PRIVACY

MAY 2024

Sharing Information in Situations Involving Intimate Partner Violence: Guidance for Professionals

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

This guidance by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only. It is intended to enhance understanding of rights and obligations under Ontario's privacy laws for sharing personal information or personal health information around the risk of intimate partner violence. It should not be relied on as legal advice, nor does it bind the IPC which may be called upon to independently investigate and decide on an individual privacy complaint or access to information appeal based on the specific facts and circumstances of a given case. This guidance is subject to change. For the most up-to-date version of this guidance, visit our website: **www.ipc.on.ca**. To access the text of privacy legislation or other relevant statutes, visit Ontario's **e-laws** and Canada's **Justice Laws Website**.

If you, or someone you know, is dealing with an immediate health or safety risk, contact 9-1-1 directly.

Acknowledgement

The Information and Privacy Commissioner of Ontario would like to thank the following organizations, service providers, and individuals for their expertise and collaboration in the development of this guidance:

- Alliance for Healthier Communities
- Association of Native Child and Family Services Agencies of Ontario
- Barrie Police Service
- Bernadette McCann House
- Building a Bigger Wave
- Catholic Family Services Peel-Dufferin
- College of Psychologists of Ontario
- Domestic Violence Death Review Committee
- Inquest Counsel to Ending Violence Against Women (EVA)-Renfrew County
- Lanark County Interval House and Community Support
- Luke's Place
- Ministry of Children, Community and Social Services
- Ontario Association of Chiefs of Police
- Ontario Association of Children's Aid Societies
- Ontario Association of Interval and Transition Houses
- Ontario College of Social Workers and Social Service Workers
- Office for Victims of Crime
- Ontario Victims Services
- Toronto Police Services
- Victim Services of Renfrew County
- WomanACT
- IPV survivors focus group (convened with WomanACT)

Contents

Introduction 1

- Why this guidance? 1
- Who is this guidance for? 2
- Key points from this guidance 3

Privacy laws in Ontario 4

- Which Ontario privacy law applies? 4
- The focus of this guidance 5

Sharing personal information under Ontario's privacy laws 5

- Consent-based practices 5
- Sharing to reduce serious harm (without consent) 6
- Justice sector: compelling circumstances under FIPPA and MFIPPA 7
- Health care sector: risk of serious harm under PHIPA 10
- Child, youth, and family services sector: risk of serious harm under the CYFSA 13
- IPV services sector: a risk of serious harm approach 15

Other potential pathways to share personal information 17

- Sharing for the same purpose or a consistent purpose 17
- Sharing if permitted or required by law 18
- Sharing to aid police 18
- Sharing to protect children from IPV harm 19

Good governance around sharing personal information 21

- Health and safety first 21
- Protecting personal information 21
- Transparency and accountability 21
- Necessity and proportionality 21
- Documentation 22
- Trauma and violence-informed approach 22
- Indigenous governance and sovereignty rights 22
- Multi-sectoral collaboration for risk management and response 22

Conclusion 23

Terms and concepts used in this guidance 23

Introduction

Why this guidance?

This guidance was developed in response to a **coroner's inquest** into the deaths of Carol Culleton, Anastasia Kuzyk, and Nathalie Warmerdam in Renfrew County, Ontario, due to intimate partner violence (IPV). The inquest jury called on the Office of the Information and Privacy Commissioner of Ontario (IPC) to develop guidance for IPV professionals to make informed decisions about privacy, confidentiality, and public safety, particularly around assessing and reducing IPV risk.

In consulting with relevant organizations and service providers, the IPC became aware that IPV professionals (staff) sometimes feel that they are not permitted to disclose personal information or personal health information (personal information) due to perceived barriers under Ontario's privacy laws. When staff do not have the consent of a victim or survivor, abusive partner, or other individual(s) involved (for example, a child), they sometimes feel conflicted about how to respond to a situation when there is a risk of serious harm because privacy rights appear to conflict with health or safety concerns.

The IPC recognizes that multiple sectors are responsible for assessing and reducing IPV harm, including justice, health, child, youth, and family (children and family) services, and IPV services sectors. Each sector may also be subject to different privacy laws. To support collaboration, this guidance provides an overview of key provisions under Ontario's privacy laws that permit sharing[1] personal information without consent, with an emphasis on the provisions related to risk of serious harm around individual health or safety. This guidance also discusses consent-based sharing.

This guidance helps support your organizational policies and practices for sharing personal information. It should be read alongside applicable laws, policies, requirements, and other guidance, such as evidence-based risk assessment tools that incorporate **risk factors associated with IPV perpetration**. It is also important to understand Indigenous governance and sovereignty rights of First Nations, Inuit, and Métis individuals and respect and uphold their data and privacy rights. The design and delivery of IPV prevention programs should also carefully consider the intersectional identities of the individuals they serve. Programs should include a trauma- and violence-informed approach that acknowledges historical, cultural, and internal biases. This approach can help prevent further victimization of individuals, who may be from Indigenous, Black, or other racialized and vulnerable communities.

1 This guidance uses the term "sharing" to refer to disclosure.

Who is this guidance for?

This guidance is for organizations, service providers, and their staff in four sectors: the justice sector, the children and family services sector, the health care sector, and the IPV services sector.

The **justice sector** can include:

- Crown counsel
- band representatives and Indigenous justice providers
- Victim/Witness Assistance Program (V/WAP) and staff
- corrections, parole, and probation (including youth correctional facilities and youth probation services)
- municipal, provincial, and Indigenous police services across Ontario
- Legal Aid/Office of the Children's Lawyer

The **children and family services sector** can include:

- child welfare
- residential/out-of-home care
- adoption
- youth justice
- children's mental health
- family service agencies
- First Nations, Inuit, and Métis child and family services

The **health care sector** can include:

- regulated health professions who provide health care (for example, doctors, nurses, psychologists, social workers and social service workers, and pharmacists)
- psychotherapists and counsellors
- hospitals
- paramedics providing ambulance services
- primary care offices
- pharmacies
- hospital-based sexual assault and domestic violence treatment centres

The **IPV services sector** can include:

- women's shelters and transitional homes
- Indigenous community services and healing lodges
- crisis and emergency shelters
- community-based sexual assault centres
- Partner Assault Response (PAR) programs and staff
- social welfare services (for example, immigration services)
- provincial advocates and coordinators to end violence against women

Key points from this guidance

Sharing personal information must comply with legal requirements	Ontario's privacy laws set the rules for sharing personal information for institutions, children and family service providers, and health information custodians. Personal information can be shared only if there is consent from the individual the personal information is about, or if the sharing is permitted or required by law.
Privacy is not a barrier to protecting health or safety	Ontario's privacy laws permit sharing personal information with an individual at risk of IPV, an organization, or service provider who can help reduce or eliminate a risk of serious harm to an individual's health or safety.
Protection from liability when acting in good faith	Organizations, service providers, and their staff are generally protected from liability under Ontario's privacy laws if sharing personal information is reasonable in the circumstances and is done in good faith.
Good governance frameworks to protect personal information	Organizations, service providers, and their staff should establish governance frameworks, with clearly defined policies and practices, to inform lawful and responsible decision-making around sharing personal information.

