones (e.g., recent escalation, lack of remorse)

The assessment indicates a high risk of serious harm. Based on this and their professional judgment, the probation officer initiates protective measures. Knowing Claire receives support from a local outreach program, the officer shares Mark's personal information with program staff, and advises them Mark recently made threats towards Claire. The officer also notifies police. Disclosure to Mark is delayed until Claire's safety is secured and the risk is actively managed.

This example illustrates how personal information may be shared under Manitoba's privacy laws when necessary to reduce or eliminate a serious threat, and how such disclosures are grounded in good faith and professional judgment.

Consulting with someone if there may be risks in sharing their information

Manitoba's privacy laws permit the sharing of personal information without consent in certain situations, including when there is a risk of serious harm to an individual's health or safety. However, this does not prevent you from consulting a victim about the impact sharing their personal information may have related to their health or safety. For example, you may need to consider consulting the victim or survivor in situations where:

- sharing could place the at-risk individual at greater risk of harm, for example, where sharing could lead to a criminal charge which could reasonably be expected to escalate the risk of harm to the victim or survivor prior to the development of a safety plan
- sharing with another organization or service provider may lead to personal information also being shared with the police

The decision on whether personal information should be shared without consent can be difficult and must be carefully assessed based on the information available and all relevant considerations. Decisions to share or not share information, when made based on these relevant factors, will generally be considered to have been made in good faith and reasonable in accordance with Manitoba's privacy laws.

Sharing for the same purpose or a consistent purpose

As provided by sections 43(a) and 44(1)(a) of FIPPA, as well as section 21(1)(a) of PHIA, public body employees and trustees can share personal information for the purpose for which it was obtained or compelled or for a consistent purpose. A "consistent purpose" depends on whether the personal information was collected directly from the individual or from a different source.

Sharing if permitted or required by law

Sections 44(1)(d) and (e) of FIPPA, as well as section 21(1)(f) of PHIA provide that public body employees and trustees can share personal information if it is permitted or required by another law, treaty, agreement, or enactment of Manitoba or Canada.

Sharing to aid police

Under section 44(1)(r) of FIPPA, public body employees may share personal information with police for law enforcement purposes or crime prevention.

Justice sector example on sharing information for a consistent purpose

Sophie is a university student living with her boyfriend Daniel. Over the past few months, Daniel has become increasingly controlling – monitoring Sophie's phone, isolating her from friends, and frequently accusing her of being unfaithful. After a heated argument, Daniel blocks the door and threatens to harm her if she tries to leave.

Terrified, Sophie manages to send a text to a friend who calls police. When officers arrive, Sophie is visibly shaken and discloses the pattern of escalating threats and intimidation. Daniel is arrested for uttering threats and unlawful confinement. Recognizing Sophie's vulnerability and lack of nearby family members, the officers refer her to a local crisis centre for support with safety planning and trauma counselling.

In this case, Sophie would reasonably expect that the personal information she shared with police to protect herself from Daniel would be disclosed by police to shelter organizations to help her access services that support her safety and recovery. The disclosure is consistent with preventing a risk of harm to the individual's safety and health.

Social services example on sharing to aid police

Jean, an Employment and Income Assistance (EIA) worker, meets with her client Sarah. Sarah has bruising to her face and difficulty walking and tells Jean that she was physically assaulted by her partner Jim. Jean talks to Sarah about the importance of her safety and that Jean must contact the police to investigate and ensure Sarah's safety.

Jean's disclosure of the incident Sarah experienced to police is permitted under FIPPA, because the purpose for the disclosure is for law enforcement.

Reporting a child in need of protection

Under section 18 of The Child and Family Services Act, anyone who reasonably believes that a child may need protection must immediately report that information to a child protection agency or to the child's parent or guardian, unless otherwise specified. The duty to report applies even when the information was obtained through professional duties or within a confidential relationship, except for solicitor-client privilege. Failing to report a child to be in need of protection is also an offence under the act.

