Domestic Violence Information Sharing Protocol

NSW GOVERNMENT

NSW Department of Justice

Justice Precinct Offices
Level 5, 160 Marsden Street
Parramatta NSW 2150

Locked Bag 5111
Parramatta NSW 2124

DX 1227 Sydney
Tel: 02 8688 7777
Fax: 02 8688 7980
Email: cpd_unit@agd.nsw.gov.au

ISBN 978-1-922257-07-9

Contents

Acknowledgements

The *Domestic Violence Information Sharing Protocol* (Protocol) was developed by the NSW Department of Justice in partnership with government agencies, including the NSW Department of Family and Community Services (FACS), Legal Aid NSW, the NSW Police Force and NSW Health. It has also been informed by consultation with the NSW Information and Privacy Commission, and peak bodies and non-government agencies within the domestic violence sector.

The Protocol was developed to support the NSW Government's Domestic and Family Violence Framework for Reform and the Domestic Violence Justice Strategy, and the introduction of *It Stops Here: Safer Pathway* (Safer Pathway). This work reflects a shared commitment to improving the response to domestic and family violence through collaborative, integrated service provision and improved information sharing.

The Protocol is the result of consultations with individuals, victims of domestic violence, service providers and agencies across the state. It was informed by experts with experience working with victims and perpetrators of violence and, to improve the response to domestic and family violence, has considered information sharing responses that have worked in other Australian states and internationally.

The Department gratefully acknowledges and extends its thanks to persons and agencies for their contribution and advice in the development of the Protocol. Your perspectives were essential to ensure that the focus of the Protocol maintained a balance between safety for victims of domestic violence and their rights to privacy and confidentiality.

Executive Summary

The *Domestic Violence Information Sharing Protocol* (Protocol) explains how to share information under Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* (Part 13A). At the heart of the Protocol is the safety and protection of victims and their children from domestic violence. Part 13A regulates information sharing in cases of domestic violence and has effect despite any provisions under NSW privacy legislation.

Public sector agencies, private organisations and individual service providers must comply with the Protocol when sharing the personal and/or health information of domestic violence victims, perpetrators and other persons under Part 13A. Part 13A and the Protocol reflect the importance of balancing the safety needs of domestic violence victims with individuals' rights to privacy.

The Protocol acknowledges that a significant number of victims have children in their care that are also victims or affected by domestic violence in the home. For this reason the safety, welfare and wellbeing of children is implied in all aspects of the information sharing provisions set out in the Protocol. Where children are victims or affected by domestic violence in the home, service providers who are prescribed bodies under the *Children and Young Persons (Care and Protection) Act 1998* (*CYPCP Act)* must share information under Chapter 16A of that Act.

The Protocol is divided into the following chapters.

Chapter 1. Introduction

Provides information on the legal status of the Protocol and guidance to service providers on how to use the Protocol where they wish to share information under Part 13A.

Chapter 2. Definitions

Provides explanatory notes of the key terms used in the Protocol.

Chapter 3. Protocol and service providers

Outlines how Part 13A and the Protocol apply to service providers within NSW. It also explains how service providers in NSW should share information with service providers in other jurisdictions.

Chapter 4. Privacy laws and other legislation

Provides information on the interaction of Part 13A and the Protocol with NSW and Commonwealth privacy laws. It also explains how Part 13A and the Protocol interact with other legislation and policy with which service providers may be required to comply.

Chapter 5. Protocol and child protection legislation

Outlines how Part 13A intersects with child protection legislation and how information sharing should occur where children are victims, are affected by domestic violence in the home, or where either the victim or the perpetrator is under the age of 18.

Chapter 6. Principle and objectives

Sets out the overarching principles that have guided the development of the Protocol and explains how service providers must be mindful of these at all times when sharing information under Part 13A and the Protocol.

Chapter 7. Information sharing under Part 13A

Outlines the legal threshold that allows personal and health information about victims, perpetrators and other persons to be shared between service providers where victims are at threat or at serious threat of domestic violence.

Chapter 8. Threat Identification

Outlines the process for consistent and early threat identification of victims of domestic violence to accurately identify victims' immediate and ongoing needs. It also includes provisions to help service providers know when and how to review threat assessments.

Chapter 9. Victim referral to support services

Explains the role of the Central Referral Point and the Local Coordination Points and provides information on referrals to address victims' safety needs. Some referrals are consent based while others are automatic and the victims' consent is sought at a later stage. This chapter explains this process. It also provides guidance on how to respond to information requests from other service providers and on contacting victims.

Chapter 10. Identification of victim and perpetrator

Outlines procedures to respond to situations where a service provider is unclear about the identification of the victim and the perpetrator, or where a victim is now identified as a perpetrator, or where both parties claim to be a victim.

Chapter 11. Conflict of interest

Outlines procedures to identify and manage conflicts of interest and, if required, how to return a referral for re-allocation.

Chapter 12. Consent

Outlines the importance of seeking consent as an essential element of sharing and managing victims' personal and health information. It also sets out consent requirements for victims at threat and processes associated with gaining informed consent from victims.

Chapter 13. Serious threat

Outlines supplementary procedures where there is a serious threat to the life, health or safety of a victim, any children or other persons, and the requirements for sharing information without consent.

Chapter 14. Information management

Sets out best practice standards for protecting individuals' right to privacy and confidentiality, and outlines clear procedures governing what, how and when information can be shared under the Protocol.

Chapter 15. Privileges and subpoenas

Provides assistance on how to respond to a subpoena and the existence of potential privileges at law in respect of health and personal information held in service provider files or databases.

Chapter 16. Access

Outlines procedures regarding requests to access victim, perpetrator or third party health and personal information held in service provider files or databases.

Chapter 17. Amendment

Outlines procedures regarding requests to amend victim and perpetrator health and personal information held in service provider files or databases.

Chapter 18. Compliance

Sets out service providers' obligations regarding compliance with the Protocol to ensure they understand the limits of information sharing and their responsibilities under Part 13A. It explains the compliance framework and processes to manage non-compliance, breaches of information and the remedial actions to address these.

Chapter 19. Complaints

Outlines processes to deal with complaints that may arise from information sharing under the Protocol and the different requirements depending on whether a service provider is a government agency or a non-government organisation, and whether they are bound by NSW or other privacy laws.

Chapter 20. Review of the Protocol

Provides information on the process to review the Protocol and how service providers may contribute to the review and formal evaluation by providing feedback to the NSW Department of Justice.

Chapter 21. Appendices

Includes the following decision flowcharts and templates to assist service providers implement the standards of the Protocol:

- Safer Pathway service delivery map, which brings together the key elements of Safer Pathway and illustrates how victims are supported in a seamless service system response
- Information sharing process flowchart, that outlines how and when service providers can share information
- Information sharing consent flowchart that outlines when service providers must seek victims' consent to share information
- Information sharing compliance checklist, which is a performance-monitoring tool to assist service providers assess their state of readiness to share information under Part 13A and to comply with the Protocol.
- Information sharing consent form, which is a template for service providers to use when seeking victims' consent to share information under the Protocol. Service providers may use this form, adapt it to their circumstances or use their own internal consent form
- Your information and your safety fact sheet for victims of domestic violence that explains the key elements of information sharing under the Protocol. Service providers are encouraged to give victims a copy of this fact sheet
- Memorandum of understanding template for service providers to adopt where they agree to share information under Part 13A and the Protocol

Suite of documents

The Protocol is part of a suite of five reference documents to support the implementation and operation of Safer Pathway. These five documents provide a framework for a common understanding of Safer Pathway and equip service providers with the information and the tools required to support the implementation of the new framework and to deliver a consistent and integrated response to domestic violence across NSW.

Service providers are encouraged to read the Protocol in conjunction with the other common documents, which include:

- Overview
  This overview document provides the context to the development of the NSW Government's Domestic Violence Framework for Reform, an overview of Safer Pathway and includes the common definition of domestic and family violence
- Safety Action Meeting Manual (SAM Manual)
  The SAM Manual is a guide for Safety Action Meeting members; it outlines the purpose and operations of Safety Action Meetings as a key element of Safer Pathway, the roles and responsibilities of members and the development of Safety Action Plans
- Domestic Violence Safety Assessment Tool Guide (DVSAT Guide)
  The DVSAT Guide includes the common assessment tool and assists service providers apply the tool and use their professional judgement to identify the level of threat to victims of domestic violence.
- Domestic Violence and Child Protection Guidelines (DV&CP Guidelines)
  These guidelines clarify the intersection between the domestic violence and the child protection systems in the context of information sharing.

1. Introduction

Domestic violence is a crime. It is also a multi-faceted issue that requires a coordinated response from service providers in the areas of policing, justice, health, welfare, education, child protection and victim support services. In this context, it is important that service providers work in partnership and share information to:

- prevent domestic violence related deaths, illness, injury and disability
- identify and manage domestic violence threats by using a common threat assessment tool where possible and sharing information about the safety of victims and any children, and the behaviour of perpetrators
- refer victims to service providers to secure their immediate safety, assist them in any legal processes, and enable their recovery from the trauma associated with the violence
- respond to identified needs of victims and their children that arise as a consequence of domestic violence or make them more vulnerable to its impacts
- increase the safety, welfare and wellbeing of children who are victims or exposed to domestic violence
- hold perpetrators accountable by reporting domestic violence incidents and alerting relevant agencies if there is evidence of an escalating threat of violence.

The *Crimes (Domestic and Personal Violence) Act 2007* was amended by inserting Part 13A to allow information sharing and improve integrated responses to domestic violence.

1.1 Legal status

The Protocol is made by an order of the Minister for Justice under s.98O, Part 13A of the *Crimes (Domestic and Family Violence) Act 2007* (Part 13A). Service providers must adopt the provisions and standards set out in the Protocol to share information under Part 13A and the Protocol. For this reason, the Protocol provides precise and detailed information on the provisions of Part 13A to ensure that service providers understand their obligations.

1.2 How to use the Protocol

Service Providers should refer to the Protocol as frequently as necessary and until such time as they have the knowledge and confidence to share victims' and perpetrators' information lawfully under the Protocol. It is important that information sharing practices build victims' confidence in Safer Pathway, promote their engagement, increase their safety, and that service providers comply with their legal obligations.

Initially, service providers must use the Protocol to ensure they meet the minimum requirements for a state of readiness to share information under the Protocol. Chapter 18 Compliance provides the necessary information and tools for service providers to adapt their information sharing practice and processes to be consistent with the Protocol.

Service providers must review their internal policies and practices against the Protocol with a view to integrating all aspects and requirements of Safer Pathway and the standards of the Protocol. This method allows service providers to adopt the provisions of the Protocol into their internal documents in their chosen formats. The Protocol must also be available as a stand-alone document to ensure that any updates or additional tools are easily accessed.

Additional resources are available in the online version of the Protocol. It contains hyperlinks to external websites, cross-references to places within the document and to any of the other four common documents where there is more information about a particular point.

In addition, the Protocol will be revised periodically to ensure relevance and accuracy, and the most recent and updated version will be available online.

1.3 Transition arrangements until full implementation of Safer Pathway

Part 13A and the Protocol commenced on the 15 September 2014 to support Safer Pathway in the launch sites at Waverley and Orange. It is planned that Safer Pathway will be rolled out across NSW in a staged approach over five years, with full implementation completed in 2019. This means that while Part 13A and the Protocol apply from 15 September, other elements of Safer Pathway, such as the Central Referral Point, Local Coordination Points and Safety Actions Meetings, referred to in the DFV Reforms and the Protocol are not available state-wide until such time as new sites have been announced and transitioned.

As Part 13A and the Protocol now apply in NSW, service providers should now adopt the provisions of the new legislation and share information about victims and perpetrators in accordance with this Protocol and where there is a legal basis to do so. Where service providers outside of the launch sites make referrals for victims and share information under the Protocol, they may use existing referral pathways and domestic violence support systems.

2. Definitions

Act	*Crimes (Domestic and Personal Violence) Act 2007*
Agency	• A public sector agency within the meaning of the *Privacy and Personal Information Protection Act 1998*. This includes NSW government departments, statutory authorities and local government authorities, such as public schools, public hospitals and correctional centres; and/or • An organisation within the meaning of the *Health Records and Information Privacy Act 2002*. This includes both public sector agencies and private organisations and individuals that hold health information, such as medical, hospital and nursing services, general practitioners, community health services, health education services and welfare services.
Apprehended Domestic Violence Order (ADVO) proceedings	Legal proceedings where an Apprehended Domestic Violence Order is sought (by the making of an application) or made.
Central referral point	Operated by Victims Services within the Department of Justice and is an electronic data collection and referral platform. It receives referrals and allocates them electronically to a Local Coordination Point based on the victim's gender and location.
Chapter 16A	The *Children and Young Persons (Care and Protection) Act 1998* allows information exchange between bodies prescribed under that Act by creating exceptions to the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Act 2002* and the *Commonwealth Privacy Act 1988*.
Children	Include all children and young people under the age of 18 years.
CYPCP Act	The *Children and Young Persons (Care and Protection) Act 1998*.
Contact purposes	Contacting a victim to seek their consent to (i) provide them with domestic violence support services directly and/or (ii) share their personal and health information with other service providers to permit the provision of domestic violence support services to the victim.
Domestic violence	Also means domestic and family violence and is defined in the Overview.
Domestic violence offence	A *personal violence offence* committed by a person against another person with whom the person who commits the offence has or has had a *domestic relationship*.
Domestic violence proceedings	Legal proceedings where an Apprehended Domestic Violence Order is sought (by the making of an application) or made, or a person is charged with a domestic violence offence.

Domestic violence safety assessment tool (DVSAT)	A common risk assessment tool to identify the level of threat to victims of domestic violence.
Domestic violence support services	Are services including, but not limited to, welfare, health, counselling, housing and accommodation, and legal assistance services that are provided to victims identified as being at threat of domestic violence or the subject of a domestic violence referral.
HRIP Act	The *Health Records and Information Privacy Act 2002*.
Health information	A specific type of personal information and includes information or opinion about the physical or mental health or disability of an individual, any health services provided, and any other health information collected to provide, or in providing, health services. For a more detailed description, refer to *s.6 of the HRIP Act*.
Local coordination point	A support agency or a non-government support service nominated by the Minister for Justice as a local coordination point, that may collect information about a victim, their children and a perpetrator and provide case coordination for victims of domestic violence and their immediate family members.
NSW privacy laws	The *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.
Non-government support service	Under Part 13A is a body (but not an individual) that provides domestic violence support services, but which is not an agency as defined under Part 13A and the Protocol. Generally, a body is likely to be a non-government support service if it is a non-government or private organisation which (a) provides a domestic violence support service but (b) does not hold health information. Non-government organisations that hold health information are organisations within the meaning of *Health Records and Information Privacy Act 2002* and therefore considered an agency for the purpose of Part 13A and the Protocol.
Part 13A	Refers to Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007*, which facilitates the collection, use and disclosure of personal and health information in cases involving domestic violence.

Perpetrator in the Protocol means, in the context of domestic violence, an alleged perpetrator or an offender and has the same meaning as an associated respondent under Part 13A. A perpetrator is a person who:

- has been charged with a domestic violence offence
- has had an ADVO sought or made against them
- is the person reasonably believed to be the cause of a domestic violence threat
- is the person identified as such in a NSW Police Force referral to the Central Referral Point.

The use of the term perpetrator to include alleged perpetrator has been adopted throughout the Protocol and other reference documents for ease of communication and in recognition that domestic violence is characterised by a pattern of repeated and habitual behaviours that tends to be much more prevalent than those matters which lead to an offence proved in the criminal justice system.

Personal information Any information or opinion about an identifiable person. This includes records containing name, address, gender, or physical information like fingerprints or body samples. For a more detailed description of personal information, refer to *s.4 of the Children and Young Persons (Care and Protection) Act 1998*. It should be noted that s.4 also explicitly excludes some types of information that might otherwise be regarded as "personal information" from the definition.

PPIP Act The *Privacy and Personal Information Protection Act 1998*.

Prescribed body Any organisation specified in *s.248(6) of the Children and Young Persons (Care and Protection) Act 1998* or in clause 7 of the *Children and Young Persons (Care and Protection) Regulation 2000*. Prescribed bodies include:

- the NSW Police Force
- a state government department or a public authority
- a government school or a registered non-government school or a TAFE
- a public health organisation or a private health facility
- any other organisation the duties of which include direct responsibility for, or direct supervision of, the provision of health care, welfare, education, children's services, residential services, or law enforcement.

Protocol Protocol means the *Domestic Violence Information Sharing Protocol*.

Safety Action Meeting (SAM) A meeting of service providers designed to facilitate information sharing for the purpose of preventing or lessening a serious threat to the life, health or safety of a victim, any children or other persons. For more information, refer to the Safety Action Meeting Manual.

Safety Action Plan A list of actions for services providers to complete to reduce or prevent a serious domestic violence threat to the life, health and safety of victims, any children or other persons. For more information, refer to the Safety Action Meeting Manual.

Service provider in the Protocol includes any entity to which the Protocol applies and means:

- a support agency, or
- a non-government support service.

In Chapter 13 Serious threat, and any other reference to serious threat in other sections of the Protocol, service provider also means:

- an agency.

Support agency An agency that provides domestic violence support services. It includes the Central Referral Point and Local Coordination Points.

Victim Has the same meaning as "primary person" under Part 13A, and is a person who is the:

- victim or the alleged victim of a domestic violence offence
- person in need of protection where an Apprehended Domestic Violence Order has been sought or made
- person a service provider believes on reasonable grounds to be subject to a domestic violence threat
- person identified as such in a NSW Police Force referral to the Central Referral Point.

3. Protocol and service providers

This chapter explains which service providers are required to comply with Part 13A and those which are covered by the Protocol. It also explains how service providers in NSW should share information with service providers in other jurisdictions.

3.1 Service providers to which Part 13A applies

Part 13A applies to the following service providers where they provide domestic violence support services:

- Any public sector agency within the meaning of the *Privacy and Personal Information Protection Act 1998 (PPIP Act)*. This includes NSW government agencies and statutory bodies, such as public schools, public hospitals and government departments.
- Any organisation within the meaning of the *Health Records and Information Privacy Act 2002 (HRIP Act)* to which that Act applies. This includes public sector agencies and private sector persons such as medical, hospital and nursing services, general practitioners, community health services, health education services and welfare services.
- Any organisation funded by a NSW government agency.
- Any non-government support service that has agreed to comply with the standards set out in the Protocol.

Provisions relating to serious threat apply to any agency or organisation within the meaning of the *PIPP Act* and the *HRIP Act*, including private sector agencies and private sector persons.

3.2 Service providers to which the Protocol applies

The Protocol applies to all service providers recognised by Part 13A.

The Protocol also applies the principles of Part 13A and NSW privacy laws to non-government support services that deal with personal and health information and:

- are under an obligation to comply with NSW privacy laws,
- act under a contract that imposes NSW privacy laws, or
- comply with privacy laws that impose substantially similar obligations to those imposed by NSW privacy laws, and
- comply with the standards set out in the Protocol.

This means that the Protocol treats these organisations in essentially the same way as support agencies, as defined in Part 13A and the Protocol. For this reason, the Protocol uses the term 'service provider' to cover the requirements attaching to both kinds of providers.