Privacy laws in Ontario

Which Ontario privacy law applies?

As an organization or service provider, you should determine which Ontario privacy statute applies to you.

The following table summarizes which Ontario privacy statute generally applies to the following organizations and service providers:

Ontario privacy statute	Generally, applies to
Freedom of Information and Protection of Privacy Act (FIPPA) *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)	institutions or parts of institutions, including, but not limited to, those in the justice sector[2]
Part X of the *Child, Youth and Family Services Act* (CYFSA)	service providers in the children and family services sector[3]
Personal Health Information Protection Act (PHIPA)	health information custodians in the health care sector[4]

Ontario's privacy statutes set the rules for organizations, service providers, and their staff in the justice sector, the children and family services sector, and the health care sector to:

- collect, use, and share personal information
- provide individuals with access to their personal information
- apply the safeguards necessary to keep personal information confidential and secure
- share personal information when there is consent or as permitted or required by law[5]

The IPV services sector does not have its own provincial privacy statute. This sector may wish to consider adapting the CYFSA's approach around "risk of serious harm" to support their policies and practices around sharing personal information. For any other organization or service provider that is generally not subject to any of Ontario's privacy statutes, you should become familiar with the privacy provisions discussed in this guidance and should also consider adapting them as best practices.

2 See section 2(1) of FIPPA and MFIPPA.

3 See sections 2(1) and 281 of the CYFSA.

4 See sections 2, 3, and 17 of PHIPA.

5 See sections 38(2), 41, 42, and 43 of FIPPA; sections 28(2), 31, 32, and 33 of MFIPPA; sections 286, 287, and 288 of the CYFSA; and sections 29, 30, and 31 of PHIPA.

The focus of this guidance

This guidance focuses on the sharing of personal information, including when there is a risk of serious harm concerning health or safety. It does not focus on permissible collection(s) and use(s) of personal information. Organizations, service providers, and their staff must ensure they are permitted to collect and use the personal information provided to them.

Find out more about the collection and use of personal information in the following IPC resources:

- **Collection and use of personal information** under FIPPA and MFIPPA
- **Collection and use of personal information** under Part X of the CYFSA
- **Collection and use of personal health information** under PHIPA

Sharing personal information under Ontario's privacy laws

Sharing personal information is permitted under Ontario's privacy laws with an individual's consent, to reduce serious harm, and as otherwise permitted or required under other provisions of Ontario's privacy laws.

Consent-based practices

Ontario's privacy laws permit consent-based information sharing. Consent refers to the permission obtained from an individual to collect, use, or share their personal information. For consent to be valid, it must be knowledgeable or informed and it must not be obtained through deception or coercion.[6] Consent can be obtained verbally or in writing.

In IPV related situations, the personal information at issue is often about both the victim or survivor and the abusive partner. When there are children involved, their personal information may also be at issue.[7]

> Obtaining a victim or survivor's consent before sharing their personal information is a recommended best practice.

When it comes to the victim or survivor, seeking their consent prior to sharing their personal information is generally a recommended best practice. Under certain circumstances, seeking their consent may not be a reasonable, practical, or safe option.

6 Sharing information with consent is permitted under 42(1)(b) of FIPPA, section 32(b) of MFIPPA, sections 286(a) and 295 of the CYFSA, and sections 6, 18, 29, and 30 of PHIPA.

7 When it comes to seeking a child's consent to share their personal information, you must consider any applicable consent and capacity related rules in, for example, sections 295 to 305 of the CYFSA or sections 21 to 27 of PHIPA. In addition, you should consider whether seeking a child's consent may tip off the abusive partner or otherwise put an at-risk individual at greater risk of harm.

This includes circumstances where consent cannot be sought at all or obtained in a timely manner, for example, because:

- the victim or survivor is unconscious or in a coma
- there have been repeated attempts to contact the victim or survivor with no response
- the victim or survivor cannot be contacted without risking tipping off the abusive partner, and the victim or survivor does not have a timely scheduled appointment with the organization or service provider
- the victim or survivor refuses to provide consent, despite efforts to seek their consent

Obtaining the consent of the abusive partner to share their personal information is often not a viable option, particularly in situations when they are perpetrating or intending to perpetrate harm to a victim or survivor or another person. Seeking the abusive partner's consent to share their personal information with police, for example, might only serve to tip them off and instigate, aggravate, or escalate the risk of serious harm.

Sharing to reduce serious harm (without consent)

> The fact that you can share a victim or survivor's personal information without their consent does not prevent you from consulting them.

Ontario'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, the fact that you are permitted to share an individual's personal information without their consent, particularly the victim or survivor, does not prevent you from consulting them about the impact of sharing their personal information for their health or safety. For example, you may need to consider consulting the victim or survivor where:

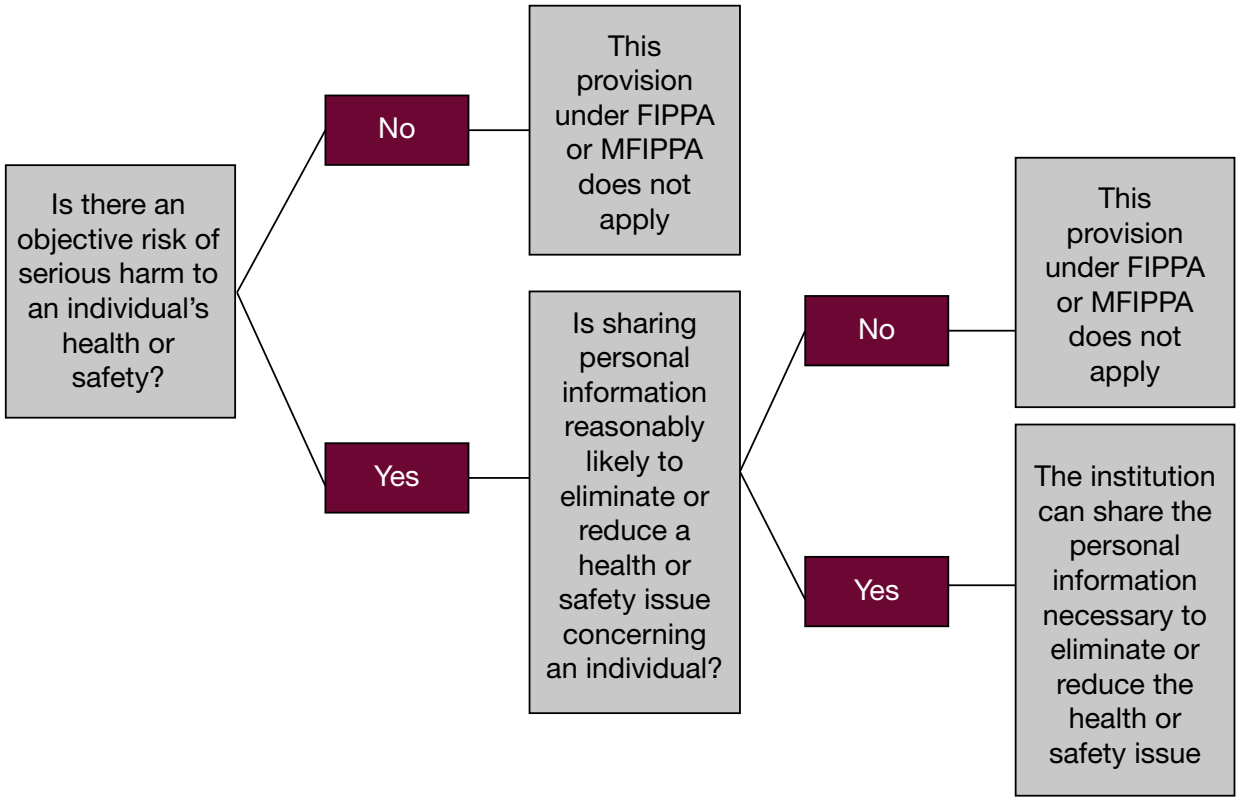
- sharing could place the at-risk individual at greater risk of harm
- sharing will lead to a mandatory charge and can reasonably be expected to escalate the risk of harm to the victim or survivor prior to the development of a safety plan
- sharing with another organization or service provider may lead to personal information also being shared with the police or a Children's Aid Society