Family services example on sharing to report a child in need of protection

Jane comes to the emergency room with a broken arm. She discloses that her broken arm was sustained in a fight with her partner, who threatened to hurt their eight-year-old child. Concerned with the threat to the child's safety, staff document the statement and assess whether there is information to reasonably believe a child may need protection. Staff review internal policies as well as section 17 of The Child and Family Services Act to assess whether it is reasonable to believe a child may be in need of protection. After considering all the information and their belief that both the mother and child are at risk of harm, the staff use their professional judgment and report the information to a child protection agency. The agency will need to know the full extent of risk of future violence to develop a protection plan that considers safety for the mother so she may in turn protect her child.

This example illustrates how sharing personal information is a legislative requirement in some cases, and that FIPPA and PHIA do not prevent information sharing where required by law.

Sharing under The Disclosure to Protect Against Intimate Partner Violence Act

The Disclosure to Protect Against Intimate Partner Violence Act (Clare's Law) received Royal Assent on November 3, 2022. The act has been proposed to come into force in Manitoba at the end of 2025. Proposed regulations under Clare's Law establish a process for individuals at risk of intimate partner violence to access information about their partner's documented history of violence. The proposed regulation sets out procedures for individuals to access information, assessing risk of intimate partner violence, as well as disclosing and sharing information.

Best practices

Data minimization

Disclosures should be limited to the minimum amount of personal information required to reduce or eliminate the risk of serious harm. If non-personal information can achieve the same outcome, it should be used instead. In complex cases, staff should consult with supervisors, legal counsel, or other appropriate resources to determine what information is necessary.

Documentation

All disclosures of personal information should be documented using a consistent format that demonstrates the decision was made on reasonable grounds and in good faith. Documentation should reference applicable privacy laws and align with organizational recordkeeping policies.

Preventing privacy paralysis

Privacy paralysis is a common issue affecting public body employees and trustees working in IPV-related contexts. Staff may experience uncertainty about whether privacy laws permit disclosure of personal information. This uncertainty can lead to hesitation or inaction which has been identified as a barrier to effective risk mitigation. Organizations need to develop tools to help staff assess when disclosure of personal information is permitted so they can confidently respond in relevant situations. Organizations must also ensure staff regularly review these tools.

Staff should take a proactive approach by assessing the situation early, seeking guidance when needed, and documenting their reasoning to support timely and informed decisions about whether to disclose or not. As noted above, this work should be supported by relevant workplace guidelines, policies and training on permissible disclosures.

Protecting personal information

Organizations should implement appropriate privacy and security controls to protect the personal information they hold. This includes, but is not limited to, internal processes to detect unauthorized access, use, or disclosure, and response plans to address and mitigate privacy breaches.

Transparency and accountability

Governance frameworks should promote transparency in how IPV-related programs collect, use, and share personal information. Individuals and the broader public should be informed about when personal information may be disclosed, to who, and under what circumstances.

Trauma informed approach

Organizations should adopt a trauma-informed approach that enhances the safety, privacy, autonomy, and resilience of victims or survivors. This includes culturally sensitive practices that recognize and respect individuals' intersectional identities and lived experiences.

Indigenous governance and sovereignty rights

Organizations must respect the governance and sovereignty rights of First Nations, Inuit, and Métis individuals, governments, and communities. Staff should be familiar with principles such as OCAP (Ownership, Control, Access, and Possession) which guide how First Nations data and personal information should be collected, protected, and shared.[5]

Multi-sectoral collaboration

Effective risk management often involves multi-sectoral collaboration. Risk intervention models allow organizations and service providers to work together to identify and respond to threats or behaviours that pose a serious risk of harm to individuals.

Endnotes

1 https://www.ombudsman.mb.ca/federal-provincial-and-territorial-privacy-regulators-address-responsible-information-sharing-in-situations-involving-intimate-partner-violence/
2 https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_241010_ipv/
3 The Freedom of Information and Protection of Privacy Act, CCSM c F175.
4 The Personal Health Information Act, CCSM c P33.5.
5 https://fnigc.ca/ocap-training/

Acknowledgement

This guidance was developed in part from the Office of the Information and Privacy Commissioner of Ontario's (IPC) Sharing Information in Situations Involving Intimate Partner Violence: Guidance for Professionals. The Manitoba Ombudsman would like to thank the Ontario IPC for sharing their knowledge and expertise with our office.

Created November 2025
This information is available in alternate formats on request.
www.ombudsman.mb.ca | ombudman@ombudsman.mb.ca | 1-800-665-0531