Service providers must satisfy themselves that other service providers they wish to share information with are compliant with NSW privacy laws or similar, or with the standards set out in the Protocol, before sharing information. A template for a memorandum of understanding (MOU) has been developed for service providers' use. Signatories to the MOU agree to share information according to the standards of Part 13A and the Protocol. Refer to Appendix 7 Memorandum of Understanding template.

If service providers are unsure about another service provider's compliance, they can share information under existing privacy laws about the victim only, with the victim's consent, or any person's information without consent where there is a serious and imminent threat to the life, health and safety of a person.

3.3 Commonwealth, state or territory service providers

Part 13A and the Protocol apply to the state of NSW. However, NSW has a number of towns on the border with other states and territories, and there are Commonwealth territories and Crown land within NSW. It may be necessary to share information across jurisdictions in cases where there is domestic violence threat, Apprehended Domestic Violence Order (ADVO) proceedings or a referral from NSW Police Force that occurs in NSW. For example:

- the perpetrator and/or victim live outside NSW
- a victim resides outside NSW and the perpetrator lives in NSW
- a perpetrator resides outside NSW and the victim resides in NSW
- a victim and the perpetrator both move outside NSW and the victim is not within range of services within NSW.

Refer to:
Section 19(2) PPIP Act or *s.14 HRIP Act schedule 1*.

In these situations, information about the victim and the perpetrator may be shared with a Commonwealth, state or territory service provider if the receiving service provider complies with privacy laws that impose substantially similar obligations to those imposed by NSW privacy laws.

Where the receiving service provider does not comply with similar privacy laws, information may only be shared about the victim and only with their consent.

For victims at serious threat, information may be shared with any Commonwealth, state or territory service provider whether or not that service provider complies with any privacy laws and whether the victim has given consent. This is a very limited exception from privacy law, and service providers must take reasonable steps to ensure the same level of protection of individuals' information is taken by the receiving service provider, as set out in the Protocol.

4. Privacy laws and other legislation

This chapter provides information on the interaction of Part 13A and the Protocol with NSW and Commonwealth privacy laws. It also explains how they interact with other legislation and policy with which service providers may be required to comply.

4.1 NSW privacy laws

The *PPIP Act* and the *HRIP Act* contain principles to protect the privacy of individuals' personal and health information in NSW.

All NSW government agencies are subject to the *PPIP Act* and the *HRIP Act*.

Private sector agencies are not subject to the *PPIP Act*, but most private sector agencies that deal with health information relating to individuals are subject to the *HRIP Act*. This means that, for example, individual general practitioners, physiotherapists, a partnership or any incorporated body and most not-for-profit organisations and non-government agencies must comply with the *HRIP Act*. Any private sector health agencies that are not subject to the *HRIP Act* will have obligations under the Commonwealth or other State privacy legislation.

Part 13A creates certain exceptions to these NSW privacy laws.

4.2 Commonwealth privacy laws

The *Privacy Act 1988* (Commonwealth) was amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* to include Australian privacy principles.

Australian government agencies and certain private sector organisations have responsibilities under Commonwealth privacy laws. These private sector organisations include:

- non-government organisations with an annual turnover greater than $3 million,
- private sector health service providers,
- private schools or private universities, if they have an annual turnover greater than $3 million, or provide a health service.

Part 13A does not create exceptions to Commonwealth privacy laws. Service providers must comply with their obligations under Commonwealth privacy laws when they share information under the Protocol.

4.3 Other legislation or policy

Service providers that share information under the Protocol are required to comply with any other legislation and their internal policies regarding privacy, confidentiality, non-disclosure and information management. Part 13A and the Protocol override privacy legislation and internal policy only to the extent specifically permitted by the legislation as set out in the following chapters.

All other legislation, including remaining privacy laws not overridden, and relevant internal policies, remain operational.

5. Protocol and child protection legislation

Refer to:
- Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*,
- *Children and Young Persons (Care and Protection) Regulations 2000* and the
- NSW Interagency Guidelines

For information on prescribed bodies, see s.248(6) of the *CYPP Act* or clause 7 of the Regulation.

A significant number of victims have children in their care and children can be direct or indirect victims of domestic violence. The Protocol does not replace information sharing practices or processes that may apply in these cases but, to ensure clarity, the following sections explain how information sharing should occur where children are victims or are affected by domestic violence in the home, or where either the victim or the perpetrator is under the age of 18.

Refer to the *Domestic Violence and Child Protection Guidelines* for further information.

5.1 Mandatory reporting obligations

Certain service providers are mandatory reporters under the *Children and Young Persons (Care and Protection) Act 1998 (CYPCP Act)* and their *mandatory reporting* obligations continue in respect of any information shared under Part 13A and the Protocol. Where these service providers have concerns for the safety, welfare or wellbeing of a child or a young person in the context of domestic violence, they must complete the *online mandatory reporter guide*. The outcome of the guide will direct the service provider to make a report to the *Child Protection Helpline* or to the Child Wellbeing Unit where available, or to take any other action as required under the *CYPCP Act*.

Case Study: Mandatory reporting and Chapter 16A

Laura and Greg have two children aged 1 and 3. Greg has assaulted Laura on many occasions and Laura has previously had an Apprehended Domestic Violence Order against Greg. Greg's physical violence towards Laura escalated following the birth of their youngest child and the frequency of his binge drinking is increasing. Laura is becoming more fearful for her safety.

One evening Greg becomes aggressive after drinking, grabs Laura by the arm and drags her towards the bedroom. Laura manages to calm the situation but the next day contacts a domestic violence crisis accommodation service and speaks with Tanya.

Tanya assesses Laura as at serious threat of domestic violence. With Laura's consent, Tanya makes an immediate referral to the Central Referral Point and assists Laura with emergency accommodation needs. Tanya then completes the online mandatory reporter guide and follows the instructions (including making a report to the Child Protection Helpline if required).

Tanya can share Laura's, Greg's and the children's information under Chapter 16A of the *CYPCP Act*.

The Local Coordination Point is a mandatory reporter. Even where the victim does not consent to further information sharing, if a Local Coordination Point worker believes that a child or young person is at risk of significant harm, and:

- it is not known whether a risk of significant harm report has been made, or
- a report has been made, but the Local Coordination Point receives additional information regarding the child or young person,

the worker must make take any action as required under the *CYPCP Act*.

A prescribed body is any organisation specified in section 248(6) of the *Children and Young Persons (Care and Protection) Act 1998* or in clause 7 of the *Children and Young Persons (Care and Protection) Regulation 2000*. Generally, prescribed bodies include:

- NSW Police Force
- a state government department or a public authority
- a government school or a registered non-government school or a TAFE
- a public health organisation or a private health facility
- a children's service any other organisation the duties of which include direct responsibility for, or direct supervision of, the provision of health care, welfare, education, children's services, residential services, or law enforcement, wholly or partly to children.

5.2 Chapter 16A information exchange

Chapter 16A of the *CYPCP Act* overrides other laws that prohibit or restrict the disclosure of personal information such as the *PIPP Act* and the *HRIP Act*. The focus of the exchange of information is on the safety, welfare and wellbeing of children, and facilitating the provision of services to these children and their families.

Service providers who are prescribed bodies under the *CYPCP Act* may exchange information that relates to a child or young person's safety, welfare or wellbeing, whether or not the child or young person is known to the FACS. A prescribed body may request information held by another prescribed body that relates to the safety, welfare or wellbeing of a child or young person, where that information assists the service provider to do any of the following in relation to the child or young person's wellbeing:

- make a decision or undertake an assessment or safety plan
- initiate or conduct an investigation
- provide a service
- manage any risk to the child or young person.

Refer to:
Responding to information requests or directions under Chapter 16A and Information Exchange: long fact sheet for workers

Unless an exemption applies, a prescribed body must comply with a request for information under Chapter 16A if they reasonably believe that the provision of the information may assist the service provider for any purpose listed above. It may include relevant information held on:

- a child or young person's circumstances or history,
- a parent or other family member,

- people having a significant or relevant relationship with a child or young person,
- the service provider's dealings with the child or young person, including past support or service arrangements.

Chapter 16A allows information to be shared even where children fall below the statutory reporting threshold. In other words, exchange of information can occur irrespective of whether a child protection report has been made to the Child Protection Helpline or not.

The threshold for sharing information under Chapter 16A is not as rigorous as that imposed by Part 13A; consent is not a requirement to exchange information, but it is best practice that service providers inform the adult victim that information about them and their children may be shared.

Case study: Sharing information under Chapter 16A

Jamia and Aazim have been together for ten years and have three children, aged 3, 8 and 9. Aazim has been abusive toward Jamia for their whole relationship, and frequently subjects her to emotional and physical violence. Jamia has never contacted the Police or a support service because she is afraid of what Aazim would do if he found out. Recently, Aazim lost his job.

One night he accuses Jamia of cheating on him and tries to strangle her, which he has never done before. Jamia is terrified because the violence is getting worse.

A few days later, Jamia tries to call a crisis accommodation service while Aazim is out of the house, but he comes home unexpectedly. Aazim becomes enraged and assaults Jamia in front of the children.

When Aazim next leaves the house, Jamia calls the accommodation service again and speaks with Rose. Rose is concerned for Jamia and the children's safety. Rose completes the online mandatory reporter guide and follows the instructions.

Rose asks Jamia if she can make a referral to a Local Coordination Point and that a support service will contact her to connect her with services to address her and her children's safety needs. Jamia agrees and Rose shares Jamia's and Aazim's information with the Local Coordination Point under Chapter 16A, and continues to assist Jamia with her accommodation needs.

5.3 Victim under 18 years of age

In cases of domestic violence where children are victims or are affected by domestic violence in the home, prescribed bodies should exchange information under Chapter 16A in the first instance. Chapter 16A prioritises the safety, welfare, and wellbeing of a child or young person over an individual's right to privacy.

Alternatively, where Chapter 16A does not apply, information may be shared under Part 13A and the Protocol.

5.4 Perpetrator under 18 years of age

In cases of domestic violence where the perpetrator is less than 18 years of age, the decision to apply Chapter 16A of the *CYPCP Act* will depend on a consideration of the safety and wellbeing of the young person and managing any threat to the victim. This decision should be made by the prescribed body involved.

Where Chapter 16A does not apply, information may be shared under Part 13A and the Protocol.

5.5 Pregnant victims

Prescribed bodies may rely on Chapter 16A to share information relating to the safety, welfare or wellbeing of an unborn infant and the family of the unborn infant, but only where the unborn child is the subject of a pre-natal report to the FACS or a referral to a Child Wellbeing Unit.

In accordance with the *CYPCP Act*, prescribed bodies must make a report to FACS or the Child Wellbeing Unit or confirm the existence of a pre-natal report before providing information about the mother and the unborn child under Chapter 16A.

In all other cases, information sharing in relation to a pregnant victim of domestic violence should occur under Part 13A and the Protocol.

6. Principles and objectives

This Protocol has been developed according to the following overarching principles and objectives. Service providers should be mindful of these at all times when sharing information under Part 13A and the Protocol.

6.1 Principles

When sharing information, service providers are to be guided by the following principles:

- The safety of victims and their children is paramount.
- Individuals have rights to both safety and privacy, but where these rights are in tension, victims' safety comes first.
- There is a presumption that informed consent to share information must be sought and obtained from victims. However, there are some limited exceptions to the requirement for consent.
- Victims can choose the service providers with which they engage.
- Victims have the right to receive domestic violence support services without consenting to information sharing.
- Victims have the right to access information held about them by service providers, and are able to correct that information.
- Information shared must be secure, timely, accurate and relevant.

6.2 Objectives

Part 13A and the Protocol support the proactive practice of information sharing between service providers to:

- increase the safety, health and wellbeing of victims and any children, and prevent domestic violence related death, disability and injury
- improve domestic violence victims' access to support services regardless of which service provider the victim first approaches or whether they have engaged with the justice system
- achieve consistent and improved threat identification and management of threat to victims
- prioritise victims who are at serious threat and undertake safety planning to reduce the serious threat
- reduce re-victimisation of persons who have experienced domestic violence
- improve perpetrator accountability for their actions
- reduce re-offending
- identify and respond to escalation of violence by the perpetrator
- improve service provider accountability for their response to victims and perpetrators.

7. Information sharing under Part 13A

The Protocol explains Part 13A and must be referred to by service providers to ensure they collect, use or share personal and health information of victims, perpetrators or other persons lawfully.

Part 13A allows sharing personal and health information about victims, perpetrators and other persons between service providers in defined circumstances. This chapter explains the legal basis and legitimate purposes for sharing information under Part 13A.

7.1 Legal basis for sharing information

Information about a domestic violence victim and a perpetrator may be shared at first instance under the Protocol where:

- there is a domestic violence threat, by a service provider
- there are ADVO proceedings, by a NSW Local Court
- disclosed by the NSW Police Force for contact purposes.

Subsequently, information can continue to be shared in any of these cases by any service provider that receives this information, where it is for a legitimate purpose as set out in section 7.3 of the Protocol.

Refer to:
The *Child Wellbeing and Child Protection NSW Interagency Guidelines*: providing and requesting information under Chapter 16A.

Where children are victims or are affected by domestic violence in the home, service providers who are prescribed bodies should take any actions as required under the *CYPCP Act* and share information under Chapter 16A of that Act.

7.2 Sharing information where the legal basis under Part 13A is not met

There may be situations where service providers want to share information about a perpetrator and a victim where the legal basis in section 7.1 of the Protocol is not been met.

Refer to:
Section 27 of the *PPIP Act* permits the NSW Police Force to share information without the requirement to comply with Privacy Principle conditions.

In this situation, personal and health information about a victim and a perpetrator can only be shared without consent, where:

- the service provider reasonably believes there is a serious and imminent threat to the life, health or safety of a person
- it is reasonably necessary for the NSW Police Force to carry out its functions, and there are reasonable grounds to believe that an offence may have been committed.

Personal and health information about a perpetrator may also be shared without consent where a service provider believes that a criminal offence may be committed or that a perpetrator's behaviour or attitude may affect another person's life, health or safety. In this situation, information about the victim cannot be shared without their consent.

In all other circumstances, the consent of the victim and the perpetrator is required to share personal or health information.

In deciding whether to disclose information to a law enforcement agency, a service provider should consider:

- whether the circumstances indicate a serious and imminent threat to the life, health or safety of a person
- relevant professional and ethical obligations
- how to best balance the protection of the perpetrator's privacy with the serious and imminent threat to a person.

Case study: Serious and imminent threat

Terry is in custody for burglary. Three days before his release, he tells a number of people including a Corrective Services nurse that his ex-wife's new partner Martin's days are numbered. Terry has a history of violence and assault charges.

Terry's ex-wife Trisha does not currently receive domestic violence support services.

Based on the nurse's professional assessment of the situation, there are reasonable grounds to believe that Trisha and Martin are at serious and imminent threat from Terry upon his release from custody.

The nurse can share information with the NSW Police Force.

7.3 Legitimate purpose for sharing information

Service providers may only collect, use and disclose victims' and perpetrators' personal and health information under Part 13A and the Protocol to:

- make a referral for domestic violence support services for a victim
- provide support services to a victim
- prevent or lessen a serious threat to a person's life, health or safety.

If allowed, information can alternatively and additionally be shared under Chapter 16A of the *CYPCP Act* to:

- make a decision or undertake an assessment or safety plan
- initiate or conduct an investigation
- provide a service to children and their families
- manage a risk to the child or young person.

Case study: No legitimate purpose

Layla has been the victim of domestic violence. She was assessed as at threat and has begun counselling sessions with Marie who works in a local domestic violence support service.

Layla has returned to her studies, and to enhance her employment prospects, has started seeing a tutor, Adam. She has told Adam that she is seeing a counsellor but has not disclosed the reason for this.

Several weeks later, Adam contacts Marie seeking information about Layla, as he believes that he and Marie can support Layla better if they have more detail about other services Layla is accessing.

Whilst it is possible that Marie and Adam could better support Layla by working together, sharing information in this circumstance does not meet any of the purposes under the Protocol. The information sharing would not be to facilitate access to domestic violence support services.

Therefore, Marie cannot share personal or health information about Layla with Adam.

Note: Where Marie reports the conversation to Layla and asks her if and what information she can share with Adam (with the intention of working together to better support her), and Layla gives her consent, information can be shared under NSW privacy laws, but only Layla's information. The perpetrator's information cannot be shared.

7.4 Information sharing for other purposes

There may be times when a service provider needs to share personal and health information about a victim or a perpetrator unrelated to the purposes allowed under Part 13A and the Protocol, or with a service provider that does not provide domestic violence support services within the meaning of Part 13A.

The provisions of Part 13A and the Protocol cannot be relied on in these circumstances, and Commonwealth and/or NSW privacy laws may apply to that information. For example, information about the perpetrator cannot be shared without the perpetrator's consent.

When sharing information for purposes other than those under Part 13A and the Protocol, service providers must:

- discuss the need for information sharing with the victim, and seek their consent to provide their personal and health information to the service provider
- where the victim consents, make a written record of the victim's consent, including the victim's information that can be disclosed
- where NSW or Commonwealth privacy laws apply, ensure the information shared complies with those laws, such as only sharing information relating to the victim
- advise and add the following statement to all written communications to the receiving service provider:
  - any inappropriate disclosure of the information has potential harmful consequences for the victim's safety,
  - the information is provided on the basis that the receiving service provider does not use it for any purposes other than that outlined in the referral/information request, and
  - the receiving service provider must not disclose that information further without the victim's consent.

7.5 Domestic violence proceedings dismissed or not proven

Where domestic violence proceedings are dismissed, withdrawn or not proven, a service provider working with the victim must consider the level of threat to the victim:

- if the victim is identified at serious threat, information sharing should continue,
- if the victim is identified at threat, information sharing can continue if the victim consents; the consent of the perpetrator is not required, or
- stop sharing information under the Protocol, and make a written record that information sharing under the Protocol has been stopped and why, and keep this record on file. Information about the victim can be shared under NSW privacy laws, with their consent, but no information about the perpetrator can be shared.

When considering whether the victim may still be at threat or at serious threat, a service provider must also take into account the circumstances that led to the domestic violence proceedings being dismissed, withdrawn or not proved.

Where children are victims or are affected by domestic violence in the home and there are concerns for their safety, welfare or wellbeing, service providers that are prescribed bodies must take actions as required under the *CYPCP Act* and information sharing can continue under Chapter 16A of that Act. Refer to Chapter 5 Protocol and child protection legislation and the *Domestic Violence and Child Protection Guidelines*.

8. Threat identification

Under Part 13A, service providers can share information where they identify that there is a threat or a serious threat to the life, health and safety of a victim. Identifying the level of threat is also important to enable service providers to address victims' immediate safety needs, to explore support that may be required, such as legal protection, support through the court process, ongoing safety planning, counselling, housing, financial or other assistance, and to make referrals for the provision of those supports.

This chapter outlines the process for consistent threat identification of victims of domestic violence.

8.1 Domestic violence threat

A domestic violence threat is a threat to the life, health or safety of a person that occurs because of the commission or possible commission of a domestic violence offence.