Sharing personal information without consent can be a difficult decision to make. For example, a threat to the health or safety of a victim or survivor may involve a risk of serious harm, but it is not clear if (or when) the risk will materialize or worsen. In these circumstances, sharing personal information without consent is not wrong simply because the threat did not materialize or worsen. If a decision to share — or not to share — personal information is made after carefully assessing all the available information and the relevant factors, it will generally be considered reasonable and made in good faith under Ontario's privacy laws.[8]

8 See section 62(2) of FIPPA and section 49(2) of MFIPPA; section 71(1) of PHIPA; and section 37 of the CYFSA.

This part of the guidance focuses on sharing personal information without consent when there is a risk of serious harm. Each section has a decision tree that summarizes the key decision-making approach for the applicable sector and text that provides additional important information. **Each decision tree should be read together with the text that follows it.**

Justice sector: compelling circumstances under FIPPA and MFIPPA



Section 42(1)(h) FIPPA and 32(h) MFIPPA

An institution shall not disclose personal information in its custody or under its control except in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates.

FIPPA and MFIPPA permit institutions to share personal information without consent in compelling circumstances affecting the health or safety of an individual.[9]

9 See s. 42(1)(h) of FIPPA or section 32(h) of MFIPPA.

To be considered a compelling circumstance, it must be reasonable to believe that sharing personal information with the individual at risk or another organization or service provider could reasonably be expected to eliminate or reduce a health or safety issue.[10] While some compelling circumstances may involve a risk of imminent harm, FIPPA and MFIPPA do not require that the risk be imminent before sharing personal information.

Before sharing personal information, you must be satisfied there are compelling circumstances about an individual's health or safety. You must consider:

- the likelihood of the harm occurring
- the severity of the harm
- how soon the harm might occur
- whether sharing personal information is reasonably likely to reduce or eliminate the risk of harm to the individual

Having carefully assessed all the available information and the relevant factors, you may share personal information if there is an objective risk of serious harm to an individual and the sharing is reasonably likely to eliminate or reduce the risk. The focus should be on only sharing personal information that is reasonably necessary to eliminate or reduce the risk.

It may be reasonable to delay giving notice to an individual if the notification would result in a significant risk to someone's health or safety.

An institution must provide written notice to the individual whose personal information was shared as soon as reasonably possible. If notification would cause a significant risk to someone's health or safety, it would be reasonable to delay giving notice until the risk has abated. For example, notice to an abusive partner can be delayed until after a safety plan is in place to protect a victim or survivor at significant risk.

Each institution should decide the personal information necessary to share with the individual at risk or another organization or service provider. They should also take reasonable steps to ensure that the personal information is accurate, complete, and up to date before sharing it. The institution should also document that the personal information was shared.

10 The IPC has considered the meaning of a "compelling circumstance" under Order **MO-3247**, para. 62.

If the provision relating to compelling circumstances does not apply, consider whether another provision under FIPPA or MFIPPA permits sharing personal information. Other relevant provisions are explained under the section, **Other potential pathways to share personal information**.

The head of an institution and any staff acting on the head's behalf are protected from liability for damages arising from:[11]

- their decision to share or not share personal information when acting in good faith under FIPPA or MFIPPA
- their failure to give a notice required under these acts if reasonable care is taken to give the required notice