Victims may suffer different levels of threat and it is important to identify as accurately and as early as possible the level of threat they face, so that the most appropriate support services can be provided to them.

Service providers must consider that particular domestic violence acts or behaviours indicate a higher level of threat to a victim. For example, attempted strangulation or choking immediately place a victim within reach of a dangerous threshold level and is often a predictor for more serious violence.

In addition, there are identified persons and communities that, due to their situation of social and cultural disadvantage, isolation, or increased dependence, are particularly vulnerable to domestic violence threats. For example women from Aboriginal and Torres Strait Islander communities, from cultural and linguistically diverse communities, and with disabilities and/or in residential settings.

8.2 Assessing the level of threat

The identification of a victim at threat is based on the following combination of factors:

- the Domestic Violence Safety Assessment Tool (DVSAT) or other recognised risk assessment tool where the total number of identified threat indicators meets the threshold for at threat or at serious threat , and/or
- professional judgement, and
- where available, the victim's perception of their own level of threat and the threat to their children, and
- the threat is a domestic violence threat.

A victim is automatically identified as at serious threat where the NSW Police Force apply the DVSAT on three separate occasions in a six-month period with a victim.

> Professional judgement can never be used to downgrade the level of threat identified by a completed DVSAT or other risk assessment tool.

For more information on threat and assessment of threat, refer to the Domestic Violence Safety Assessment Tool Guide. The Guide also includes the most recent version of the DVSAT and information on how to use the tool.

Case study: Police DVSAT – at threat

The NSW Police Force attend a home following a phone call from neighbours reporting a domestic violence disturbance between Connie and Victor. The Police apply the DVSAT and based on Connie's answers ('yes' to the question related to pregnancy and to Victor having been physically violent towards her in the past) identify her at threat.

The Police apply for a provisional ADVO and make an automatic referral to the Central Referral Point, recording Connie as at threat.

Case study: Service provider DVSAT – at threat

Maria attends a domestic violence support service to seek advice on her options in relation to dealing with her partner, Nico who has become jealous and controlling of her life. Janet applies the DVSAT. The context is domestic violence and Maria's answers to the DVSAT, together with Janet's professional judgement and Maria's own perspective of the level of threat to her by Nico place her within the threshold for at threat.

Janet seeks Maria's consent and makes a referral to the Central Referral Point.

There may also be times when a service provider cannot complete a DVSAT due to the nature of their work, such as a general practitioner in a medical clinic. For this reason, the DVSAT should not be the sole instrument relied on to assess a victim's level of threat. It is important to consider the victim's experience and perception of the violence, and the judgement of the professional applying the tool.

Case study: Professional judgement and victim's own perception – at threat

Dr Cabello, a local GP is in consultation with Julie, a patient who is seeking treatment for a badly sprained elbow. Julie reports that her partner, Craig has been violent towards her and caused her to fall over during an argument. Julie tells the doctor that her fear of Craig is increasing and that she is considering moving out with a girlfriend. Given Julie's disclosure, Dr Cabello asks some additional questions and then tells Julie she is concerned there is a current domestic violence threat. The doctor seeks Julie's consent to share her information with a domestic violence support service.

The context is domestic violence and although no formal assessment is completed, Dr Cabello uses her professional judgement and Julie's own perception of her level of threat to identify that Julie is at threat of domestic violence and makes a referral to the Central Referral Point.

A person can rely on their professional judgement alone to assess the victim's level of threat, with or without the victim's perception of their own level of threat. Professional judgement is an assessment based on information gathering with the victim, professional discretion or intuition that may be justified through the service provider's qualifications and/or experience.

A person can use their professional judgement to upgrade the level of threat where the threshold for at serious threat has not been met on the DVSAT.

Similarly, the victim's perception of their own safety can be used to upgrade a level of threat.

A person can never use their professional judgement to downgrade the level of threat identified by a completed DVSAT or other risk assessment tool.

Case study: Police DVSAT and professional judgement – at serious threat

The NSW Police Force attend a home following a phone call from neighbours reporting a domestic violence disturbance. They charge Clive with a domestic violence offence and apply for an ADVO on behalf of Jackie. The police officer completes a Police DVSAT with Jackie, and she answers 'yes' to the number of questions that place her below the threshold for at serious threat. In light of the seriousness of the domestic violence and the charges laid against Clive, the police officer uses his professional judgement to upgrade the threat level to Jackie to at serious threat. The police officer makes a referral to the Central Referral Point, recording Jackie at serious threat.

Case study: Professional judgement and victim's own perception – at serious threat

Jamila attends a doctor's surgery after being assaulted by her partner Salaam. The doctor is not trained in the use of a threat identification tool, but based on the evidence of physical injury and her psychological state, the doctor believes that Jamila is at serious threat. The doctor asks Jamila for an assessment of her own level of threat, and Jamila says she is worried Salaam will seriously harm her. With Jamila's consent, the doctor makes a referral to the Central Referral Point based on his professional judgement and Jamila's own perception of the threat to her life, health and safety.

The dynamics of domestic violence are such that a victim's response may vary over time and depending on which service provider administers the assessment tool. This may be because of fear of speaking with particular service providers, the circumstances of the domestic violence, the proximity of the perpetrator or other persons to the victim when the tool is being applied, or for other reasons.

Case study: Victim varied response to DVSAT

The Local Coordination Point receives an automatic referral from the NSW Police Force. The NSW Police Force application of the DVSAT has identified Georgina as at threat. The Local Coordination Point contacts Georgina to offer domestic violence support services.

When the Local Coordination Point speaks to Georgina, she reports her distrust of police and that she did not want to answer the officer's questions fully because her husband, Simeon, was present at the time. The Local Coordination Point undertakes a comprehensive threat assessment with Georgina and re-applies the DVSAT. Georgina answers the questions fully this time, and the assessment identifies that there is a serious threat to Georgina's life, health and safety.

8.3 Domestic Violence Safety Assessment Tool

The consistent and ongoing application of a common threat identification tool is essential to determine the level of threat faced by a victim. This ensures that, regardless of how victims enter the system, the system response is consistent and victims are connected to the most appropriate domestic violence support services to meet their needs.

To achieve consistent identification of threat to victims, application of the Domestic Violence Safety Assessment Tool (DVSAT) is encouraged.

The DVSAT consists of a series of questions that relate to recurring factors or behaviours that are recognised as indicators of threat to victims of domestic violence. Based on these indicators, the DVSAT provides a score of the seriousness of the threat to a victim. The victim's responses to the questions provide a score that is then considered against a set threshold. The score suggests that there is:

- not sufficient evidence of a threat to the victim
- evidence of a threat to the victim
- evidence of a serious threat to the victim.

The threshold to determine the level of threat to a victim is set out in the Domestic Violence Safety Assessment Tool Guide. Refer to the DVSAT Guide for the most recent version of the DVSAT and for further information on how to use the tool.

8.4 Other risk assessment tools

While the consistent application of the DVSAT is encouraged, its use is not mandatory under the Protocol. Other service providers may apply their own recognised assessment tool to determine the level of threat to a victim if they align with commonly agreed risk indicators for domestic violence.

8.5 Review of threat assessment

A comprehensive review and assessment using the common DVSAT provides consistency in identifying domestic violence threats and developing appropriate responses across all referrals.

Upon receipt of a referral (refer to Chapter 9 Victim referral to support services), the Local Coordination Point must conduct a comprehensive assessment of the level of threat to the victim. In cases where the DVSAT was not applied, such as where the level of threat was determined by professional judgement or by a different risk assessment tool, the Local Coordination Point must apply the DVSAT.

The Local Coordination Point will either confirm the level of threat or upgrade a threat to a serious threat. The Local Coordination Point must never downgrade the original assessment of threat, until further actions have been undertaken. Refer to section 8.7 Downgrading threat assessment.

Case study: Review of threat does not downgrade original assessment

Nicoli and his partner Carlos have been in a relationship for four months. Carlos' controlling behaviour has escalated over the past two months and he is increasingly jealous and controlling towards Nicoli. One morning Carlos and Nicoli have an argument and Carlos gets into a rage, smashes furniture and some of Nicoli's belongings and threatens to do the same to Nicoli.

Nicoli is terrified but does not want to call the police. He makes an appointment to speak to his counsellor. Nicoli is still very agitated and fearful while recounting to the counsellor the violence and Carlos' threats to harm him. The counsellor is very concerned for Nicoli's safety but does not have access to the DVSAT. She uses Nicoli's perception of the level of threat and her professional judgement to determine that Nicoli is at serious threat. She refers Nicoli to the Central Referral Point.

The Local Coordination Point receives the referral and contacts Nicoli the following day. A support worker undertakes a comprehensive risk assessment of Nicoli's threat level by applying the DVSAT. Nicoli's answers place him below the threshold for at serious threat.

Even though the level of threat is only identified as at threat using the DVSAT, the Local Coordination Point still considers Nicoli to be at serious threat, as professional judgement and Nicoli's own perception of his level of threat were relied upon.

The Local Coordination Point seeks Nicoli's consent and still refers him to a Safety Action Meeting and makes appropriate referrals to secure Nicoli's immediate safety.

8.6 Subsequent threat assessment

In domestic violence situations, it is common for the level of threat to fluctuate or escalate very rapidly. For this reason, it is important that service providers identify at the earliest opportunity when a victim has moved from at threat to at serious threat.

The victim's circumstances, a victim's self-report, or professional judgement may guide when a further assessment is required. As a guide, circumstances such as those listed below may trigger a new threat assessment:

- Victim has separated from the perpetrator or current partner
- Victim has a new partner
- Perpetrator is about to be released from detention
- Initiation of family court matters
- Victim or perpetrator loss of employment
- Victim is pregnant or gives birth
- Victim ends engagement with support services
- Information suggests the perpetrator is back living with the victim
- Perpetrator becomes aware the victim is engaged with support services
- Information indicates the perpetrator is escalating in their substance abuse or is experiencing increased mental health symptoms.

Case study: New information changes level of threat

Vladimir suffers from depression and an obsessive-compulsive disorder, and attends a Men's Behaviour Change Program (MBCP). Vladimir reveals to a number of people at the MBCP that he believes his partner Ivana has started an intimate relationship with another man and that he has threatened to harm her as a result.

Ivana is being supported by a partner support service in accordance with the minimum standards for MBCPs. She was previously assessed as at threat and referred to a Local Coordination Point for support.

The Manager of the MBCP is concerned about Ivana and contacts the partner support service to provide information about Vladimir's threats to harm Ivana.

In light of this new information, the partner support service contacts Ivana and completes a new assessment to review the level of threat to Ivana. The new assessment identifies that Ivana is at serious threat and the support service immediately begins safety planning with her.

With Ivana's consent, the support service makes a referral directly to the Local Coordination Point to include Ivana on the next Safety Action Meeting.

8.7 Downgrading threat assessment

A service provider can only downgrade a victim's identified threat level if:

- a change in the victim's circumstances has occurred that reduces or eliminates the threat, or
- actions taken by service providers have reduced the threat. Actions may include verification of the change in the victim's circumstances that reduces or removes the threat, and
- consideration of the victim's perception of their own safety.

Where the level of threat is downgraded, the service provider must make a record in the victim's file and notify the Local Coordination Point.

Case study: Actions taken result in downgrading level of threat

Pilar and Gustav have been living together for 6 years in a small town in regional NSW. Gustav is very controlling and emotionally abusive towards Pilar, and there have been occasions during the relationship where Gustav has been physically abusive towards Pilar.

On one occasion, Gustav seriously assaulted Pilar, but Pilar did not seek police assistance or legal protection.

The relationship is experiencing difficulties due to Pilar confessing to an affair with an ex-partner. The affair ceased months ago, and Gustav and Pilar are making efforts to rebuild their relationship. It has not been very successful, and Gustav's behaviour is becoming more and more controlling and abusive towards Pilar, while Pilar begins to spend more time at work and with friends to avoid confrontations.

More recently, Pilar has noticed that Gustav is monitoring her emails and mobile phone.

In the week leading up to a second serious domestic violence assault, Gustav's behaviour becomes more threatening and one evening Pilar comes home from work and is assaulted by Gustav resulting in her arm being fractured.

NSW Police Force attend and Gustav is charged with assault occasioning actual bodily harm. The police also take out an ADVO that includes an exclusionary order from the home he shares with Pilar.

NSW Police Force assess Pilar as at serious threat and make a referral to the Central Referral Point.

The referral is allocated to a Local Coordination Point and listed at the next Safety Action Meeting.

Pilar returns home from hospital the following morning and, after speaking to her mother in Sydney, makes a decision to leave the relationship and move back to Sydney. Her plans are to move within the next fortnight, apply for a work transfer and stay with her mother until she finds her own accommodation.

When Cassie from the Local Coordination Point calls Pilar to offer domestic violence support services, Pilar informs her of her plans. Cassie makes a referral for legal support for Pilar in the assault matter and lists her on the next Safety Action Meeting.

At the Safety Action Meeting, Cassie informs the members that Pilar is moving to Sydney and that she has made referrals for court support and counselling.

Actions from the Safety Action Meeting include;

Cassie to arrange for Pilar's file in the assault case to be transferred to the Local Coordination Point in Sydney, including listing Pilar on the Safety Action Meeting in Sydney.

Cassie to develop a personal safety plan with Pilar and inform her of the actions that were developed at the meeting.

Housing NSW to contact Housing Pathways for an assessment of Pilar's eligibility for community housing and to make a referral for her.

When the Safety Action Meeting is held in Sydney a fortnight later, the members are prepared with information they have received from their counterparts in Orange, and with information relating to Pilar's current situation, provided by the Sydney Local Coordination Point. The members are informed that Pilar has changed her mobile phone, that Gustav does not know she has moved to Sydney and that Pilar has been linked in with domestic violence support services in Sydney.

Case study: Actions taken result in downgrading level of threat, cont.

They note she is staying with her mother but community housing is currently being arranged for her. They are also informed that Pilar has indicated she no longer fears for her safety.

The Safety Action Meeting members do not have any new actions in relation to Pilar and close the case.

When the Local Coordination Point next contacts Pilar, her threat assessment is reviewed and it is agreed that Pilar's threat can now be reduced to at threat. The worker makes a note on Pilar's file.

For specific information on threat assessment and how to use the DVSAT, refer to the *Domestic Violence Safety Assessment Tool Guide*.

9. Victim referral to support services

Referrals support victims' access to domestic violence support services to address their safety and welfare needs. Part 13A allows sharing personal and health information of the victim and the perpetrator of domestic violence when making a referral. This avoids the victim having to repeat their story each time they are referred to a new service provider.

To share information under Part 13A, referrals initially must be made to the Central Referral Point and/or a Local Coordination Point.

Where a victim is identified at serious threat other consent provisions apply, and referrals can also be made to other service providers in addition to the referral to the Central Referral Point or a Local Coordination Point. Refer to Chapter 13 Serious threat.

This chapter explains the role of the Central Referral Point and the Local Coordination Points. It also provides information on referrals to address victims' safety needs.

Where children are victims or are affected by domestic violence in the home, service providers that are prescribed bodies under the *CYPCP Act* should exchange information under Chapter 16A of that Act. Refer to Chapter 5 Protocol and child protection legislation and the *Domestic Violence and Child Protection Guidelines*.

9.1 Central Referral Point

Most initial referrals under Part 13A are made to the Central Referral Point. The Central Referral Point is a state-wide electronic data collection and referral platform. The Central Referral Point receives and sorts referrals from all service providers and allocates them electronically to a Local Coordination Point based on the victims' gender and location. This process is fully automated.

Part 13A allows the Central Referral Point to electronically process the information it has received and allocate the referral to a Local Coordination Point without the victim or perpetrator's consent.

The Central Referral Point also monitors the responsiveness of the system to victims' needs, from referral to case closure. It provides real time de-identified data on domestic violence referrals and the timeliness of services provided to victims. For this reason, it is recommended that service providers complete a de-identified referral even where the victim has not consented to share their information.

9.2 Local Coordination Point

The Local Coordination Points are a network of non-government services that provide case coordination, threat assessment and review, and safety planning for victims of domestic violence. They also ensure that victims at serious threat are considered at a Safety Action Meeting. For more information on Safety Action Meetings, refer to the *Safety Action Meeting Manual*.

The Local Coordination Points receive referrals electronically from the Central Referral Point. The Local Coordination Points access referrals by logging into the electronic database and retrieving the referral information relevant to their location.

Part 13A allows service providers to make initial referrals directly to the Local Coordination Point. The Local Coordination Point will enter the referral information into the Central Referral Point, with the victim's consent. However, service providers are encouraged to make the initial referral to the Central Referral Point first.

9.3 Victim already supported by a support service

Victims with an existing relationship with a domestic violence or other support service and receiving case management and support may continue to be supported by that service. It is good practice to maintain a continuity of care. Service providers should still make a referral to the Central Referral Point or Local Coordination Point to ensure that no victim falls through the gaps. This enables the Central Referral Point to record the service provided to all victims, and collect accurate data regarding the number of victims experiencing domestic violence and the services required to meet their needs.

A referral to the Central Referral Point or Local Coordination Point is essential to refer victims at serious threat to a Safety Action Meeting. For more information on Safety Action Meetings, refer to the *Safety Action Meeting Manual*.

9.4 Referrals to Safety Action Meetings

Referrals to Safety Action Meetings for victims at serious threat are made through Local Coordination Points. Victims at serious threat must be referred to the Central Referral Point, or directly to a Local Coordination Point, for inclusion at a Safety Action Meeting.

Information shared at a Safety Action Meeting must only be used for the purpose set out in Part 13A and the Protocol. For more information on Safety Action Meetings, refer to the *Safety Action Meeting Manual*.

9.5 Types of referrals

Two types of referrals can be made where a victim has been identified at threat:

1. an automatic referral, which may be made by:
   - NSW Police Force – without the consent of the victim or perpetrator, or
   - a NSW Local Court – where the victim has not expressly objected to their information being disclosed, and without the consent of the perpetrator; and
2. a consent-based referral, which can be made by a service provider with the consent of the victim but without the consent of the perpetrator.

9.6 Automatic referrals

Automatic referrals are referrals from the NSW Police Force or a NSW Local Court to the Central Referral Point.

The NSW Police Force makes an automatic referral to the Central Referral Point where the NSW Police Force has attended a domestic violence incident or a domestic violence incident is reported to them.

The NSW Police Force does not require the consent of the victim to make an automatic referral, but must inform the victim that a referral will be made to the Central Referral Point and on to a Local Coordination Point.

A NSW Local Court makes an automatic referral to the Central Referral Point only where there are ADVO proceedings, that is where and ADVO has been sought or made.

The NSW Local Court does not require the explicit consent of the victim to make the referral, but the victim can choose to opt out of the referral. The victim can exercise this option when the NSW Local Court informs the victim that a referral will be made to the Central Referral Point and on to a Local

Coordination Point. There are two ways in which a victim can opt out; the victim can:

- agree to a referral being made to the Central Referral Point, but object to any subsequent referral being made to a particular Local Coordination Point. In this case, the referral will be made to another Local Coordination Point, or
- opt out of being referred to any service; in this case, no referral will be made to the Central Referral Point for the victim.

The perpetrator's consent is never required to make an automatic referral.

Case study: Opting out of a Local Court referral

Diana makes a private application for an ADVO against her husband, Dirk, at a regional NSW Local Court. On completing the application, the Registrar advises Diana that she will be referred to the Local Coordination Point (via the Central Referral Point) and that someone will contact her to offer domestic violence support services.

Diana tells the Registrar that she does not want to be referred to any service. The Registrar asks why and Diana explains that Dirk's sister works at the Local Coordination Point in the area. The Registrar tells Diana that in that case he will add information on the referral that there is a conflict of interest with that Local Coordination Point and that Diana should be referred to another Local Coordination Point. Diana consents to the referral.

In the event that Diana still does not want to be referred to any Local Coordination Point, the Registrar would not make the referral but, without identifying Diana, would advise the Central Referral Point that an application for an ADVO was made, the postcode of the victim and that the victim opted out of the referral.

9.7 Victim consent and automatic referrals

Upon receipt of an automatic referral via the Central Referral Point, the Local Coordination Point must contact the victim using the information in the referral, to offer domestic violence support services. At this point, the victim's consent must be sought to use the information to provide a service, to share the information or to make a further referral to another service provider. For detailed information on how to seek consent, refer to Chapter 12 Consent.

There are some permitted exceptions to this where a victim is at serious threat, and the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of a person. For more information, refer to Chapter 13 Serious threat.

9.8 Consent-based referrals

Consent based referrals: A victim's consent is always required.
A perpetrator's consent is never required.

These referrals can only be made with the explicit consent of the victim and are for providing domestic violence support services to the victim. The consent of the perpetrator is never required.

Case study: Consent based referral

Mary attends a community health centre and tells a worker that Tim, her partner, has been threatening her. Mary would like to know what options are available to her. The service provider assesses Mary as being at threat and asks Mary's consent to be referred to the Central Referral Point for specialist domestic violence case coordination and support. Mary consents to information about her being shared with the Central Referral Point.

Consent based referrals may occur:

- initially, when a service provider working in an area such as health, education, community services, disability services, housing, domestic violence or other services assesses that a victim is at threat or at serious threat of domestic violence and wants to refer the victim to the Central Referral Point and/or Local Coordination Point for domestic violence support services, or
- subsequently, consent based referrals can be made for providing domestic violence support services to a victim by:
  - the Local Coordination Point to any service provider, or
  - a service provider to another service provider, where the initial referral came through the Central Referral Point and/or a Local Coordination Point.

A key aspect of the coordinated response for victims is that service providers can make initial and subsequent consent based referrals to complement their service delivery and meet the needs of victims.

Case study: Subsequent consent based referral

Li makes a private application for an ADVO against her partner Jiang in the Local Court. A referral is made to the Central Referral Point and then allocated to a Local Coordination Point.

She receives a phone call the following day from the Local Coordination Point and accepts their support. Li advises that she would like assistance with finding accommodation so she can leave Jiang. The Local Coordination Point helps Li find a refuge and asks Li for her consent to share her information to make the referral to the refuge. Li is concerned that her community is small and she does not want people to know about her situation. The Local Coordination Point worker informs Li that there are strict confidentiality and security guidelines for any information shared with another service provider, but that if Li is unsure, she can be referred but her history or case information will not be shared.

Li is reassured and consents to the referral and to having her information shared with the refuge.

For more information on consent, refer to Chapter 12 Consent.

9.9 Information provided to victim before referral

When making an automatic or a consent based referral, service providers should provide the following information to the victim either before or at the time of making the referral:

- that a referral will be made and to which service provider
- that the referral is for providing domestic violence support services
- the potential services that will be provided by the service provider
- contact details of the service provider receiving the referral, where possible

- a statement that information will not be disclosed to the perpetrator
- details of how the victim can access and amend information provided in the referral
- an explanation that accepting any services offered is voluntary.

Service providers working with victims from Aboriginal and Torres Strait Islander communities and from culturally and linguistically diverse backgrounds should consider cultural sensitivities when informing victims that their information will be shared with certain service providers. In particular, Aboriginal and Torres Strait Islander persons may be sensitive about sharing their information with government agencies, and may fear government agency interventions in their lives.

9.10 Victim contact

All referrals must include the victim's contact information and a safe method to contact the victim. Service providers must take detailed information from the victim about methods of communication to facilitate safe contact and ensure that interventions will not place them at further threat from the perpetrator. For example, a victim may request that the service provider call their mobile telephone at certain times of the day, or contact them via a new email address unknown to the perpetrator.

The service provider must follow the instructions on the referral by the referring service provider.

To ensure victim's safety, when making a telephone call the receiving service provider should also:

- call from a blocked number,
- check they are speaking with the victim before identifying themselves or the service from which they are calling
- check it is safe for the victim to speak
- if calling a mobile telephone, advise the victim that they may wish to delete any record of the call once the call is completed
- state that information will not be disclosed to the perpetrator.

If no safe method of contact is provided, service providers may contact the victim by email or post unless information in the referral suggests this would be unsafe.

9.11 Victim cannot be contacted

If a victim cannot be contacted after three separate attempts, this may be taken to mean the victim does not consent to receiving a service, and no further information can be shared.

Where there is information in the referral to suggest otherwise, the service provider must send back the referral to the referring service provider and record that no contact was made with the victim.

Where the victim has been assessed at serious threat, refer to Chapter 13 Serious threat.

Where the victim cannot be contacted and no further information is shared, the referring service provider must be informed. Information provided by the referring service provider must be securely destroyed. Refer to the procedure on disposal of personal and health information in Chapter 14 Information management.

9.12 Victim can receive support services without sharing information

When a service provider offers domestic violence support services to a victim, the service provider must advise the victim that they can choose to receive those services without having their information shared.

If the victim does not consent to their information being shared but still wishes to receive support services, a referral should be made that only includes information that the victim consents to being shared; for example, the victim's first name, date of birth and contact details.

Alternatively, the victim may be provided with the service provider's contact details and can then choose when and what information they disclose, directly to the service provider, and in their own time.

9.13 Information requests

Service providers may request information about a victim and/or a perpetrator from other service providers providing there is a legal basis to do so and it is for a legitimate purpose. Refer to Chapter 7 Information sharing under Part 13A.

The obligation to verify that the victim has given explicit consent for the disclosure of information rests with the service provider disclosing the information. This means that a service provider that has received a request must have satisfactory evidence of consent, either by:

- seeking the consent of the victim to release the information, or
- verifying that the victim has given their consent to the service provider requesting the information, and sighting the written consent.

This is essential to ensure that information is not disclosed in a manner that increases threat to a victim and to ensure the disclosing service provider complies with their obligations under the Protocol. It is also important where a service provider does not have an established relationship with the requesting service provider.

If the victim does not consent to their information being shared, the information must not be shared. The only exception is where a victim is identified at serious threat and the conditions for sharing information are satisfied under the Protocol. Refer to Chapter 13 Serious threat.

10. Identification of victim and perpetrator

There may be occasions where a service provider has concerns about the identification of the victim and the perpetrator in a domestic violence relationship, or where a victim is now identified as a perpetrator, or where both parties claim to be a victim. This chapter provides guidance to service providers on how to respond to these situations under Part 13A and the Protocol.

10.1 Victim and perpetrator incorrectly identified

A service provider may receive a referral or information regarding a victim and a perpetrator where it believes:

- the parties are incorrectly identified as victim and perpetrator at the scene of the domestic violence incident, or
- a private application for an ADVO at a NSW Local Court is made and may potentially be vexatious or frivolous, that is, the person listed on the ADVO as the victim may actually be the perpetrator.

Where a service provider forms this belief, on the balance of probabilities, then it may:

- consider if the person listed as the victim is assessed at serious threat. In this case, information should continue to be shared until further clarification,
- if the person listed as the victim is not assessed at serious threat, stop sharing information about the person listed as the perpetrator. Information can still be shared about the person listed as the victim with their consent,
- advise the referring service provider of the basis for the belief and that information sharing has been stopped,
- make a written record of the basis for the belief and that information sharing has been stopped, and keep this record on the file of the person listed as the victim, and
- apply the DVSAT to the person listed as the perpetrator or use professional judgement and take actions as necessary under the Protocol, including making a new referral to the Central Referral Point and/or a Local Coordination Point.

Case study: Service provider unsure that person referred is a victim

Mike contacts a men's crisis accommodation centre seeking temporary accommodation. Mike tells the worker that he has left the family home after a violent altercation with his wife, Rebecca. Mike reports that his wife has a substance abuse problem and that she is often unable to care for the children due to intoxication. He adds that Rebecca frequently throws things about the house and has attacked him using household implements. He reports that this time she has gone too far when she hit him and that he will seek an ADVO to protect himself

Mike arrives at the centre and upon further questioning by a support worker, says that he has successfully disarmed and restrained Rebecca in the past.

The worker completes the DVSAT with Mike, establishes that he is at threat, and makes a referral to the Local Coordination Point with Mike's consent. The worker also shares Rebecca's information in the referral.

When the Local Coordination Point contacts Mike he admits that he keeps a gun in the house and has been feeling depressed lately. Mike also exhibits anger towards Rebecca and blames her for losing his job.

From Mike's answers, the Local Coordination Point is unsure of the situation between Mike and Rebecca, but because Mike is identified as the victim, continues to support him. The Local Coordination Point stops sharing Rebecca's information when making referrals for more permanent accommodation and counselling for his depression.

Given concerns for the safety and wellbeing of the children who have remained in the care of Rebecca, the Local Coordination Point also completes the mandatory reported guide and takes any actions as required under the *CYPCP Act*.

There may be situations where a service provider stops sharing information about a person listed as the perpetrator and a court of law later determines that the victim and perpetrator were correctly identified (through granting an interim or a final ADVO, or a finding or plea of guilt for a domestic violence offence). In these cases, the service provider may resume sharing information about both the victim and the perpetrator, as identified in the referral, under the Protocol.

10.2 Perpetrator previously victim

A service provider may receive a referral or information about a victim and a perpetrator where there has been a history of domestic violence, and the person listed as the perpetrator in the current incident was previously:

- the primary victim in domestic violence proceedings, or
- assessed as being at threat from the person currently listed as the victim.

Where the victim in the current referral was previously the primary perpetrator, and is correctly identified in the referral, for example, by verifying with the referring service provider, they are entitled to benefit from the information sharing provisions under the Protocol, and to receive domestic violence support services.

Where a service provider receives a referral or information and forms the opinion that the person listed as the perpetrator in the current incident is the primary victim, the service provider should complete a threat assessment and, if necessary, make a referral to the Central Referral Point or a Local Coordination Point.

Case study: Perpetrator was previously the victim

Dana and Mirko were in a long term relationship characterised by domestic violence and have recently divorced. Dana has had a previous ADVO against Mirko following assault and stalking charges.

Recently, there have been confrontations between them about childcare arrangements for their daughter and one day both parents turn up to pick up the child. Mirko becomes verbally abusive and, coming in close to Dana, pushes her against a wall. Dana becomes fearful, lashes out, and scratches his face to get him to release her. Mirko yells out in pain and is seen holding his face by several witnesses. He calls the police.

When the police attend, Dana refuses to answer their questions. The police charge her with assault and make an application for a provisional ADVO against Dana. The police also make an automatic referral for Mirko to the Central Referral Point.

The Local Coordination Point who receives the referral identifies from records that Dana has previously been the victim and Mirko the perpetrator.

The Local Coordination Point continues to offer a service response to Mirko, but does not share information about Dana, and makes a referral to the Central Referral Point for Dana.

10.3 Both parties claim to be victim

A service provider may receive information or two separate referrals where both parties claim to be the victim. The service provider may wish to review available information relating to the parties, such as the circumstances of the current domestic violence incident or the existence of domestic violence proceedings, or seek clarification from the referring service provider to confirm the identity of the victim in the current domestic violence incident.

If there is no clear perpetrator and victim, then both parties can be treated as a victim and are entitled to receive domestic violence support services.

The decision to provide support services to one victim or the other rests with the service provider. For example, the decision may be based on which referral was first received by the service provider or whether the service provider previously worked with one of the persons listed in the referrals. In this case, the other referral must be sent back to the referring service provider for referral to a different service provider.

Case study: NSW Police make referrals for two identified victims

Police are called to an incident at Lucy and John's house in Cowra. On arrival, they find that both parties have serious injuries – John has stab wounds to the leg and Lucy has serious bruising to her face and neck. Lucy and John appear heavily intoxicated, and neither will speak to Police. Given the nature of the incident, Police assess both Lucy and John as at threat and make two referrals to the Central Referral Point.

The Central Referral Point refers Lucy to the Local Coordination Point in Cowra and John to the Local Coordination Point located within Victims Services NSW.

When the Local Coordination Point in Cowra speaks with Lucy, she discloses John's history of extreme violence towards her. Lucy states that she was sure that John was going to kill her that night, and only stabbed him in self-defence. The Local Coordination Point identifies Lucy as at serious threat and lists her on the agenda for the next Safety Action Meeting. The Local Coordination Point also contacts the Police and the Local Coordination Point supporting John to advise them of the situation.

The Local Coordination Point proceeds to support John carefully while ensuring that they do not share any information about Lucy that may place her at further threat from John.

Alternatively, if a service provider believes, on the balance of probabilities, that it should not continue to share information about, or provide domestic violence support services to one of the named victims, the service provider must:

- consider if the victim is assessed at serious threat. In this case, information should continue to be shared,
- if the victim is not assessed at serious threat, the service provider may stop sharing information,
- advise the referring service provider that information sharing has been stopped in relation to this victim,
- make a written record of the fact that information sharing has been stopped and why, and keep this record on file, and
- continue to share information for the provision of support services for the other identified victim.

11. Conflict of interest

This chapter provides guidance to service providers on how to identify and manage a conflict of interest in a way that will protect victims' safety and not breach their privacy. This is especially important for service providers that work in rural and remote communities, where the likelihood of conflicts of interest arising in the workplace is much higher.

11.1 Identifying a conflict of interest

A conflict of interest occurs when a worker's services to, or relationship with, the victim is compromised, or might be compromised, because of their existing professional or personal relationship with:

- the victim
- the perpetrator
- a third party (for example, a family member of the perpetrator).

In these situations, it may not be appropriate for the service provider to work with the victim.

A conflict of interest can be identified at the time a service provider receives a referral, or during the time they are working with a victim.

The actual or perceived safety of the victim must be a primary consideration for service providers dealing with a conflict of interest. For this reason, it is generally good practice for different service providers to deal with victims and perpetrators separately to avoid any real or perceived conflict of interest. Given the potential for serious threats and the sensitive nature of the work in the domestic violence context, service providers must have policies and procedures to ensure they can assist victims in a way that makes them feel protected and safe and that their privacy is protected. Such policies and procedures must also apply to the engagement of independent and professional translators or interpreters.

11.2 Dealing with a conflict of interest

Where a conflict of interest is identified, the matter should be declared immediately and escalated to a line manager for consideration whether the conflict can be dealt with through internal policies or procedures. If it can in a way that the safety and wellbeing of the victim is not compromised, then the service may provide services to both the victim and the perpetrator.

The following questions will help service providers consider whether their internal policies and processes are adequate to manage such a situation:

- Are procedures in place to identify and respond to conflicts of interest?
- Are procedures in place to ensure that separate staff members or teams work with the victim and the perpetrator?
- Will the victim feel safe and protected, and confident that their information will remain confidential?
- Are there information barriers so that information (verbal and written) about the victim cannot be shared with workers who:
  - have a personal relationship with the victim, or
  - have a professional or personal relationship with the perpetrator?

- If an identified conflict of interest can be managed internally, will an external party (client or other service provider) still perceive that the conflict of interest exists?
- Are there processes to monitor timing of appointments to ensure the victim and perpetrator do not come face to face in or around the premises?

Case study: No conflict of interest

A domestic violence support service receives a referral for Ofra, following a referral from the Local Court. The referral is allocated to Batel who has not had any previous client relationship with Ofra. As she reads the referral, Batel recognises the perpetrator's name as that of her cousin's ex-partner, whom she never met.

Batel stops reading and meets with her manager to discuss whether it is appropriate for her to work with Ofra given the relationship.

Batel maintains that she is confident that her professional ethics and prior relationship between her cousin and the perpetrator will not influence her decision-making capacity and her ability to support Ofra. Her manager is satisfied that Batel can maintain strict confidentiality and that, in the event that Batel feels the victim's safety would in any way be compromised, she will advise her manager straight away.

The manager of the support service documents the situation and records the outcome of the discussion. Batel continues working on the file.

Case study: Conflict of interest

In the same scenario, additional information indicates that the perpetrator, who runs a small real estate conveyance firm, is currently refinancing Batel's and a colleague's mortgages.

Batel, the colleague and her manager meet and conclude that the professional relationship with the perpetrator would compromise their ability to work with Ofra. As there is no other staff available to take on the referral, the manager decides that the referral should be sent to another Local Coordination Point.

All referral material is deleted and destroyed.

11.3 Returning a referral

Where a service provider determines that it cannot manage a conflict of interest internally or assist a victim in a way that makes them feel protected and safe, it must send the referral back to the referring service provider as soon as possible for reallocation.

In addition, the service provider must securely destroy any referral information collected and held in paper files and electronic databases. This practice is subject to any other legal and record keeping requirements that service providers are required to follow. Refer to Chapter 14 Information management.

12. Consent

Consent is an essential element of sharing and managing victims' personal and health information. Gaining consent is not only best practice in terms of privacy protection; it is also an individual's right under NSW privacy law. Unless otherwise expressly stated, when a service provider contacts the victim, the service provider must seek the victim's consent to share their personal and health information with other service providers.

In some cases, serious threats to the life, health or safety of victims, children and other persons will require that steps to prevent or reduce the serious threat will take precedence over the confidentiality and privacy of individuals' information.

This chapter provides information on consent requirements. For victims at serious threat, refer also to Chapter 13 Serious threat.

A consent flowchart to assist service providers comply with their obligations regarding victim's consent is located at Appendix 3.

A consent form to record victim's consent is located at Appendix 5. Service providers may to use the form, adapt it to their circumstances or use an existing internal consent form.

12.1 Essential elements of consent

Consent can be verbal or in writing and must be voluntary, informed, reasonably specific, current, and given by a person who has capacity to give consent.

Consent best practice

The essential elements of consent are:

Voluntary

Informed

Specific

Current

Capacity

Voluntary

Consent must always be voluntary. The victim must feel they have a genuine choice about whether to give or withhold consent. The victim must not be coerced, pressured or intimidated into giving consent. Sufficient time must be given to the victim so that they can consider the request and, if appropriate, take advice.

It is important to consider the experiences of victims from Aboriginal or Torres Strait Islander communities or from culturally or linguistically diverse backgrounds. Some communities' understanding of privacy may be influenced by cultural traditions and beliefs, and experiences of trauma may make victims fearful of giving consent to share their information.

Informed

Consent must always be informed. Make reasonable efforts to ensure that the victim has all the relevant facts and information they need to understand what they are consenting to, and what the consequences of consenting or not consenting may be, such as the potential loss of a privilege at law. For further information on privileges, refer to Chapter 15 Privileges and subpoenas.