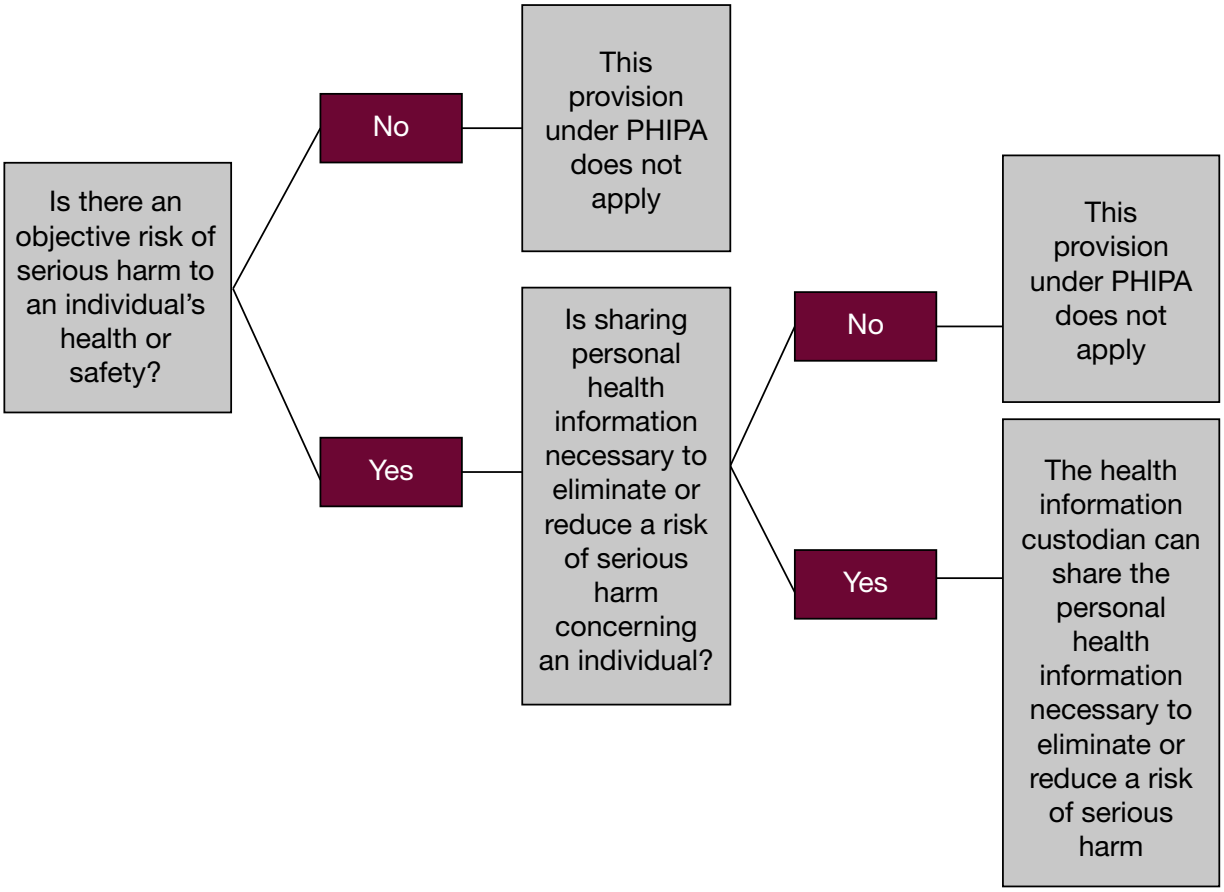
Justice sector example

After several minor offences, including threatening his ex-girlfriend Anjali, Johnny is conditionally discharged by the court and must attend a Partner Assault Response (PAR) program. As part of his conditional discharge, Johnny must meet weekly with his probation and parole officer (PO) and PAR program coordinator. During a weekly check-in, Johnny tells his PAR program provider that he is feeling depressed and wants to "get even with his ex." The PAR program provider questions what Johnny means. Johnny explains that Anjali does not deserve to continue her life without him. After the meeting, the PAR program provider contacts Johnny's PO and notifies him of a potential risk of serious harm to Anjali.

The PO reviews Johnny's file and considers his prior history of violence towards Anjali, his disclosed depression, worrisome behaviour, and veiled threats to Anjali. After using a validated risk assessment tool, the PAR program provider and PO agree that there is an increased risk of serious harm, leading them to believe that without intervention, Johnny may cause harm to Anjali. Based on his records, the PO is aware that Anjali receives support from a women's shelter. The PO decides to share Johnny's personal information with Anjali and her shelter support. The PO notifies them that he will also be calling the police. The PO delays notifying Johnny that his personal information was shared until the PO confirms Anjali is in a safe place and the significant risk to her is sufficiently reduced.

11 See section 62(2) of FIPPA and section 49(2) of MFIPPA.

Health care sector: risk of serious harm under PHIPA



Section 40(1) PHIPA

A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

PHIPA permits a health information custodian to share personal health information about an individual without their consent if they believe on reasonable grounds that sharing is necessary to eliminate or reduce the risk of serious harm to a person or group of persons.[12] The need to eliminate or reduce serious harm by sharing an individual's personal health information outweighs an individual's prior explicit instructions not to share it.[13]

12 See section 40(1) of PHIPA.

13 See the IPC's Lock-box Fact Sheet, page 3.

PHIPA requires a health information custodian to have reasonable grounds to believe that sharing an individual's personal health information is *necessary* for eliminating or reducing a risk of serious harm. Each health information custodian must decide the extent of personal health information necessary to share with the individual at risk or another organization or service provider.[14]

> Health information custodians can share personal health information that is necessary to eliminate or reduce risk of serious harm.

Having carefully assessed all the available information and the relevant factors, you can share personal health information if there is an objective and significant risk of serious harm to an individual and the sharing is necessary to eliminate or reduce the risk. The focus should be on sharing only the personal health information necessary to eliminate or reduce risk.

Health information custodians must also take reasonable steps to ensure that the personal health information is as accurate, complete, and up to date before sharing it. Otherwise, they must inform the information recipient of any relevant limitations potentially affecting its accuracy, completeness, or currency.[15] The health information custodian should also document that the personal health information was shared.

If the provision around risk of serious harm does not apply, consider whether another provision under PHIPA permits sharing personal health information. Other relevant provisions are explained under the section, **Other potential pathways to share personal information**.

14 See section 30 of PHIPA.

15 See section 11(2) of PHIPA.

A health information custodian, including staff acting on their behalf, is protected from liability if they act in good faith and do what is reasonable under the circumstances when performing their duties under the law. This legal immunity applies to the health information custodian in respect of:[16]

- anything done, reported, or said, both in good faith and in the circumstances, in the exercise or intended exercise of any of their powers or duties under PHIPA
- any alleged neglect or default that was reasonable in the circumstances in the good faith exercise of any of their powers or duties under PHIPA