Examples of relevant facts:

- the purpose for sharing the victim's personal and health information
- information will not be shared with the perpetrator
- who will have access to the information
- how the recipient will use the information
- whether provision of the information is voluntary or required by law
- the consequences of giving or refusing consent.

See Health Privacy Principle 4 and s.10 of the *PPIP Act*.

Any discussion with the victim must include an explanation that the services provided by the service provider may be declined, or that the victim may choose to receive services from the service provider without having their information shared.

Provide victims from Aboriginal or Torres Strait Islander communities or from culturally or linguistically diverse background with interpreters or translators, if necessary, to ensure that consent is informed.

Specific

The consent given by the victim must be specific. It must relate expressly to the purpose for sharing the information, such as to refer the victim for support services provided by another service provider, or so action can be taken to protect the victim and prevent or reduce a serious threat. It is important not to rely on a general or 'blanket' consent, as the victim may later feel they were not informed of the particular purpose for the information sharing and that their privacy has been breached.

Part 13A and the Protocol prescribe the different consent requirements depending on whether information is shared to:

- provide domestic violence support services to the victim; refer to Chapter 9 Victim referral to support services, or
- take action to prevent or reduce a serious threat to a person's life, health or safety; refer to Chapter 13 Serious threat.

Current

Consent has a use-by date and does not continue indefinitely. The validity of consent may be questioned where a lengthy period has passed or the victim's personal situation has changed. It is good practice to inform the victim of the specific period for which their consent will be valid. A recommended timeframe for consent is three months and no longer than twelve months. Service providers should also make it clear that a person is entitled to change their mind and revoke their consent at any time.

Capacity

Generally, when a person has capacity to make a particular decision, they are able to do all of the following:

- understand the facts involved
- understand the main choices
- weigh up the consequences of the choices
- understand how the consequences affect them
- communicate their decision.

A victim cannot give consent or make other decisions if they do not have the necessary capacity to do so. Incapacity may be due to youth, age, injury or illness, or physical or mental impairment. This means that, where there is a doubt about a person's capacity, this capacity must be re-assessed every time a decision around consent is required.

The following principles apply when assessing a person's capacity:

- always presume a person has capacity
- capacity is decision-specific
- avoid the assumption that a person lacks capacity based on appearances
- assess the person's decision-making ability, not the decision they make. A decision that is regarded as uninformed or misguided does not indicate a lack of capacity, even if the victim makes a decision that the service provider believes may not be in their best interest
- respect a person's privacy
- substitute decision-making is a last resort.

The complexity, seriousness and impact of the decision will influence the level of understanding required. A victim's capacity to consent may depend on appropriate support provided to them, such as using an interpreter or a support person for a victim with a physical, mental or cognitive impairment.

When seeking written consent, service providers must be sensitive to the written language capacity of victims.

Test for capacity:

Section 7 HRIP Act establishes a test for capacity and states that a person is incapable of giving consent if they:

- cannot understand the general nature and effect of a particular decision or action under the *HRIP Act*, or
- cannot communicate their intentions or consent (or refusal of consent) to the decision or action.

This test for capacity is a guide only and does not necessarily govern how consent should be given under the Protocol.

12.2 Giving consent on behalf of victim

- Where a victim is incapable of giving consent, an authorised representative may give consent on their behalf where the information concerned is health information. The *HRIP Act* sets out the list of people who can be an authorised representative:

Refer to:
Section 8 HRIP Act.

- someone who has an enduring power of attorney for the victim, or
- a guardian within the meaning of the *Guardianship Act 1987*, or a person responsible within the meaning of Part 5 of that Act who has been allocated a specific function to provide consent to medical or support services, or
- any other person who is authorised by law to act for or represent the victim.

Before allowing an authorised representative to give consent on behalf of a victim to share health information, the service provider must take reasonable steps to ensure that the authorised representative is not also the perpetrator or acting on behalf of the perpetrator.

In cases where the victim does not have the capacity to give consent and the authorised representative is not available, information cannot be shared unless the victim is also at serious threat.

12.3 Implied consent

Implied consent means that a victim does not explicitly, either verbally or in writing, give their consent to share information. Under NSW privacy laws, consent can be inferred by, for example:

- conduct or behaviour and the facts and circumstances of a particular situation
- silence or inaction
- consenting to one action, thereby implying their consent to a range of other actions.

Case study: Victim gives implied consent

Trudi is a young woman with three small children. She lives in a rented house five kilometres from a large regional centre. Trudi goes to a non-government service provider in a very distressed state accompanied by her three children. Trudi's regular counsellor, Agnes, comes in and speaks to her.

Trudi tells Agnes that her uncle Tim has moved in with her and the children. When Trudi confronted Tim after she discovered that he had not paid rent as he had promised to do and she had received an eviction notice as a result, Tim threatened to hurt her. The threats frightened Trudi so much that she fled the house and walked to town with the children to seek refuge. Just telling the story upsets Trudi so much that she is crying and shaking. Agnes seeks verbal consent to share information with a women's emergency housing service but Trudi is too upset to give explicit consent.

Agnes believes that safe accommodation is the first priority for Trudi and the children. Agnes' manager, Helen, agrees that, even though Trudi is too distressed to give explicit verbal consent, the fact that she has walked with her children to seek help and support and has said she wants to go to a refuge, implies that she has given consent to share information for this purpose.

Agnes proceeds with sharing information about Trudi and her children with the women's emergency housing service. Only the information necessary to make the referral and to secure a place in the service is disclosed.

In Trudi's file, Agnes notes that information was shared with implied rather than explicit consent, with the manager's approval, and notes the outcome of sharing the information.

It can be difficult to demonstrate that a victim has genuinely consented where a service provider relies on implied consent. The victim may not have heard, fully understood or had all the available information to make an informed decision.

Service providers may have difficulty distinguishing a victim's silence or inaction as an intention to give implied consent because of fear or trauma.

For this reason, and particularly in a domestic violence context, it is preferable to seek a victim's explicit consent.

12.4 Documenting consent

Consent can be obtained verbally or in writing. Where obtained verbally, service providers must make a written record of the information exchange and the verbal consent.

Any consent obtained from a victim must be stored on the victim's file.

Where the victim's consent is implied, it must be noted in the victim's records, with a record of a manager's approval to share information with implied rather than explicit consent and the outcome of sharing the information.

A consent form to record victim's verbal or written consent is located at Appendix 5. Service providers are encouraged to use the form, adapt it to their circumstances or use an existing internal consent form.

12.5 Victim does not consent

Where a referral is received from the Central Referral Point and/or a Local Coordination Point, and the victim does not consent to share information, no further information can be shared under the Protocol.

A service provider must still consider whether:

- the victim is at serious threat; in this case, refer to Chapter 13 Serious threat
- there are concerns for the safety, welfare or wellbeing of a child or young person; in this case, the service provider should take any actions as required by the *CYPCP Act*
- the victim still wishes to be referred to a support service; if the victim chooses not to consent to information being shared but still wishes to receive support services, a referral should be made that only includes information that the victim consents to being shared, for example, the victim's first name, date of birth and contact details. Alternatively, the victim may be provided with the service provider's contact details and choose which information they will disclose directly with the service provider.

Where no consent is given and the victim is not at serious threat, the service provider must advise the referring service provider that consent was refused.

For automatic referrals, any information provided by the referring service provider must be securely destroyed. This practice is subject to any other legal and record keeping requirements that service providers are required to follow. Refer to Chapter 14 Information management.

12.6 Victim withdraws consent

The victim may withdraw their consent at any time. The withdrawal of consent can occur verbally or in writing. Where obtained verbally, a written record of the withdrawal of consent must be made. Any withdrawal of consent by a victim must be stored on the victim's file.

Service providers should not destroy personal and health information about the victim and the perpetrator collected up to the time that the victim's consent is withdrawn.

Where a victim identified at serious threat withdraws consent, refer to Chapter 13 Serious threat.

13. Serious threat

The procedures in this chapter are supplementary for cases where there is a serious threat to the life, health or safety of a victim, any children or other persons. Where there is a conflict between the procedures outlined in this chapter and those outlined in the rest of the Protocol, the procedures outlined in this chapter take precedence for victims at serious threat.

While there are some situations where consent is not required for victims at serious threat, it is best practice to obtain their consent to share their information. Where possible, service providers must involve victims at every step of the process to ensure they have an understanding of, and confidence in, the process. Victims at serious threat will feel more reassured about their information being shared if they have been involved and where their consent has been sought.

For identification of a victim at serious threat, refer to Chapter 8 Threat identification.

13.1 Imminence

Before Part 13A, NSW privacy laws allowed information sharing without a person's consent only where a threat to a person's life, health or safety was *serious* and *imminent*. Part 13A changes this and allows information to be shared where a threat is serious. There is no requirement to show that the threat is also imminent

This change was made because, in domestic violence situations, a serious threat may exist but it might be hard to determine whether the threat is imminent. For example, in cases of long-term domestic violence where there have been repeated assaults, there may be no identifiable immediate threats to a victim's safety, but serious concerns about the victim's safety remain.

13.2 Consent

In the case of a serious threat to the life, health or safety of a victim, service providers must always try to obtain the victim's consent before sharing their personal and health information.

For example, service providers should inform the victim that there are serious threats to their life, health or safety, that of any children or other persons and advise the victim that only information necessary to prevent or lessen the serious threat will be shared, and the potential outcomes of sharing that information.

Sharing information without consent is allowed where:

- it is unreasonable or impractical to obtain consent from the victim, or
- the victim has refused consent.

In cases where a victim is at serious threat and children are victims or affected by domestic violence in the home, service providers that are prescribed bodies must take actions as required under the *CYPCP Act*, and also make a referral for the victim to the Central Referral Point and/or a Local Coordination Point. Refer to Chapter 5 Protocol and child protection legislation and the *Domestic Violence and Child Protection Guidelines*.

13.3 Unreasonable or impractical to gain consent

What is unreasonable or impractical is difficult to define, as it will vary depending on the circumstances of each situation. When deciding if something is unreasonable or impractical, service providers must consider what an ordinary person (not a professional) would expect or think would be acceptable in the situation.

Service providers must not determine that something is unreasonable or impractical simply because it is inconvenient.

Examples where unreasonable or impractical to gain consent:

- The victim is unconscious or in a coma.
- The victim has not answered their telephone despite repeated attempts to contact them each day over several days or a week.
- The victim cannot be contacted independently of the perpetrator and does not have regular appointments with a service.
- Where the need to provide support requires an urgent response and there is either no time or the victim cannot be contacted.
- Where there is a history of the perpetrator extracting information from the victim about what they have done and who they have talked to.

In assessing whether it is unreasonable or impractical to obtain consent, service providers must consider whether seeking the victim's consent may increase their level of threat. In some instances, telling a victim that information about them and the perpetrator will be shared can jeopardise the victim's safety. For example, in domestic violence situations it can be important for the victim's safety that the perpetrator remains unaware of impending interventions. If the perpetrator is aware, this may result in an escalation of violence.

Service providers must also consider the potential for placing the victim at increased risk of violence where the attempt to reduce or prevent the serious threat was not successful and the perpetrator becomes aware that the victim has reached out for support.

Case study: Impractical to obtain victim's consent

Emily is a disability support worker visiting Diane at home. Diane has a long history of hospital admissions for multiple sclerosis.

During home visits, Diane's partner, Craig, refuses to leave the room, stating that as her carer he needs to know what is happening. Emily has noted that Diane continuously looks at Craig before answering questions and that it is not uncommon for Craig to speak for Diane.

At a recent visit, Emily noted that Diane had large bruises on her arms, a black eye and a cut to her head. Diane said that she had fallen over in the dark and hit some furniture because she forgot to turn on the light.

Emily receives a phone call from Diane's sister, Sarah, stating that Craig often hits Diane and does not allow her to leave the house. Sarah reports that Diane's most recent admission to hospital for a broken arm was the result of an attack by Craig, but that Diane denied this to police and discharged herself from hospital.

Case study: Impractical to obtain victim's consent, cont.

Sarah says that if she visits Diane when Craig is out, Diane cannot let Sarah into the house because Craig locks the doors and Diane does not have keys. Sarah fears for Diane's life. She says that Diane has told her that Craig has started holding her head under water when angry. Sarah says that Diane wants to leave but is too scared because she thinks that Craig will find her.

At her next visit, when Diane is talking about aspects of her health, Sarah asks her if she would like help from a women's health service. Craig replies that Diane already has a doctor and that he takes her to appointments whenever necessary. Diane does not respond. Emily observes that Diane is very subdued and dishevelled and will not make eye contact.

Emily talks to her supervisor about Diane and that in her professional judgement, Diane is at serious threat of serious injury or death. Emily seeks permission to contact a women's domestic violence support service without seeking Diane's consent on the basis that it is unreasonable and impractical. The supervisor endorses Emily's request to contact the domestic violence service without seeking Diane's consent.

Emily makes a referral for Diane to the Central Referral Point, which refers the case to the Local Coordination Point. The Local Coordination Point lists Diane on the next Safety Action Meeting agenda.

For more information on Safety Action Meetings, refer to the Safety Action Meeting Manual.

13.4 Overriding a refusal to consent

Service providers and other agencies have an obligation to respect a victim's right to privacy. If a victim does not consent to having their information shared, the service provider must not share information about that victim.

An exception exists where a service provider reasonably believes that by sharing information, actions could be taken that are necessary to prevent or lessen a serious threat to the victim's life, health or safety, that of any children or other persons. Where those conditions are met, the service provider may override a victim's refusal to consent.

This is a difficult decision but the service provider must consider the impact to a person's safety if the information is not disclosed. Ultimately, the safety of the victim, any children or other persons is paramount and must always guide decision-making.

Case study: Overriding victim's refusal to consent

Evelyn lives with her boyfriend Wiremu a few kilometres out of a small country town in western NSW. They both used to work at the abattoir in the next town and travel to and from work together, but Evelyn stopped working about 3 months ago. Wiremu goes to the pub with his friends every Friday night and often brags that he has the perfect life: a girlfriend who does what she is told and never complains because she knows better.

People around town have noticed that they never see Evelyn anymore except when she and Wiremu come to town to do the shopping. He always drops her off at the supermarket and goes to the pub for a while.

On one of these occasions, the local Community Health worker, Carmen is also in the supermarket and notices that Evelyn is hunched over and appears to be in pain. She asks Evelyn to come by the health centre after she has finished shopping. Carmen also notices several large bruises on Evelyn's arms, neck and face. Evelyn hesitates for a second but then tells Carmen that she is fine.

A few days later Carmen drives to Evelyn's house knowing that Wiremu is at work. Evelyn does not invite her in and appears very scared. She has a black eye and a large cut on her cheek. Carmen asks Evelyn about her injuries, but she refuses to answer her questions. Carmen tries to engage her, suggests that Wiremu has been assaulting her, and tells her that she can make a referral for domestic violence support services.

Evelyn denies that Wiremu has assaulted her, refuses any assistance and tells Carmen that she must leave.

Carmen returns to the Community Health Centre and using professional judgement assesses that Evelyn is at serious threat and that actions are necessary to prevent or lessen the threat.

Although Evelyn has denied that Wiremu had assaulted her and has refused assistance for domestic violence support services, Carmen discusses the situation with her manager who approves Carmen to override Evelyn's refusal to consent.

Evelyn makes a referral to the Central Referral Point.

13.5 Sharing information without consent

Where a service provider believes a serious domestic violence threat exists and it is unreasonable or impractical to obtain the victim's consent or the victim's refusal to consent should be overridden, the service provider must:

- ensure that there is a valid threat assessment evidencing the victim is at serious threat; refer to Chapter 8 Threat identification, and
- believe, based on reasonable grounds, that the use or disclosure of personal and health information is:
  - necessary to prevent or lessen a serious threat to the victim's life, health or safety, that of any children or other persons, and
  - the serious threat relates to the commission or possible commission of a domestic violence offence.

On reasonable grounds

What is reasonable will vary depending on the circumstances of each situation. When deciding if something is reasonable, service providers must consider what an ordinary person (not a professional) would expect or think would be acceptable in the situation.

Necessary

Service providers must consider if there are any actions that can be taken to reduce or prevent the serious threat to the life, health or safety of a victim without sharing the victim's information. If the only way to reduce or prevent the serious threat is by sharing information, service providers should override the victim's refusal to consent and share the information necessary so that actions can be taken.

To prevent or lessen a serious threat

The use or disclosure of personal or health information must allow the service provider using or receiving it to take steps it would not otherwise be able to take to, either to remove the serious threat entirely, or to reduce it.

Service providers must also consider that not sharing the information of a victim identified as at serious threat because the victim has refused consent may preclude them from being referred to a Safety Action Meeting.

When making this assessment, service providers must consider whether sharing information would actually increase the threat to the victim or any other persons. If the threat cannot be prevented or lessened and, sharing information would actually increase the threat, then the information must not be shared.

If the attempt to prevent or lessen the threat by sharing information is unsuccessful, the use or disclosure of the information will not have contravened Part 13A or the Protocol as long as there was a reasonable belief that using or disclosing the information without consent was necessary to prevent or lessen the serious threat.

Case study: sharing information without consent

Rhye is a manager at a Community Mental Health Centre and has been informed by staff that Connor has stopped taking medication to treat paranoid schizophrenia. Connor has been a patient at the centre for 8 years and although he mostly complies with his medication and appointments, he has previously refused to comply with treatment and consequently had a severe paranoid episode, which resulted in him being physically restrained by a neighbour during an assault on his partner Tara. Rhye also knows from Connor's file that Connor has received a custodial sentence for a serious domestic violence assault on a previous partner.

Rhye reasonably believes that there are no actions that he can take that would reduce or prevent the serious threat to Tara's life, health or safety, other than by sharing Connor's information.

Rhye believes that to respond effectively to the serious threat posed by Connor refusing to take his medication and his history of paranoia and violence towards partners, it is necessary for him to share information with the Local Coordination Point without Connor's consent so that appropriate actions can be taken to prevent a domestic violence offence.

Commission or possible commission of a domestic violence offence

Information can only be shared without the consent of a victim at serious threat if the threat to the victim or other persons relates to an offence that the service provider believes on reasonable grounds is about to be committed or may be committed, and that offence is a domestic violence offence.

Refer to:
Section 11, Crimes (Domestic and Personal Violence) Act 2007.

A domestic violence offence means a personal violence offence committed by a perpetrator against a victim where they have or have had a domestic relationship. It can also refer to a crime that may be committed against another person because of that domestic relationship, such as against the victim's new partner, any children or other persons.

Questions to consider:

The following questions may assist service providers considering sharing information without the consent of a victim:

- Is there a serious threat to the life, health or safety of the victim, any children or other persons?
- Can the information be shared under Chapter 16A of the *CYPCP Act*?
- Has the serious threat been identified using the procedures outlined in *Chapter 8 Threat identification*?
- Does the threat relate to the commission or possible commission of a domestic violence offence?
- Is the sharing of information motivated by an intention to prevent or lessen the serious threat?
- Is the use or disclosure of personal or health information necessary to prevent or lessen the serious threat?
- Can the threat be prevented or lessened without disclosing personal or health information?
- If disclosed, can the recipient service provider take action to prevent or lessen the threat?

Where information cannot be shared under Chapter 16A and the service provider is still uncertain, they must consider the impact on the victim's safety if the information is not disclosed. Ultimately, it is preferable to disclose the information as the life, health or safety of victims, any children or other persons is paramount.

If there are child protection issues, the service provider must also comply with its child protection obligations, and complete the mandatory reporter guide if necessary. Child protection issues override any provisions relating to victim consent.

13.6 Informing victims

Where a decision is made to share information without the consent of the victim, it is important to inform the victim at the earliest opportunity. Where possible, inform the victim before the information is shared. The only exception is where it is determined that informing the victim may actually increase the serious threat.

Victims must be informed:

- that there are serious concerns for their life, health and/or safety, that of any children or other persons
- that information will be shared even without their consent
- of the service providers with which the information will be shared
- that only information that is necessary to prevent or lessen the serious threat will be shared, and advise what information will be shared
- the potential outcomes of sharing that information.

13.7 Record keeping

A service provider that has serious concerns for a victim's life, health or safety and makes a decision to share or not share their information must:

- make a written record which clearly articulates why a decision was made to share or not share information (referring to the serious threat and how the threat will or will not be prevented or reduced by the collection, use or disclosure of information)
- attach a copy of any threat assessment undertaken, to the written record
- keep both on the victim's file.

Where a decision is made to share information, the written record must include:

- if the victim was informed of the decision, a summary of what information was provided to the victim, or
- if the victim was not informed of the decision, a summary of the reasons why it was decided not to inform the victim.

If a victim's refusal of consent is overridden, the written record must include a summary of the reasons for the victim's refusal to consent, why it was necessary to share the information without the victim's consent and the outcome of any agency actions.

Case study: Documenting a decision to override victim's consent

Jim was previously on a community treatment order for a mental illness. The order provided for compulsory medication and attendance at a Mental Health specialist. The order has now lapsed and Jim attends a Community Health Centre. The Centre is aware of a history of serious domestic violence assaults by Jim against his wife Karen.

Jim reports to the doctor at the Centre that he has stopped taking his medication and is hearing voices. Karen is also present but appears withdrawn and subdued. The doctor considers that in his professional judgement, Karen is at serious threat, but there is nothing to suggest that the threat is imminent.

The doctor asks if he could speak to Karen alone. The doctor advises her that he has concerns that she may be at serious threat of domestic violence. He asks Karen if he could make a referral to a domestic violence support service for her. The doctor explains why he wants to share information and make the referral. Karen tells the doctor that it would only make matters worse and refuses to give her consent.

Despite Karen's refusal of consent, the doctor reasonably believes that sharing information about Karen and Jim to the Central Referral Point is necessary to prevent or lessen the serious threat to Karen's life, health or safety. The doctor assesses that there is no reasonable alternative way of preventing or lessening that serious threat.

The doctor overrides Karen's refusal to consent. He explains to Karen that he is doing this by making a referral to the Central Referral Point. The doctor tells Karen what information he will share and what she can expect.

The doctor then makes a referral to the Central Referral Point. The doctor also makes a written record of Karen's refusal to consent on the Client Consent Form and on the Central Referral Point referral.

The doctor then takes necessary steps to address Jim's immediate mental health issues and for a new psychiatric assessment.

14. Information management

Sharing information can save lives but it must be balanced with people's rights to privacy and confidentiality. This means that the information shared under the Protocol must be necessary for the provision of domestic violence support services to the victim, or to lessen or prevent a serious threat to the life, health and safety of a victim, any children or other persons.

This chapter outlines procedures governing what, how and when information can be shared. Service providers must ensure they have clear information management procedures in place for the collection, use, disclosure, storage and disposal of personal and health information that comply with the Protocol.

Refer to:
See *Responding to information requests or directions under Chapter 16A* and *Information Exchange: long fact sheet for human service workers*.

Where children are victims or are affected by domestic violence in the home, service providers who are prescribed bodies should take any actions as required under the *CYPCP Act* and share information under Chapter 16A of that Act. Where information is shared under Chapter 16A, the provisions for managing information under the *CYPCP Act* apply. For more information, refer to Chapter 5 Protocol and child protection legislation and the *Domestic Violence and the Child Protection System Guidelines*.

14.1 Information that can be shared

Each service provider is responsible for decisions about what information it considers reasonably necessary to share under the Protocol. As a guide, information shared may include, but is not limited to:

The Protocol takes precedence over section 19(1) of the *PPIP Act* relating to disclosure of an individual's ethnic or racial origin, where the disclosure is made under the Protocol. Another exception is where the individual has consented under section 26(2).

- name, date of birth, gender, address and contact details of the victim
- relationship to the perpetrator and whether the victim is living with the perpetrator
- whether the victim has or is thought to have any mental illness, disability or drug and alcohol issues
- injuries resulting from an act of violence
- Aboriginal or Torres Strait Islander background or another cultural background
- whether an interpreter, an Aboriginal or Torres Strait Islander identified person or disability support worker is required to make contact with the victim
- a safe method and time to contact the victim
- the perpetrator's name, date of birth, gender and address, whether the perpetrator has or is thought to have any mental illness, a disability or drug and alcohol issues, and any assessment made regarding the perpetrator's risk of re-offending
- the names of any children normally present in the victim's or perpetrator's home, their dates of birth, whether they are living with the victim, whether they have or are thought to have any mental illness, a disability or drug and alcohol issues

- whether any children have sustained any injuries resulting from an act of violence, and the risk of harm to any children as a result of domestic violence (the *CYPCP Act* applies in these circumstances. Refer to the Chapter 5 Protocol and child protection legislation and *Domestic Violence and Child Protection Guidelines)*.
- any recognised risk factors for domestic violence, including copies of any completed risk assessment tools
- support services currently of previously provided to the victim or the perpetrator, any actions taken in relation to threat factors and date of last contact.

Where there are domestic violence proceedings underway, information shared may also include:

- administrative details, including date of the domestic violence incident, court file number, court date, and conditions of any ADVO sought or in existence
- the grounds of any ADVO application
- any previous domestic violence incidents involving either the victim or the perpetrator (including where the victim was previously a perpetrator and the perpetrator a victim), whether the perpetrator has at any time breached an ADVO, community based order or bail; and whether the perpetrator is or at any time was in custody
- any police event number, the officer in charge and Local Area Command, nature of any charges, and conditions of any bail conditions sought or in existence.

14.2 Information management principles

Information sharing must be secure, timely, accurate and relevant.

Best practice

When information is shared it should be:

Secure

Timely

Accurate

Relevant

Secure

Personal and health information must be shared and stored securely.

Information may be shared verbally or in writing, but written information exchange is preferred. Referral forms, letters, e-mails and other forms of electronic communication may be used. Do not share personal and health information by facsimile, unless the fax machine is secure, the recipient can guarantee sole access and the fax number is confirmed prior to sending the information. Hard copies of documents must be marked 'confidential' and electronic copies must be password protected where possible. Make a written record of the information exchange and store on file.

Service providers should advise and add the following statement to all written communications with the receiving service provider:

- any inappropriate disclosure of the information has potential harmful consequences for the victim's safety

- the information is provided on the basis that the receiving service provider does not use it for any purposes other than those outlined in the referral/information request
- the receiving service provider must not disclose the information further without the victim's consent.

Information can be shared verbally over the telephone or in person. Verbal information exchange is more likely to occur when a victim is considered at serious threat and a more immediate response is required. A written record of the verbal exchange detailing the information shared must be noted on file. Do not leave personal or health information on voicemail.

Service providers should also refer to their internal policies and procedures related to management of confidential information.

Timely

Provide information in a timely manner to facilitate the provision of domestic violence support services at the earliest opportunity. This is particularly important in cases of serious threat, where information is shared to prevent or lessen a serious threat to the life, health or safety of a victim or other persons. Service providers sharing information must consider the level of threat to the victim and the urgency of the information request response and prioritise the information sharing process accordingly.

Accurate

Accuracy of information is vital. Each service provider is responsible for taking reasonable steps to ensure that the information it shares is up-to-date and accurate. It is good practice to check with the victim that the information is correct.

If a service provider discloses information that is not up-to-date, this must be declared and the receiving service provider must consider the limitations and usefulness of historic information. It is recommended that service providers add the following statement when sharing information:

- the information provided is accurate as at dd/mm/yy, this date being that of the last contact with <<service provide name>> that is providing the information.

A receiving service provider must advise the disclosing service provider if they are aware of inaccuracies in information shared with them.

Where the information is factual or first hand, it can be recorded as such and passed on as being factual. Where the information contains a personal or professional opinion or belief, then the identity of the person who held that opinion or belief – whether it is a victim, worker or other professional – should be included. This includes when a professional assessment is made about the victim.

Examples of how facts should be recorded:

- The hearing in this matter is set down for 12 March 2014.
- Jason was previously found guilty at Campbelltown Local Court of a domestic violence related assault on the victim that occurred on 24 September 2011.
- Chen [the victim] advised that Lok was no longer living in the family home.

NOT Lok is no longer living in the family home.

Examples of how opinion should be recorded:

- Bernadette was assessed by a psychiatrist on 12 November 2010 and the psychiatrist concluded that Bernadette has bipolar traits.

NOT The victim has bipolar.

- Linda [the victim] advised that she is scared of Steve's behaviour.

NOT Linda is scared of Steve.

- In his report, the social worker concluded that there is a serious threat that Akashi will harm Kiyomi and may even kill her.

NOT There is a serious threat that Akashi will harm Kiyomi and may even kill her.

Relevant

The information shared must be limited to what is needed to fulfil the purpose of sharing the information. The information must be proportionate to the purpose and not excessive or unnecessarily detailed. Each service provider is responsible for decisions about what information it considers reasonably necessary to share for the legitimate purposes set out in the Protocol.

Examples of relevant information shared:

- In one case, it may be important to list the schools attended by a victim's children because the perpetrator is stalking the victim when she picks the children up from school, but for another case, this information may not be relevant.
- A referral to emergency accommodation for a victim would not typically need to include a full disclosure of the victim's health information, unless her health issues need to be considered in determining an appropriate placement.

Service providers must not share more than is necessary to make a referral for the provision of support services or to prevent or lessen a serious threat. In cases of serious threat, however, the life, health or safety of victims is paramount and where a service provider is uncertain as to whether or not to disclose information additional to what is necessary to make the referral or to prevent or lessen the serious threat, it is preferable to err on the side of disclosure.

Service providers must have information management policies and procedures in place. Where there is a direct conflict between the Protocol and internal policies and procedures, the Protocol takes precedence.

14.3 Recording information shared

Where a service provider collects, uses or shares personal or health information about a victim or perpetrator for the purposes set out in the Protocol, service providers must make a record of the information exchange and place on the client's file:

- where the information is shared in writing, a copy of the information collected, used or disclosed, or
- where the information is shared verbally, a written record must be made that explains what information was collected, used or disclosed.

An exception is where an automatic referral is made by the NSW Police Force or a NSW Local Court, and the victim declines assistance and does not give consent to share their information. In this case, and if there is no serious threat, service providers must securely destroy any information collected from paper files or electronic databases.

This practice is subject to any other legal and record keeping requirements that service providers are required to follow.

14.4 Protecting stored information

Refer to:
PPIP Act IPP 12 and *HRIP Act HPP 5*.

Service providers are responsible for the protection of personal and health information, including client files and any other records containing personal or health information. Service providers must implement reasonable safeguards against loss or unauthorised access, use, modification or disclosure, and ensure that information is managed securely to avoid the risk of intentional or unintentional privacy breaches.

Service providers must conduct regular self-assessments of information security arrangements to ensure they are effective.

Some reasonable physical safeguards include:

- locking file cabinets and unattended storage areas
- securing the areas in which personal and health information is stored
- not storing information in public areas
- positioning computer terminals and fax machines so they cannot be seen or accessed by unauthorised people or members of the public
- not removing any client file from work premises without a compelling reason.

Some reasonable technological safeguards include:

- using individual password protection for computer access and databases (and regular changes to passwords)
- establishing information access levels for staff
- ensuring information is transferred securely
- using electronic audit trails
- installing virus protection software and firewalls

- not using portable storage devices such as CDs or flash drives to store and transport identifiable client information
- not storing client information on laptop computers.

Some reasonable administrative safeguards include:

- introducing appropriate policies and procedures to address information security and information confidentiality awareness
- training staff on those policies and procedures.

14.5 Retention of information

A medical practitioner or medical corporation must comply with the *Health Practitioner Regulation (New South Wales) 2010* and retain health records:

- where the most recent entry relates to a person when they were an adult, for seven years from the last occasion on which the person was provided with a service, or
- where the most recent entry relates to a person when they were under the age of 18 years, until the person has reached 25 years of age.

Refer to:
PPIP Act IPP 12 and *HRIP Act HPP 5*.
For NSW government agencies, see s.12 of the *State Records Act 1998*.

NSW government agencies must also comply with record retention and disposal policies under the *State Records Act 1998*.

Refer to:
Part 4 s.10 of the Health Practitioner Regulation (NSW) 2010.

Under NSW privacy guidelines, service providers must only keep information for as long as it is required for the purposes for which it was originally obtained. It is not a sufficient requirement under NSW privacy laws and the Protocol that service providers keep information because a person might have further contact with a service provider at a later stage.

Where service providers decide to destroy a victim's file, they may consider contacting the victim to see if they want to keep their file instead (ensuring that there is nothing in the file that might breach another person's privacy).

In some instances, clients may need records as evidence for future legal action, such as where a victim has experienced assault, or trauma, or a negative experience with the service provider.

When considering how long personal and health information should be kept, service providers must ensure they understand their obligations under NSW privacy laws, other NSW legislation that deals with retention and disposal of personal and health records, the Protocol, and their internal policies. Service providers may refer to their internal Records Management Unit, if available, for further guidance.

14.6 Destruction of information

Service providers must destroy or permanently de-identify personal and health information collected that is no longer required for its original purposes. This practice is subject to any other legal and record keeping requirements that service providers are required to follow.

Destruction of records must be irreversible. This means that there is no reasonable risk of recovering or restoring the information. Failure to ensure the total destruction of records may lead to the unauthorised release of information and potential breaches of NSW privacy laws.

Service providers must securely destroy hardcopy records such as paper files by shredding or using secure disposal facility. It is not enough to put files into recycling bins. Similarly, all digital records, stored in shared drives, databases or emails, must also be destroyed. Destruction of digital records is different to the destruction of hardcopy records. Pressing 'delete' does not necessarily mean that the records are completely gone; while the link used to access them may be removed, they may still exist in a data store or on a server. The destruction of records must be such that there is no reasonable risk of the information being recovered.

15. Privileges and subpoenas

This chapter provides assistance on how to respond to a subpoena and what potential privileges at law exist in respect of information.

15.1 Subpoenas

A court may issue a subpoena to a service provider to produce documents to assist the court in considering a matter before it. A subpoena may be sought by any party to a court proceeding (commonly through their legal representative) and is similar to a court order as it must be obeyed unless the court decides differently. The court proceedings may or may not relate to domestic violence. Compliance with a subpoena is required by law.

> If a service provider receives a subpoena to produce information about a victim or a perpetrator, that service provider must seek legal advice before producing any information. A subpoena may be challenged on a number of different grounds, including abuse of process, oppression and/or on the basis of a privilege at law over the information.

A service provider that has received, used or disclosed information may be subpoenaed to produce the information held. A subpoena may request that certain documents be produced to the court, such as case notes, files or any other records. Subpoenaed documents do not automatically become evidence in legal proceedings, but even if the documents are not used in evidence, the information obtained from them could potentially cause harm to a victim, particularly in domestic violence cases.

Where a victim's record has been subpoenaed and the victim is not a party to the proceeding, the service provider must notify the victim that the subpoena has been received.

15.2 Privileges at law

Privileges exist at law that create a right to keep communication between a person and a professional confidential. The professional may be a legal practitioner, social worker or sexual assault counsellor. The communication that is subject to the privilege may be either written or verbal. When a communication is protected by a privilege it may not need to be disclosed, even where that information is subpoenaed by the court for legal proceedings (either related or not related to domestic violence).

> Privileges belong to victims; so while file notes belong to the service providers, any subpoena must be discussed with the victim.

This means that service providers can potentially object and raise a privilege at law if they are subpoenaed to produce certain records about a victim. For service providers working with victims of domestic violence, it is critical to be aware of these privileges and how they apply to victims.

Although documents such as case notes or files belong to the service provider, any privilege belongs to the victim and so the subpoena must be discussed with them. If the victim consents to disclosure of the information, the information can be disclosed.

There are three privileges at law that service providers may potentially rely upon to keep information about the victim confidential:

- legal professional privilege
- sexual assault communications privilege
- professional confidential relationship privilege.

15.3 Legal professional privilege

> Refer to:
> The client legal privilege in Part 3.10, Division 1, s.117-126 of the *Evidence Act 1995*.

Legal professional privilege (known as client legal privilege under the *Evidence Act 1995* operates in the context of the lawyer-client relationship. It relates to communication between a client and their legal representative to provide the client with legal advice for legal proceedings.

The purpose behind this legal principle is to protect a person's ability to access the justice system by encouraging complete disclosure to legal representatives without fear that any disclosure of those communications may prejudice them in the future.

15.4 Sexual assault communications privilege

> Refer to:
> The Sexual Assault Communications Privilege in Part 3.10, Division 1, sections 126G – I of the *Evidence Act 1995* and in Part 5, Division 2, sections 295 to 306 of the *Criminal Procedure Act 1986*.

Sexual assault communications are communications made in the course of a confidential relationship between a victim of sexual assault and a counsellor.

Similar to the legal professional privilege, the sexual assault communications privilege provides an absolute prohibition against requiring the production of documents recording counselling communications in preliminary criminal proceedings. Once the main criminal proceedings have started, the privilege will also apply unless the court specifically grants leave and requires the documents be provided. Documents that are the subject of this privilege in any criminal proceedings continue to be privileged in subsequent civil proceedings.

A sexual assault privilege also applies in ADVO proceedings.

In NSW, an objection may be made to producing a protected confidence on the ground that it is privileged; but the victim of the sexual assault can consent to disclosure.

The purpose of this privilege is to give victims a confidential and safe place to talk about, or disclose, information about their traumatic experience, personal or sensitive issues and concerns. It includes counselling communications made by, to or about a victim.

The communications privilege will still apply if the communication is made in the presence of a third party, where the third party is present to facilitate the communication or to further the counselling process.

Case study: Disclosure where third party present

Amy attends therapy sessions with a counsellor at the local domestic violence support service for a sexual assault that occurred six months ago. A student on placement is also in the room, observing Amy's counselling session. The counsellor receives a subpoena from a court requesting access to her case notes. A claim of sexual assault communications privilege can be made by the counsellor on behalf of Amy even though there a was a third party in the counselling session.

Case study: Disclosure in support group

Trung attends a support group for sexual assault victims and discloses information to the group. The facilitator receives a subpoena from a court requesting she give evidence about information disclosed by Trung at the support group. A claim of sexual assault communications privilege can be made by the facilitator on behalf of Trung even though other participants were present at the support group.

For more information on sexual assault communications privilege, victims should be referred to the *Sexual Assault Communications Privilege Service*.