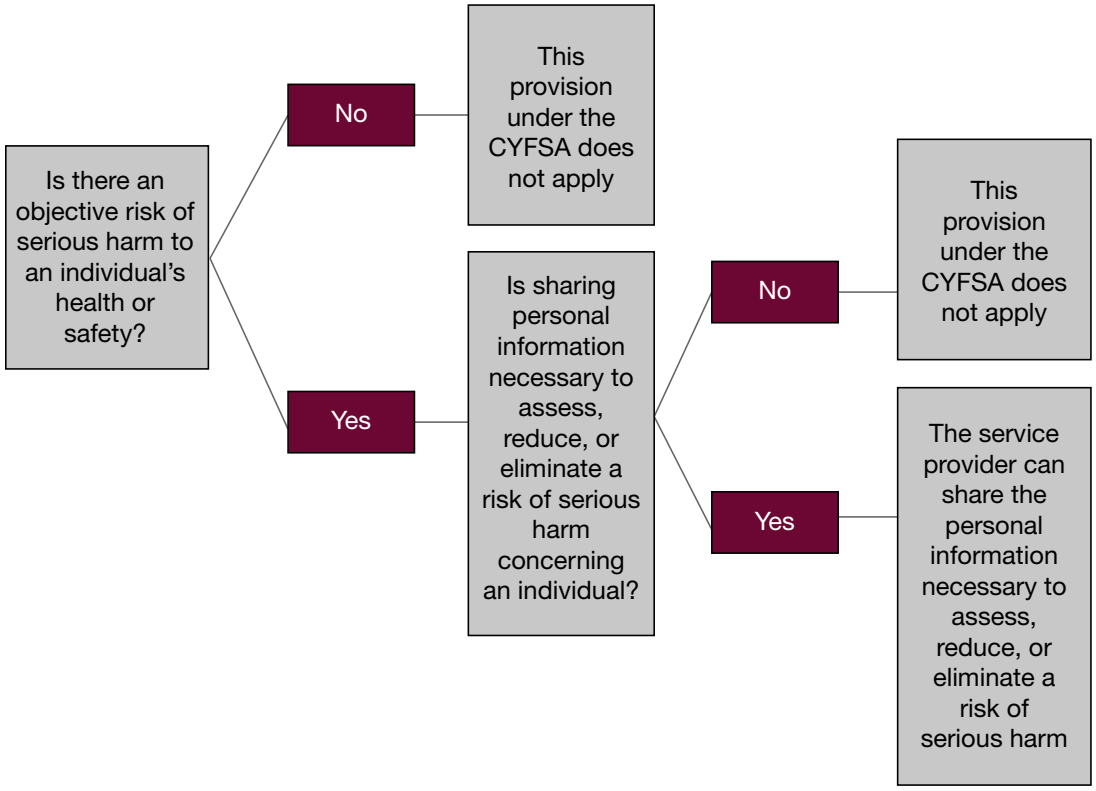
Health care sector example

Benjamin, a psychologist, has been treating his client, David, for several months. Benjamin has observed that David's mental health has been getting worse, his drug use is increasing, and he has become more abusive to his wife, Michelle. During one appointment, David tells Benjamin that he plans to kill Michelle when she gets home from work but asks Benjamin not to tell anyone. Benjamin has reasons to believe that this threat is real and is concerned for Michelle's safety. For example, he knows that David has assaulted Michelle before and that he has a long history of physical violence associated with drug use.

Looking at all the facts available, Benjamin determines sharing David's personal health information is necessary to reduce a risk of serious harm to Michelle. Further, the need to protect Michelle's health and safety outweighs David's request to keep his plan confidential. Benjamin calls the police after the appointment with David and tells them that David has stated that he plans to kill Michelle. Benjamin also contacts Michelle to tell her about David's plan to kill her, that the police have been notified, and to advise her to seek safety instead of returning home after work. With her agreement, Benjamin refers Michelle to a local women's community centre to help her get the assistance and supports she needs.

16 See section 71(1) of PHIPA.

Child, youth, and family services sector: risk of serious harm under the CYFSA



Section 292(1)(g) CYFSA

A service provider may, without the consent of the individual, disclose personal information about an individual that has been collected for the purpose of providing a service, if the service provider believes on reasonable grounds that the disclosure is necessary to assess, reduce or eliminate a risk of serious harm to a person or group of persons.

The CYFSA permits service providers to share personal information without consent if they have reasonable grounds to believe that sharing is necessary to assess, reduce, or eliminate a risk of serious harm to a person or group of persons.[17]

The CYFSA requires a service provider to have reasonable grounds to believe that sharing an individual's personal information is *necessary* to assess, reduce, or eliminate a risk of serious harm. Each service provider under the CYFSA must decide the extent of personal information necessary to share with the individual at risk or another organization or service provider.[18]

17 See section 292(1)(g) of the CYFSA.

18 See section 287 of the CYFSA.

Having carefully assessed all the available information and the relevant factors, you can share personal information if there is an objective risk of serious harm to an individual and sharing is necessary to assess, reduce, or eliminate the risk. The focus should be on only sharing personal information that is necessary to assess, eliminate, or reduce the risk.

Service providers must also take reasonable steps to ensure that the personal information is as accurate, complete, and up to date before sharing it.[19] Otherwise, they must inform the recipient of the personal information of any relevant limitations potentially affecting its accuracy, completeness, or currency. They must also document that they shared the personal information.[20]

If the provision relating to risk of serious harm does not apply, consider whether another provision under the CYFSA permits sharing personal information. Other relevant provisions are explained under the section, **Other potential pathways to share personal information**.

Members of the board of directors or an officer or an employee of a society under the CYFSA are protected from liability for:[21]

- any act done in good faith in the execution or intended execution of the person's duty
- for an alleged neglect or default in the good faith execution of that person's duty

Service provider under the CYFSA example

The local Children's Aid Society has been involved with Jennifer, a youth, and her family due to ongoing concerns about her exposure to IPV between her mother and stepfather. One morning, Jennifer calls Marshall, her assigned worker, and tells him that her stepfather seriously injured her mother during an argument the previous evening. Jennifer explains that her mother is unable to get out of bed due to her injuries. Jennifer tells Marshall that she is scared because her stepfather is still in the family home.

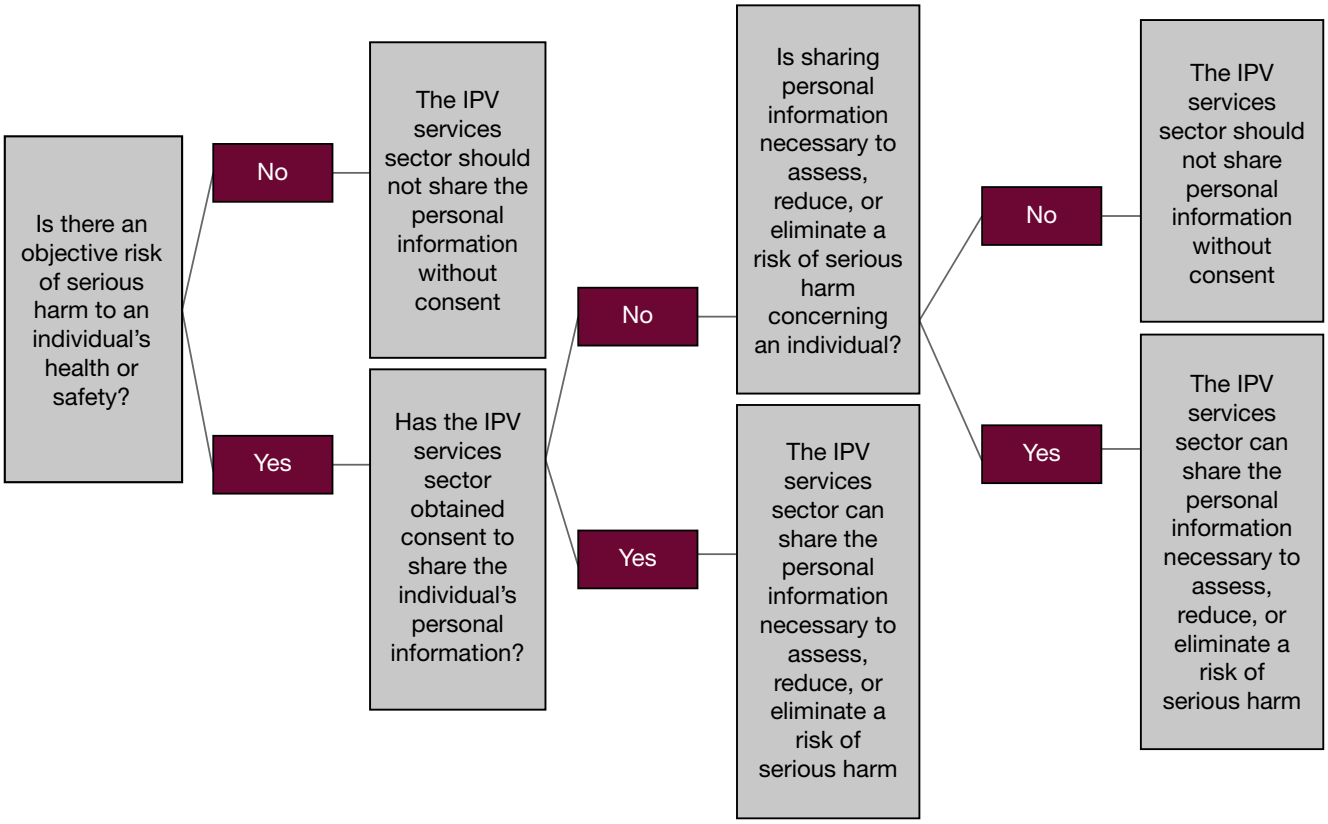
Marshall consults with his supervisor. After considering the situation, including the level of risk and degree of urgency, and weighing various options for responding, Marshall believes that Jennifer and her mother may be at risk of serious harm. He decides it is necessary to share relevant information with the police so that they can further assess the situation and put into place a safety plan, such as arranging a home visit, removing the stepfather from the family home, or contacting a women's shelter for support.