15.5 Professional confidential relationship privilege

Refer to:
Professional Confidential Relationship Privilege in Part 3.10, Division 1, s.126A – F of the *Evidence Act 1995*

The professional confidential relationship privilege is designed to protect communications from disclosure where those communications are made in the context of a professional-client relationship and the professional is acting under an obligation not to disclose the communications. This protection extends to a wide range of professions, including health professionals, counsellors, social workers and professionals in other relationships where confidentiality is essential to the continuation of the relationship.

Refer to:
See exclusion of evidence of protected confidences in Part 3.10, Division 1, s.126B of the *Evidence Act 1995.*

This privilege is distinct from legal professional privilege. There is no absolute protection where the professional confidential relationship privilege exists. It only gives the court discretion to direct that information not be presented where it would involve the disclosure of a protected confidence and it is likely that harm would, or might, be caused to the person who disclosed the confidence, and the nature and extent of that harm outweighs the desirability of having the information produced.

Case study: Professional confidential relationship privilege

Ben is seeing a social worker about his relationship with John who is controlling and abusive. He also has regular visits to the local health clinic for medical check-ups. The social worker and the medical clinic receive subpoenas from a court requesting access to Ben's files. A claim of professional confidential relationship privilege can be made by both the social worker and the medical clinic on behalf of Ben.

15.6 Privilege at law and information sharing

Any privilege at law belongs to the client and the privilege can only be waived by the client. A waiver can be express or implied. A privilege at law may also be waived or lost if there is conduct inconsistent with the maintenance of the privilege. This includes situations where confidentiality is not maintained, through the complete or partial sharing of information received or provided in confidence.

As a privilege may be waived, it is important that service providers understand and identify what information may be subject to a privilege before any decision is made to share information.

If a service provider makes an assessment that it is essential to share the information, then the service provider must discuss with the victim what the privilege means, why the service provider believes it is important to share that information and that sharing the information may mean that the privilege is lost. The victim must give informed consent before the information can be shared.

15.7 Information shared without consent

Where a service provider:

- makes an automatic referral,
- shares information where it is unreasonable or impractical to obtain the victim's consent, or
- overrides a victim's refusal to consent,

and shares information that would have been subject to a privilege at law, then the victim should not be considered to have waived their privilege in respect of that information, as they have not consented to that information being shared.

16. Access

This chapter outlines procedures in relation to requests to access victim, perpetrator or third party personal or health information held in service provider files or databases.

16.1 Victim access

> Refer to:
> A victim can apply to access personal information held by service providers under s.14 of the *PPIP Act*.
> A victim can apply to access health information held by service providers under HPP 7 of the *HRIP Act*.
> If the HRIP Act applies to a support agency, a victim may apply to access health information held by the support agency under Division 3 of Part 4 of the *HRIP Act*.

Under NSW privacy laws, a victim has the right to apply for access to their personal and health information held by a service provider. Where a service provider is subject to the *PPIP Act* and the *HRIP Act*, it must provide this information to a victim.

Where a service provider is not subject to the *PPIP Act* or the *HRIP Act*, it is strongly encouraged to provide this information to the victim. Only a manager, when satisfied of the victim's identity, can make the decision to provide this information.

Where a victim seeks to access their information held by a government agency, NSW privacy laws do not require the victim's request to be in writing. In contrast, where a victim seeks to access their information held by a non-government organisation, NSW privacy laws require the victim's request to be in writing, to state their name and address, and to identify the information they wish to access.

To ensure the security of victims' personal and health information and for compliance and management of obligations under NSW privacy laws, it is recommended that applications to any service provider for access to information always be made in writing with appropriate identification and verification processes.

Any release of information must be documented in the victim's file.

Belief victim being coerced by perpetrator

A service provider may receive a request for information from a victim and the service provider may form the belief that the victim is being coerced by the perpetrator to access the information.

The service provider must take all reasonable steps to ensure that the personal and health information of the perpetrator is not accidentally disclosed with the information of the victim. This involves reviewing the file and thoroughly redacting records to remove any information that relates to the perpetrator or any other person.

To ensure the safety of the victim and to comply with NSW privacy laws, service providers must also refer to their internal procedures on releasing client records before providing any personal and health information to a victim.

16.2 Access on behalf of victim

A person can provide consent for someone else to access health information on their behalf. This may include a relative, interpreter, medical practitioner or legal representative. It is important to check the scope of the authority provided, which must be in writing.

In addition, where a person lacks capacity to make a request about their health information, an authorised representative may make a request on the person's behalf.

Refer to:
Section 8 *HRIP Act*.

The *HRIP Act* sets out the list of people who can be an authorised representative:

- someone who has an enduring power of attorney for the victim
- a guardian within the meaning of the *Guardianship Act 1987*, or a person responsible within the meaning of Part 5 of that Act who has been allocated a specific function to provide consent to medical or support services
- any other person who is authorised by law to act for or represent the victim.

Before allowing an authorised representative or other person to access health information on behalf of a victim, the service provider must take reasonable steps to ensure that the authorised representative or other person is not the perpetrator or acting on behalf of the perpetrator.

It is recommended that service providers contact the victim to seek confirmation that they have given consent for another person to obtain information on their behalf.

The service provider must take all reasonable steps to ensure that the personal and health information of the perpetrator is not accidentally disclosed with the victim's information. This involves reviewing the file and thoroughly redacting records to remove any information that relates to the perpetrator.

16.3 Perpetrator access

Refer to:
Section 98I of Part 13A exempts service providers from providing access to information obtained under Part 13A to a perpetrator, even where the perpetrator makes an application under s.14 of the *PPIP Act*, HPP 7 of the *HRIP Act*, Division 3 of Part 4 of the *HRIP Act*. This is consistent with s.98K of Part 13A.

As a general rule, a victim's personal and health information must never be disclosed to a perpetrator or any other person acting on behalf of the perpetrator, such as the perpetrator's legal representative. Part 13A and the Protocol seek to ensure that the victim's safety is not compromised by individuals' right to access their information under NSW privacy laws. For this reason, Part 13A and the Protocol override the *PPIP Act* and the *HRIP Act* in relation to perpetrators' access to their information.

Service providers are not required to take any steps to make a perpetrator aware that information is held about them, or to provide a perpetrator with access to that information where that information was received under Part 13A and the Protocol.

Where a perpetrator contacts a service provider and requests to access their information, the service provider must inform a line manager, if available, to speak with the perpetrator. The manager is not required to inform the perpetrator that information is held about them.

There may be situations where it is necessary to disclose information where a subpoena is issued; but there are also privileges at law held by the victim. Before disclosing any information in response to a subpoena, service providers should check if a privilege exists. Refer to Chapter 15 Privileges and subpoenas.

16.4 Third party access

> Refer to:
> Where an application is received from a third party under s.14 of the *PPIP Act*, HPP 7 of the *HRIP Act*, or Division 3 of Part 4 of the *HRIP Act*, an agency or organisation should only disclose specific information relating to the third party themselves, deleting any references to the victim or any other party.

A third party that may be referred to or named in information held by a service provider has the right to apply for access to that information under NSW privacy laws. Where a service provider is subject to the *PPIP Act* and the *HRIP Act*, it is required to provide this information to the third party.

Where an organisation is not subject to the *PPIP Act* and the *HRIP Act*, it is encouraged to provide the information to a third party. The decision must be made by a manager, who must be satisfied of the third party's identity and that they are the person to whom the information relates.

Where a third party seeks to access their information held by a government agency, NSW privacy laws do not require the third party's request to be in writing. In contrast, where a third party seeks to access their information held by a non-government organisation, NSW privacy laws require the third party's request to be in writing, to state their name and address, and to identify the information they wish to access.

To ensure the security of the third party health and personal information and for compliance and management of obligations under NSW privacy laws, it is recommended that applications to any service provider for access to information always be made in writing with appropriate identification and verification processes.

When providing this information, the personal or health information of others, including the victim, perpetrator and any other party, must not be disclosed to the third party. Care must be taken to ensure the information of the third party only is disclosed and all other information, particularly information about others, is deleted from the information provided.

Any release of information must be documented in the victim's file.

Where a third party is unsatisfied with a decision not to provide them with access to their health or personal information, the third party may seek a review of the decision. Refer to Chapter 19 Complaints.

16.5 Public access under GIPA

> Refer to:
> The *Government Information (Public Access) Act 2009* replaced the *Freedom of Information Act 1989*.

The *Government Information (Public Access) Act 2009 (GIPA Act)* governs public access to government information in NSW. The objective of the *GIPA Act* is to make government information more accessible to the public by requiring government agencies to make certain information freely available.

The *GIPA Act* places a legislative onus in favour of the release of government information through consideration of the public's best interest. The *GIPA Act* should not affect how information is shared under Part 13A and the Protocol, as it is in the public interest to protect victims of domestic violence.

A government agency that has received a request for release of information under the *GIPA Act* must apply the public interest test to determine whether there is an overriding public interest against disclosure of information.

Applying the public interest test

The public interest test involves 3 steps:

1. Identify the relevant public interest considerations in favour of disclosure,
2. Identify the relevant public interest against disclosure, and
3. Assess whether the public interest against disclosure outweighs the public interest in favour of disclosure.

Public interest against releasing information

There are only limited and specific interests against disclosure that a service provider can take into account. These are:

- law enforcement and security
- individual rights, judicial processes and natural justice
- responsible and effective government
- business interests of agencies and other persons
- environment, culture, economy and other matters
- secrecy and exemption provisions in other laws.

Examples of situations in which these interests arise include where disclosure of particular information may:

- prejudice relations with, or the obtaining of confidential information from, another government
- prejudice the effective exercise by an agency of their functions
- found an action against an agency for breach of confidence or otherwise result in the disclosure of information provided to it in confidence
- prejudice the prevention, detection or investigation of a contravention or possible contravention of the law, or prejudice the enforcement of the law
- endanger, or prejudice any system or procedure for protecting, the life, health or safety of any person
- reveal an individual's personal information
- contravene an information protection principle under the *PPIP Act* or a Health Privacy Principle under the *HRIP Act*
- expose a person to a risk of harm or of serious harassment or serious intimidation
- in the case of the disclosure of personal information about a child, the disclosure of information that it would not be in the best interests of the child to have disclosed.

16.6 Granting access

When the service provider is satisfied that the person making the application for access is the person to whom the information relates, and they have consulted their internal procedures on releasing client records, they can provide access in a number of different ways. This may include:

- providing the person with a copy of the information
- providing a reasonable opportunity for the person to inspect the information, take notes on its contents and talk through the contents with an appropriate staff member, if required

- allowing the person to listen to or view the contents of an audio or visual recording
- giving the person a printout of the information if it is stored electronically, or giving them an electronic copy of the information.

When granting access in person for the information, service providers must ensure only the person to whom the information relates is given access.

For non-government organisations, if a person requests access in a particular form, then this request should generally be approved. A request should only be refused if it would:

- place unreasonable demands on organisational resources
- be detrimental to the preservation of the information.

In these cases, the information requested should be provided in another convenient form.

It is the responsibility of service providers to allocate persons within their agency with appropriate delegation to supervise how access is provided. This person must be adequately informed about their privacy and other obligations under the Protocol.

17. Amendment

This chapter outlines procedures in relation to requests to amend victim or perpetrator personal or health information held in service provider files or databases.

17.1 Victim request

A victim should be provided with details of the service provider that will receive their information before their information is shared. If the victim is aware that inaccurate information has been shared, the victim may at any time contact either the referring or the receiving service provider to correct that information. Alternatively, the victim may amend the information when the service provider contacts them or at any time during their interaction with a service provider.

Where a victim seeks to amend their personal or health information held by a government agency, NSW privacy laws do not require the victim's request to be in writing. In contrast, where a victim seeks to amend their health information held by a non-government organisation, NSW privacy laws require the victim's request to be in writing, to state their name and address, and to identify the information they wish to amend.

To ensure the security of the victim's personal and health information and for compliance and management of obligations under NSW privacy laws, it is recommended that requests to amend information always be in writing with appropriate identification and verification processes.

Where a victim notifies a service provider that they wish to amend their information, the service provider must keep a written record of the victim's request.

Amendments must be made by way of additional notes, but the incorrect information must be retained on file so that a trail of the information history can be kept. The service provider should also contact any other service provider it has shared that information with to advise of the amendments.

17.2 Refusing victim request

A service provider may refuse to amend a victim's information if it is satisfied that:

- the information is complete, correct, relevant, current and accurate
- the request to amend information contains information that is incorrect or misleading.

Where a service provider refuses to amend the victim's information as requested, it should:

- provide the victim with a written reason for the refusal, and
- keep a written record of the victim's request to amend information on file together with the written reason for the refusal.

Where a victim is unsatisfied with the service provider's response not to amend the information, they may seek a review of the decision. Refer to Chapter 19 Complaints.

17.3 Request on behalf of the victim

A victim may consent for someone else to seek amendment of their health information on their behalf. This includes a relative, interpreter, medical practitioner or legal representative. It is important to check the scope of the authority provided, which must be in writing.

In addition, where a victim lacks capacity to make a request to amend their health information, an authorised representative may make a request on the victim's behalf.

Refer to:
Section 8 *HRIP Act*.

The *HRIP Act* sets out the list of people who can be an authorised representative:

- someone who has an enduring power of attorney for the victim,
- a guardian within the meaning of the *Guardianship Act 1987*, or a person responsible within the meaning of Part 5 of that Act who has been allocated a specific function to provide consent to medical or support services, or
- any other person who is authorised by law to act for or represent the victim.

It is recommended that service providers contact the victim to seek confirmation that they have given consent for another person to amend information on their behalf.

Before allowing an authorised representative or other person to amend health information on behalf of a victim, the service provider must take reasonable steps to ensure that the authorised representative or other person is not the perpetrator or acting on behalf of the perpetrator.

17.4 Perpetrator request

Under Part 13A and the Protocol, a perpetrator does not have an automatic right to request amendment of their personal or health information that has been obtained under Part 13A.

Where domestic violence proceedings are dismissed, withdrawn or not proven, the service provider should note the outcome against the perpetrator on the victim's file. It is the decision of the service provider whether the perpetrator is given the opportunity to amend any information relating to them in these circumstances.

Where a perpetrator seeks to amend their information held by a government agency, NSW privacy laws do not require the perpetrator's request to be in writing. In contrast, where a perpetrator seeks to amend their health information held by a non-government organisation, NSW privacy laws require the perpetrator's request to be in writing, to state their name and address, and to identify the information they wish to amend.

To ensure the security of the victim's personal and health information, for compliance and management of obligations under NSW privacy laws, it is recommended that applications to any service provider for amendment to information always be in writing with appropriate identification and verification processes.

Where a perpetrator notifies a service provider that they wish to amend their personal or health information, the service provider must keep a written record of the perpetrator's request.

Where the service provider agrees to amend a perpetrator's information, amendments must be made by way of additional notes, and the incorrect information must be retained on file so that a trail of the information history can be kept. The service provider should also contact any other organisation with which it has shared that information to advise of the amendments.

17.5 Refusing perpetrator request

Under Part 13A and the Protocol, a perpetrator does not have an automatic right to request amendment of their personal or health information that has been obtained under Part 13A.

Where a service provider refuses to amend a perpetrator's information as requested, it should:

- provide the perpetrator with a written reason for the refusal, and
- keep a written record of the perpetrator's request to amend information on file together with the written reason for the refusal.

18. Compliance

Service providers should be committed to upholding people's rights to privacy and confidentiality and comply with information sharing under Part 13A and the Protocol. To promote best practice and to limit intentional or unintentional behaviour that contravenes people's rights and may expose victims to increased threats, the Protocol outlines a compliance-monitoring framework.

This chapter sets out the obligations of service providers regarding compliance with the Protocol to ensure they understand the limits of information sharing and their responsibilities under Part 13A.

Service providers must complete the Compliance Checklist and demonstrate a state of readiness before commencing sharing the victim or perpetrator's information under the Protocol. The Compliance Checklist is located at Appendix 4.

18.1 Compliance responsibilities

All service providers that collect, hold or share information under the Protocol are expected to monitor their own compliance with the Protocol and to develop systems to support continuous quality control of their internal information sharing processes.

Service providers are expected to:

- adopt NSW privacy laws about personal and health information about victims and perpetrators of domestic violence
- require any organisations they fund to comply with NSW privacy laws
- implement organisational, administrative and security measures to ensure the lawful collection, use, disclosure and disposal of information shared under the Protocol
- promote staff awareness of the requirements of the Protocol
- independently monitor and evaluate compliance with the Protocol
- implement clear procedures for dealing with complaints under the Protocol
- address any failure by staff to follow the Protocol through internal disciplinary procedures
- agree to participate in the compliance monitoring process and to comply with remedial directions as necessary.

18.2 Compliance-monitoring framework

The compliance-monitoring framework consists of:

- self-assessments, using the Compliance Checklist on a regular basis, including before accepting referrals or sharing information under the Protocol, to demonstrate compliance
- desktop reviews using the Compliance Checklists and other evidence as required
- formal audits, which include a more rigorous compliance checks.

Service providers are responsible for implementing the compliance-monitoring framework in their workplace and foster a culture of voluntary compliance and self-monitoring.

NSW government agencies are responsible for monitoring compliance in their own agencies and in any service provider they fund.

The NSW Department of Justice will conduct ad hoc desktop reviews or formal audits of service providers periodically or if triggered by a complaint.

The NSW Privacy Commissioner may also monitor service providers' compliance on an ad hoc basis or if triggered by a complaint.

18.3 Compliance Checklist

The Compliance Checklist is a standard performance monitoring tool for service providers to use to assess their compliance with the Protocol. It sets out broad criteria against which a service provider's compliance is measured, such as:

- victim consent; for example, seeking consent, documenting consent or overriding consent
- information provided to victims; for example on consent or threat assessment, access to and amending information, complaint procedures)
- conflict of interest; for example, identifying, managing, documenting
- information management; for example, procedures for collection, storage, sharing and disposal of personal and health information
- staff; for example, induction, training, reporting and management of breaches of information sharing
- management of complaints.

The Compliance Checklist provides a rating of the service provider's compliance with the Protocol to promote best practice, to remedy issues of non-compliance and to ensure future compliance. A service provider can found to be:

- compliant
- partially compliant
- non-compliant.

The Compliance Checklist is located at Appendix 4.

18.4 Self-assessments

Self-assessments using the Compliance Checklist aim to build service providers' compliance capacity rather that set penalties for failure to comply with the Protocol.

Before sharing information under the Protocol, service providers must undertake a self-assessment to demonstrate a state of readiness. They are then expected to conduct annual self-assessments to demonstrate ongoing compliance.

The completed Compliance Checklist must be dated and signed by a manager and maintained on a secure compliance file.

18.5 State of readiness

To demonstrate a state of readiness to share information under Part 13A and the Protocol, a service provider must:

- complete a self-assessment using the Compliance Checklist,
- meet the threshold of compliance for a state of readiness on the Checklist, and
- provide a copy of their completed Compliance Checklist to their funding body.

The compliance threshold for a state of readiness is set by the NSW Department of Justice and is outlined in the Compliance Checklist located at Appendix 4.