19 See section 306(2) of the CYFSA.

20 See section 306(3) of the CYFSA.

21 See section 37 of the CYFSA.

IPV services sector: a risk of serious harm approach



Although Ontario's privacy statutes do not apply to the IPV services sector, the IPC recommends that, consistent with current practice in the sector, a consent-based approach to sharing personal information is used. This approach is designed to maintain the privacy, confidentiality, and trust of victims or survivors.

Under this "consent first" approach, you would first determine whether there is an objective risk of serious harm to an individual's health or safety. If you reasonably believe there is, you should seek the individual's consent to share their personal information.

However, as explained in the section on **consent-based practices**, there may be circumstances when the consent of the victim or survivor cannot be sought or obtained. In such circumstances, the IPC recommends that the IPV services sector consider adapting the **CYFSA's "risk of serious harm"** provision to share personal information without consent. Your practices may also require additional considerations to inform decision-making before sharing personal information. As examples:

- consultations with supervisors and the victim or survivor
- using an evidence-based risk assessment tool
- developing or putting in place a safety plan

When it comes to applying the risk of serious harm approach, you should carefully assess all of the available information and the relevant factors. After completing this assessment, you can share personal information if there is an objective risk of serious harm to an individual and sharing is *necessary* to assess, reduce, or eliminate the risk. The focus should be on only sharing personal information that is necessary to assess, reduce, or eliminate the risk.

IPV services sector example

For the past year, Lira has been dropping in irregularly at her local IPV support centre. In recent months, she has been visiting the centre more often. Grace, a staff member who works closely with Lira, asks her if everything is okay at home. Lira tells Grace that her partner is always mad at her and, on the worst days, punching and kicking her to relieve his frustrations. Concerned for her safety, Grace offers to develop a safety plan with Lira to get her safely out of the situation. Lira says no. Lira loves her partner and believes he does not mean to hurt her. After the conversation, Grace consults with her supervisor. While they both feel they could call the police and make a report, they decide that sharing information about Lira's personal situation at this point may isolate her and make her stop visiting the centre, causing more harm than good. Grace will continue to provide Lira support, advocate for her safety, and assess changes in risk.

One night, Grace receives a call from Lira, who is crying and clearly panicking. Lira tells Grace that she has locked herself in the bedroom because her partner is threatening to stab her with a kitchen knife. Grace can hear someone in the background screaming and banging on the door. Before Grace can respond, the phone goes silent. As there is a significant risk of serious harm to Lira, Grace immediately calls 911.

Other potential pathways to share personal information

Other provisions under Ontario's privacy laws permit sharing personal information without consent, which may be relevant for an IPV or potential IPV situation. The IPV services sector should familiarize itself with these provisions and consider adapting them as best practices.

Sharing for the same purpose or a consistent purpose

Institutions can share personal information for the purpose for which it was obtained or compiled 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.[22]

If the personal information is collected directly from an individual, a consistent purpose for sharing personal information means that the individual might reasonably expect that their personal information may be shared.[23] If personal information is collected indirectly from another source, a consistent purpose means that the purpose for sharing personal information is reasonably compatible with the purpose for which it was originally obtained or compiled by the institution.[24]

Justice sector example

Arya and her husband, Ahmed, are recent immigrants to Ontario. Ahmed has found it difficult to find a job in Canada because his degree from his country is not widely accepted. This has put a lot of strain on their marriage, leading to Ahmed's escalated aggression towards Arya. One night, after blaming Arya for his job struggles, Ahmed punches Arya and threatens to kill her. Not knowing who to go to for support, Arya calls 911.

Arya tells the police she is worried for her safety and is in distress. The police visit Arya's home, charge Ahmad with assault, and arrest him. After confirming that Arya has no family or friends to support her and observing that she is in considerable distress, the police also reach out to a local women's support centre to help Arya get the mental health and safety planning support she needs. In this case, Arya would reasonably expect that the personal information she provided to police to seek protection from Ahmed would be used for the consistent purpose of obtaining critical mental health and safety planning support.

22 See section 42(1)(c) of FIPPA and section 32(c) of MFIPPA. The IPC has considered the meaning of a "consistent purpose" in Privacy Report **PC18-18** (a case involving a direct collection) and Privacy Complaint Report **MC-060007-1** (a case involving an indirect collection).

23 See section 43 of FIPPA and section 33 of MFIPPA.

24 See IPC Privacy Complaint Report **MC-060007-1**.

Sharing if permitted or required by law

Institutions, service providers under the CYFSA, and health information custodians can share personal information if it is permitted or required by another law or by a treaty, agreement or arrangement made under a federal or provincial act.[25]

Justice sector example

Sierra and Jacob have a volatile relationship and have been on and off for almost ten years. After Jacob nearly chokes her, Sierra calls the police and files an IPV report. The police charge Jacob with assault and arrest him. When Jacob is released from the station, the police immediately notify Sierra about his release conditions. After four months, Sierra calls the police to learn more about the court process and asks when the trial will take place, whether Jacob is still subject to the same release conditions, and whether his location or custodial status has changed. The police review the Disclosure of Personal Information regulation under the *Community Safety and Policing Act* and determine that providing the requested information to Sierra is permitted.

Health care and justice sectors example

Josh shoots his girlfriend, Stacey, seriously injuring her. Stacey is taken to Memorial Hospital, where staff treat her for the gunshot wound. PHIPA applies because Stacey is treated for a gunshot wound by a hospital (a public hospital and health information custodian). But another law, the *Mandatory Gunshot Wounds Reporting Act* (MGWRA), requires public hospitals that treat an individual for a gunshot wound to share the person's name, if known, and the name and location of the treating facility with the police.[26] The doctor treating Stacey shares the necessary personal health information with police to comply with the MGWRA.

Sharing to aid police

Institutions, service providers under the CYFSA, and health information custodians *may* share personal information with police to help with an IPV investigation or help the police decide whether to conduct an IPV-related investigation.[27] In some cases, they *must* share personal information with the police to comply with the law (for example, by a court order or warrant).

25 See section 42(1)(e) FIPPA; section 32(e) of MFIPPA; section 292(1)(h) of the CYFSA, and section 43(1)(h) of PHIPA.

26 See subsection 1(a) and 2(1) of the *Mandatory Gunshot Wounds Reporting Act*. The preamble of this act states that mandatory reporting of gunshot wounds will enable police to take immediate steps to prevent further violence, injury, or death.

27 See sections 42(1)(g)(i) and 42(1)(g)(ii) of FIPPA; sections 32(g)(i) and 32(g)(ii) of MFIPPA; section 292(1)(a) of the CYFSA, and sections 43(1)(f) and 43(1)(g) of PHIPA.

Voluntary sharing of personal information to assist with a police investigation should generally be limited to what is reasonably necessary.[28] In such cases, you should make a careful and informed assessment of the circumstances before sharing personal information with the police. This includes assessing the situation and deciding whether sharing personal information would put a victim or survivor at a greater risk of harm. For example, if sharing will lead to a mandatory charge and can reasonably be expected to escalate the risk of serious harm to the victim or survivor prior to the development of a safety plan.

Justice sector example

Mariam is a staff member of the Victim/Witness Assistance Program. She is working with Keisha who obtained a restraining order against Jerome, her on-and-off-again abusive partner. Jerome is not allowed to have any contact with Keisha for a year. Over the weekend, Keisha receives several text messages from Jerome, including pictures of a gun and threats to end her life.

Keisha is worried for her safety and shares these text messages with Mariam. Since Jerome is breaching the restraining order, Mariam encourages Keisha to call the police. Keisha is scared that Jerome may find out she contacted the police, as he has a tracking app on her phone. Mariam offers to make the report to the police and help her with a safety plan. Keisha abruptly hangs up, mid-sentence. Mariam tries calling Keisha several times, but her calls go straight to voicemail. She is concerned and alerts the police about the situation.

IPC resource:

- **Disclosure of Personal Information to Law Enforcement**

Sharing to protect children from IPV harm

Staff across each sector may face a conflict between child protection law and their ethical obligation to maintain the privacy, confidentiality, and trust of the individuals they serve. Although these situations can be complex, the lawful basis for sharing personal information without consent for child protection is clear.

Under the CYFSA, you have a duty to report information to a Children's Aid Society if you have reasonable grounds to suspect a child under 16 may be in need of protection.[29] The duty to report applies to any person regardless of whether you are working in a professional capacity. If you perform professional duties with respect to children and get this information while performing your professional duties, a failure to report this information is an offence.[30]

28 See section 287 of the CYFSA and section 30 of PHIPA for data minimization requirements.

29 Section 125 of the CYFSA.

30 See sections 125(5) and 125(6) of the CYFSA.

In the interests of protecting children, the duty to report does not require you to have reasonable grounds to *believe* that abuse or neglect has occurred or will occur. The duty to report also does not require you to conduct your own investigation. Rather, you need only have reasonable suspicion or reasonable cause to report a concern to a Children's Aid Society.[31] Although the duty to report only applies to children under 16, you may voluntarily make a report concerning a child who is 16 or 17 years old if you have reasonable grounds to suspect that that child may be in need of protection.[32]

Anyone who acts on a duty to report is protected from liability under the CYFSA if they have reasonable grounds to suspect harm and the report is not made maliciously.[33] If you have reasonable grounds to suspect that a child may be in need of protection, contact your local Children's Aid Society or Indigenous Child and Family Well-Being Agency.

Example for IPV services sector

Kaia and Greg have three children between the ages of two and five. Greg has been emotionally and physically violent toward Kaia on several occasions. The violence against Kaia has been escalating since the birth of their youngest child. One evening, Greg returns home in a bad mood and takes his anger out on Kaia in front of the children. The following morning, Kaia goes to a women's shelter. She confides in Sarah, a shelter staff, about what is happening at home.

Sarah learns that Kaia has three children and is planning to return home after her appointment. Sarah explains she has a duty to report this to a Children's Aid Society (CAS) because Greg is a risk to her and her children. Sarah offers to either support Kaia in contacting her local CAS by calling together or to file a report on her behalf. In the end, Sarah files a report on Kaia's behalf to her local CAS so that Kaia and her children can receive support and safety planning, which may include Greg needing to leave the family home.

IPC resources:

- **Yes, You Can: Dispelling the Myths about Sharing Information with Children's Aid Societies**
- **Part X of the *Child, Youth and Family Services Act:* A Guidance to Access and Privacy for Service Providers**

Other resource:

- **Report child abuse and neglect**

31 See *Young v Bella*, 2006 SCC 3 at para. 50; *K.O. v Hospital for Sick Kids*, 2017 HRTO 145 at paras. 31-33.

32 See section 125(4) of the CYFSA.

33 See section 125(10) of the CYFSA.

Good governance around sharing personal information

Each organization and service provider should establish governance frameworks to protect the privacy and confidentiality of the individuals they serve. Your governance framework should include policies and practices focused on sharing personal information. Staff should be regularly trained on how to interpret and apply these policies and practices.

At a minimum, your policies and practices should include the following principles:

Health and safety first

Ontario's privacy laws do not prevent the sharing of personal information to assess or reduce risk of serious harm to individual health or safety. Personal information can be shared with the individual at risk or another organization or service provider when it is reasonably necessary to assess or reduce a risk of serious harm.

Protecting personal information

Ensure there are appropriate privacy and security controls in place to protect the personal information held by your organization or service provider.[34] For example, develop internal processes to detect unauthorized collection, use, and sharing of personal information and ensure that response/mitigation plans are in place to address privacy breaches.[35]

Transparency and accountability

Establish transparent and accountable frameworks to communicate with the individual, and to the broader public, about how IPV prevention programs may collect, use, and share personal information.[36] This also includes communicating under what circumstances personal information may be shared and with whom.

Necessity and proportionality

Limit the amount of personal information shared to what is necessary to prevent the risk of serious harm. If non-personal information could serve the same purpose, share that information instead. Likewise, if less personal information will do, limit the sharing of personal information to that. In difficult cases, consult with your supervisor, legal counsel, or others to assess the information necessary to meet this objective.

---

34 See section 4 of O. Reg 459 (FIPPA) and section 3 of R.R.O, Reg 823 (MFIPPA); see sections 308 and 309 of the CYFSA; and sections 12, and 13 of PHIPA.

35 Service providers under the CYFSA must notify the affected individuals, the IPC, and the Ministry of Children, Community, and Social Services of any privacy breach that meets the criteria under the law. See sections 308(2) and (3) of the CYFSA and sections 8 and 9 of O. Reg. 191/18. Additional guidance can be found here: **www.ipc.on.ca/part-x-cyfsa/safeguarding-and-managing-personal-information/responding-to-privacy-breaches/**. Similarly, health information custodians must notify the affected individuals and the IPC of any privacy breach that meets the criteria under PHIPA. See subsection 12(2), (3) and (4) of PHIPA and section 6.3 of O. Reg. 329/04. Additional guidance can be found here: **www.ipc.on.ca/health-organizations/responding-to-a-privacy-breach/privacy-breach-protocol/**.

36 For institutions, service providers under the CYFSA and health information custodians, a notice of collection to the individual about how their personal information is collected, used, or shared is required.

Documentation

Document instances when personal information is shared. Use a specific template or format to demonstrate that you made decisions on reasonable grounds and in good faith.[37] Refer to Ontario privacy laws, as applicable, and retain records based on your information management and recordkeeping policies.

Trauma and violence-informed approach

Adopt a trauma and violence-informed approach to increase the safety, control, and resilience of victims or survivors around decisions that affect their health or safety.[38] This includes taking a culturally sensitive approach that considers the victims' or survivors' intersectional identity and agency.

Indigenous governance and sovereignty rights

Indigenous governance and sovereignty rights assert the ability of First Nations, Inuit, and Métis individuals, governments, organizations, and communities to determine, participate, and steward data and personal information collected with and about them. Organizations, service providers, and their staff should familiarize themselves with Indigenous governance and sovereignty rights to ensure they are upheld and respected when engaging with Indigenous individuals. For example, the First Nations Principles of Ownership, Control, Access, and Possession — the OCAP principles — establish how First Nations' data and personal information should be collected, protected, used, or shared.[39]

Multi-sectoral collaboration for risk management and response

A recognized approach to risk management and response includes developing multi-sectoral risk intervention models. Such models can enable organizations and service providers to collaboratively identify and respond to threats and behaviours that pose a risk of serious harm to an individual.[40]

37 Under section 306(3) of the CYFSA, service providers must document instances where personal information is shared.

38 To learn more about a trauma and violence-informed approach, visit the **Public Health Agency of Canada**.

39 Visit the First Nations Information Governance Centre to learn more about the **First Nations OCAP principles**.

40 To learn more, review the Government of Ontario's **Guidance on information sharing in multi-sectoral risk intervention models**.

Conclusion

This guidance clarifies and demonstrates that Ontario's privacy laws are not a barrier to the lawful sharing of vital — and, in some cases, lifesaving — personal information. Institutions, children and family service providers, health information custodians, and IPV service providers should feel empowered to make informed decisions about privacy, confidentiality, and public safety to protect a victim or survivor and their children from IPV harm.

A best practice for sharing personal information is to get individual consent. However, this may not always be possible. Under Ontario's privacy laws, organizations, service providers, and their staff are permitted to share personal information about an individual when there is reason to believe there is a risk of serious harm to an individual's health or safety. Remember, if a decision about whether to share personal information under Ontario's privacy laws is made after carefully assessing all available information and the then relevant factors, it will generally be considered reasonable and made in good faith.

If you have questions about this guidance, contact us at **info@ipc.on.ca**.

Terms and concepts used in this guidance

Abusive partner: refers to an individual who has committed or is alleged to have committed an offence or who has or is alleged to have inflicted physical, psychological, or emotional harm, property damage, or economic loss as the result of the commission or alleged commission of the offence, whether or not an IPV or domestic violence-related charge has been laid.

Child: refers to a person under 18 years old.[41]

Child, youth, and family services sector: refers to service providers under the CYFSA and their staff.[42]

Disclosure: in this guidance, disclosure refers to making personal information or personal health information available or releasing it to another organization, service provider, or their staff.

Health care sector: refers to organizations and service providers that deliver health care services to Ontario residents. Health care refers to any observation, examination, assessment, care, service, or procedure that is done for a health-related purpose.[43]

Health information custodian: in relation to PHIPA, refers to certain organizations and service providers who have custody or control of personal health information in connection with their work (for example, physicians and hospitals).[44]

Intimate partner violence (IPV): refers to a form of women and gender-based violence, which includes multiple forms of harm caused by a current or former intimate partner.[45]

41 See section 2(1) and section 281 of the CYFSA.
42 See section 2(1) and section 281 of the CYFSA.
43 See section 2 of PHIPA.
44 See section 3 of PHIPA and section 3 of O. Reg. 329/04.
45 See Women and Gender Equality Canada's **Fact Sheet: Intimate partner violence**

IPV services sector: refers to community-based organizations and service providers that provide IPV-related services and are generally not subject to FIPPA, MFIPPA, the CYFSA, or PHIPA.

Institution: in relation to FIPPA and MFIPPA, refers to a head of an institution and body designated as an institution under the act. For example, a ministry, agency, board and commission, a municipality, or a police service.[46]

Justice sector: refers to institutions and other organizations and service providers across the criminal justice system that provide services to a victim or survivor of IPV and/or abusive partner.

Personal health information: refers to identifying information about an individual, whether oral or recorded, if the information, for example, relates to their physical or mental condition, the health care services they have received, their health number, or to other identifying information mixed with the personal health information.[47]

Personal information: in relation to FIPPA and MFIPPA, refers to information about an identifiable individual whether oral or recorded (for example, an individual's name, address, sex, age, and education).[48]

Risk assessment: in this guidance, risk assessment is a decision-making process used to determine the best course of action by estimating, identifying, qualifying, or quantifying risk of IPV perpetration for the purpose of prevention, risk management, and safety planning. Typically, risk assessment involves the use of evidence-based risk assessment tools.

Risk of serious harm: refers to a risk of serious physical harm and/or serious psychological harm to an individual, including in relation to this guidance's discussion of "serious harm" under the CYFSA[49] and "serious bodily harm" under PHIPA.[50]

Service provider under the CYFSA: in relation to the CYFSA, refers to a person or entity that provides a service funded under the CYFSA (for example, Children's Aid Societies, including Indigenous Child and Family Well-Being Agencies); a licensee; a lead agency; the Minister of Children, Community and Social Services; and any additional person or entity prescribed through a regulation.[51]

Victim or survivor: refers to an individual against whom an offence has been committed, or is alleged to have been committed, who has suffered, or is alleged to have suffered physical, psychological, or emotional harm, property damage, or economic loss as the result of the commission or alleged commission of the offence whether or not an IPV or domestic violence-related charge has been laid.

46 See section 2(1) of FIPPA and MFIPPA.

47 See section 4 of PHIPA.

48 Personal information also includes information that is not recorded and that is otherwise defined as personal information. See sections 2(1) and 38(1) of FIPPA and sections 2(1) and 28(1) of MFIPPA.

49 See section 292(1)(g) of CYFSA.

50 See section 40(1) of PHIPA.

51 See section 2(1) and section 281 of the CYFSA.

Sharing Information in Situations Involving Intimate Partner Violence: Guidance for Professionals

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

May 2024