Some service providers may not have adequate technical and administrative measures in place to ensure secure information sharing and information management procedures. These service providers may be required to take additional steps such as:

- reviewing processes to ensure that paper and electronic methods used to collect and share personal or health information are secure
- reviewing processes to identify and manage conflicts of interest
- implementing security measures to protect personal and health information, with different levels of security depending on the sensitivity of the information; refer to Chapter 14 Information management
- training staff or issuing circulars to ensure staff are aware of their obligations under the Protocol.

18.6 Cannot demonstrate a state of readiness

If a service provider cannot meet the threshold for a state of readiness, it should highlight relevant barriers or issues with its funding body if applicable. The funding body may provide assistance as part of its performance management and support.

Until such time as a service provider has demonstrated a state of readiness, it must not receive information under the Protocol. Instead, the service provider may receive information under NSW privacy laws or, if there are concerns for the safety, welfare or wellbeing of children, and the service provider is a prescribed body, under Chapter 16A of the *CYPCP Act*.

18.7 Desktop reviews

A desktop review is a mechanism to encourage agencies to monitor their compliance with the Protocol, and the compliance of any service providers they fund. Desktop reviews provide an opportunity for agencies to provide corrective feedback and to identify and overcome any systemic barriers in information sharing processes. Desktop reviews must be undertaken on an ad hoc basis.

The Compliance Checklist forms part of a desktop review. Services providers must submit completed, dated and signed checklists to their funding body (if applicable) when requested and must also submit the Compliance Checklist to the funding body when a self-assessment rating falls below full compliance.

The funding body must review the completed checklist and any other evidence as required during desktop reviews. Findings from the desktop reviews, in particular systemic issues, will contribute to strengthening or amending sections of the Protocol to ensure they serve their intended purpose.

18.8 Formal audits

Formal audits involve a more rigorous enquiry to ensure compliance with the Protocol. They are conducted by the funding bodies:

- annually, on a selection of their funded service providers
- on an ad hoc basis, when triggered by a complaint, advice or notification
- where there are significant changes in a service provider's structure or business operations.

The NSW Department of Justice also conducts formal audits on an ad hoc basis, on:

- a selection of service providers that are not funded by a NSW government agency
- any service provider, government or non-government, to ensure general compliance with Part 13A and the Protocol.

The funding body may conduct a formal audit with a service provider even where its self-assessments indicate full compliance.

If a formal audit is initiated, the funding body must provide the service provider:

- written advice at least 10 working days prior to commencing the audit
- the terms of reference for the audit if its scope is wider than that of the Compliance Checklist
- any instructions about the service provider's obligations during the audit.

The funding body must provide a copy of any report arising from the audit to the service provider and give the service provider an opportunity to respond.

18.9 Partial or non-compliance and breach

Non-compliance is where there is evidence that a service provider is not complying with the Protocol or where a service provider does not have sufficient processes in place to ensure compliance with the Protocol.

Partial compliance is where a service provider has most, but not all, of the necessary processes in place to ensure compliance with the Protocol.

A service provider may be identified as partially compliant or non-compliant during the conduct of monitoring activities, including a self-assessment, desktop review or formal audit, or because of a complaint.

An information sharing breach is where a service provider undertakes activities that, either knowingly or through negligence, contravene the provisions of the Protocol.

Where a service provider becomes aware of a breach or partial or non-compliance with Part 13A or the Protocol, it must notify its funding body (where applicable) and the NSW Department of Justice immediately.

The funding body and/or the NSW Department of Justice may undertake any of the following actions:

- request previously completed self-assessment reports from the service provider
- conduct a desktop review of the documentation and, if required, request the service provider to complete a new self-assessment
- conduct a formal audit including, if required, an on-site review that may involve a review of the service provider's records and policies

- advise the service provider that information sharing under the Protocol must cease until further notice
- advise the victim if required
- notify the NSW Privacy Commissioner
- keep the NSW Privacy Commissioner informed of the progress of the internal review
- consider any relevant material submitted by the applicant or by the NSW Privacy Commissioner
- meet with the service provider to discuss the issue
- prepare a compliance review report
- develop an agreed compliance improvement plan with the service provider
- monitor the compliance improvement plan until full compliance is achieved
- recommend suspension of funding or defunding of the service provider.

The actions undertaken by the funding body and/or the NSW Department of Justice will be determined by the level of the breach, or the partial or non-compliance.

Where a breach has occurred, the investigation should consider whether the breach is due to systemic concerns, such as unclear internal procedures that suggest a need for further staff training or a review of policies and procedures.

If there are clear internal processes in place, the investigation should consider whether the breach is due to staff behaviour, in which case the matter must be dealt with through internal disciplinary procedures.

18.10 Informing a person of a breach

The decision to inform a person of a breach of their privacy through the unauthorised or negligent sharing of their personal and/or health information will depend on the nature and level of the breach.

Not all breaches will result in the same level of threat or infringement of a person's privacy. For example, in relation to a victim, a breach about information storage may not create the same level of threat as sharing personal and health information without their consent in a manner inconsistent with the Protocol.

A service provider who identifies a breach that could increase the level of threat to the victim must inform the victim as soon practicable and take any steps necessary to reduce the level of threat.

18.11 Information subject to a breach

Until a complete assessment of the extent of a breach is completed, service providers must take necessary precautions in relation to information that is the subject of a breach, particularly to ensure there is no added threat to the safety of the victim or other persons.

The service provider must immediately take steps to remedy the causes of the breach and, in some cases, limits may be placed on any further sharing of that information under Part 13A and the Protocol until the matter is resolved.

Where the funding body or the NSW Department of Justice has placed limits or stopped information sharing under Part 13A and the Protocol, the service provider must not share information under Part 13A and the Protocol until further notice.

18.12 Compliance record keeping

Service providers must maintain accurate and up-to-date records of compliance activities. Record keeping includes securely storing:

- completed Compliance Checklists
- completed desktop reviews
- completed formal audits
- any records about partial or non-compliance, complaints or breaches, and any steps taken to resolve them
- any notifications to funding bodies or the NSW Privacy Commissioner.

Records must be stored and managed as per the information management provisions under the Protocol. Refer to Chapter 14 Information management.

Additionally, service providers should comply with their internal information management policy requirements.

19. Complaints

This chapter outlines processes to deal with complaints that may arise from information sharing under the Protocol. Complaint procedures have different requirements depending on whether a service provider is a government agency or a non-government organisation, and whether they are bound by NSW or other privacy laws. The following sections outline these procedures.

In the first instance, the person should be encouraged to make the complaint directly to the service provider concerned. Service providers must have procedures to deal with a complaint and make these available to the person.

19.1 NSW government agency

Where an agency receives a complaint about a breach of privacy, it must conduct an internal review to examine whether Part 13A or the Protocol have been breached and consider the *PPIP Act* or the *HRIP Act*, as applicable. The agency must assess whether or not it has complied with privacy obligations and inform the person who made the complaint of its findings and what it will do as a result.

If the internal review is not completed within 60 days or the person is unhappy with the conduct or result of the internal review, they can ask the NSW Civil and Administrative Tribunal to review the conduct or the decision.

The NSW Civil and Administrative Tribunal reviews conduct by a government agency where there is an allegation that a government agency has not complied with privacy principles under the *PPIP Act* or the *HRIP Act*.

For any review of the conduct or decision by the government agency or NSW Privacy Commissioner, the NSW Civil and Administrative Tribunal can make legally binding orders, including ordering an agency to correct its conduct or pay compensation.

Alternatively, the person can make a complaint directly to the NSW Privacy Commissioner. The NSW Privacy Commissioner will consider whether they have jurisdiction to investigate the complaint. Where the NSW Privacy Commissioner determines they have jurisdiction to investigate, the Commissioner may attempt to resolve the complaint by conciliation and make a written report containing findings and/or recommendations. The Commissioner cannot make binding orders or pay compensation, and there is no right of review of the Commissioner's conduct or decision.

Internal review

An internal review is an internal investigation conducted by a government agency into a complaint. The agency must assess compliance with privacy obligations and in doing so, take into account Part 13A and the Protocol.

When a government agency conducts an internal review, it is required by law to:

- notify the NSW Privacy Commissioner that they have received an application for an internal review
- keep the NSW Privacy Commissioner informed of the progress of the internal review
- consider any relevant material submitted by the applicant or by the NSW Privacy Commissioner

- complete the internal review as soon as possible and no later than 60 days from receipt of the complaint
- once the review is finished, notify the applicant and the NSW Privacy Commissioner of the findings of the review (and the reasons for those findings), and the action proposed to be taken
- notify the applicant of their right to have those findings, and the agency's proposed action, reviewed by the NSW Civil and Administrative Tribunal.

Following an internal review, the agency may:

- take no further action
- apologise to the person
- take remedial action including paying compensation
- undertake that the conduct will not occur again
- take action to ensure that the conduct does not occur again.

19.2 Non-government service providers that comply with NSW privacy laws

Where a non-government service provider receives a complaint about a breach of privacy, it must assess whether or not it has complied with privacy obligations, and tell the person who made the complaint of its findings and what it will do as a result.

If the handling of the complaint is not completed within a reasonable time or the person is unhappy with the conduct or result of the process, and the non-government service provider is funded by a NSW government agency, the person can ask the funding agency to undertake a review of the complaint. If the funding agency does not undertake a review of the complaint, the person can ask the NSW Department of Justice to undertake a review.

Alternatively, the person can make a complaint directly to the NSW Privacy Commissioner. The NSW Privacy Commissioner will consider whether they have jurisdiction to investigate the complaint. If the NSW Privacy Commissioner determines they have jurisdiction to investigate, the Commissioner may attempt to resolve the complaint by conciliation and make a written report containing findings and/or recommendations. The Commissioner cannot make binding orders or pay compensation, and there is no right of review of the Commissioner's conduct or decision.

19.3 Non-government service providers that comply with Commonwealth privacy laws

Non-government service providers that are subject to Commonwealth privacy laws must continue to meet their obligations under those privacy laws when sharing information, as Part 13A and the Protocol do not create exceptions to Commonwealth privacy laws.

Any complaint to a service provider about a breach of privacy must be made under Commonwealth laws. The service provider must assess whether or not it has complied with its privacy obligations under Commonwealth privacy laws and tell the person who made the complaint of its findings and what it will do as a result.

If the handling of the complaint is not completed within reasonable time or the person is unhappy with the conduct or result of the process, the person can make a complaint to the Office of the Australian

Information Commissioner (OAIC). The OAIC is a federal independent body that deals complaints about non-government organisations subject to Commonwealth privacy laws or acting under a contract to comply with Commonwealth privacy laws.

If the person is not satisfied with a decision the OAIC has made, they can ask the OAIC to review the decision. An officer not previously involved with the complaint will generally investigate this request.

An application can also be made for a review of the decision or the determination by the Federal Court of Australia or the Federal Magistrates Court. This application can be made under the *Administrative Decisions (Judicial Review) Act 1977*, if the person believes:

- a decision by the OAIC not to investigate, or not to further investigate, the complaint under the *Privacy Act 1988* is not legally correct, or
- a determination by the Australian Information Commissioner following the investigation of the complaint is not legally correct.

19.4 Non-government service providers that do not comply with privacy laws

Service providers must not exchange information under Part 13A and the Protocol with service providers that do not comply with privacy laws that impose substantially similar privacy obligations as NSW privacy laws.

Where a person wishes to make a complaint about a non-government support service that is under no obligation to comply with any privacy laws, they should make a complaint directly to that organisation.

In addition, the person may inform the NSW Department of Justice to undertake a separate review of the complaint. The NSW Department of Justice will undertake a review and tell the person who made the complaint of its findings.

Refer to:
For information on making a complaint to the NSW Privacy Commissioner, see the *Information and Privacy Commission's Protocol* for handling privacy complaints at http://www.ipc.nsw.gov.au/privacy/ipc_index.html and the *PPIP Act* Part 5.

Alternatively, the person can make a complaint directly to the NSW Privacy Commissioner. The NSW Privacy Commissioner will consider whether they have jurisdiction to investigate the complaint. If the NSW Privacy Commissioner determines they have jurisdiction to investigate, then the Commissioner may attempt to resolve the complaint by conciliation and make a written report containing findings or recommendations. The Commissioner cannot make binding orders or pay compensation, and there is no right of review of the Commissioner's conduct or decision.

19.5 Complaint under Charter of Victims Rights

Refer to:
Charter Right 8 – Protection of identity of victim.

If a person, including the perpetrator, wishes to make a complaint about the sharing of their personal and health information by a NSW government agency under the Protocol, they can also make a complaint under the *Charter of Victims Rights*.

The person should first make the complaint directly to the NSW government agency concerned. If the person is not satisfied or is concerned about making a complaint to the NSW government agency, they can contact Victims Services at the NSW Department of Justice. Victims Services will assist the person with the complaint.

19.6 Disclosure of information to investigate complaints

In the case of a complaint made under the Protocol, it may be necessary to disclose personal or health information of the complainant to investigate or report on the conduct that lead to the complaint. Such information may be shared with the service provider's funding body, the NSW Privacy Commissioner, the NSW Department of Justice or an appeal tribunal. These agencies are subject to NSW privacy laws when handling that confidential information, and only information that is reasonably necessary to properly investigate or report on the conduct should be provided.

19.7 Complaints Register

The NSW Department of Justice maintains a confidential register of all complaints made about information sharing under Part 13A and/or the Protocol. The information will be analysed to identify any systemic issues and resolve any problems, and may be used for monitoring and reporting purposes. For this reason, service providers are required to provide a summary of all complaints received in relation to information sharing under the Protocol. The information must include:

- date of the complaint
- de-identified information about the complainant (for example, gender, post code, victim or perpetrator)
- the nature of the complaint and specific details
- what action was taken to resolve the complaint
- what action has been taken by the service provider to ensure the conduct does not happen again
- details of any ongoing monitoring arrangements
- the time taken to resolve the complaint.

The information must be provided to the NSW Department of Justice within one month of the resolution of the complaint.

20. Review of the Protocol

The Department of Justice will review this Protocol following evaluation of Safer Pathway and at regular intervals thereafter.

Service providers may provide feedback at any time about the Protocol by writing to the NSW Department of Justice. The Department will consider the feedback as part of the ongoing review process and the formal evaluation.

Appendices

The appendices include practical guides, decision flowcharts and templates to assist service providers share information in accordance with Part 13A and the Protocol.

The appendices consist of:

Safer Pathway service delivery map

Brings together the key elements of *It Stops Here: Safer Pathway* (Safer Pathway) and illustrates how victims are supported in a seamless service system response.

Information sharing process flowchart

Outlines how and when service providers can share information.

Information sharing consent flowchart

Outlines when service providers must seek victims' consent to share information.

Information sharing compliance checklist

A performance monitoring tool to assist service providers assess their state of readiness to share information under Part 13A and to comply with the Protocol.

Information sharing consent form

A template for service providers to use when seeking victims' consent to share information under the Protocol. Service providers may use this form, adapt it to their circumstances or use their own internal consent form.

Your information and your safety fact sheet

Service providers are encouraged to give victims a copy of this fact sheet that explains the key elements of information sharing under the Protocol.

Memorandum of understanding template

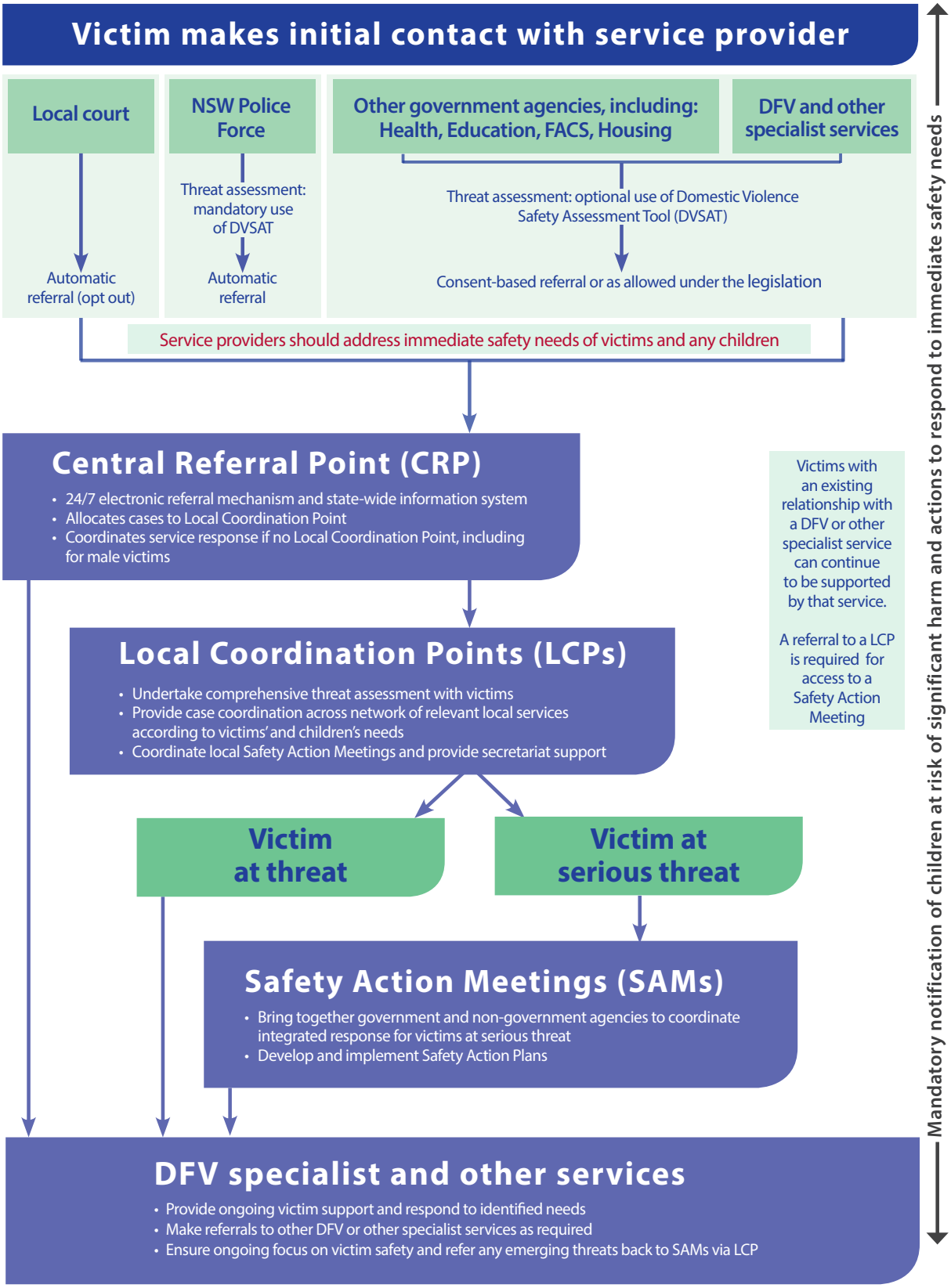
For service providers to adopt where they agree to share information under Part 13A and the Protocol.

1 NSW Police Force and NSW Local Courts refer to the Consent Flow Chart.

Appendix 1

Safer Pathway service delivery map

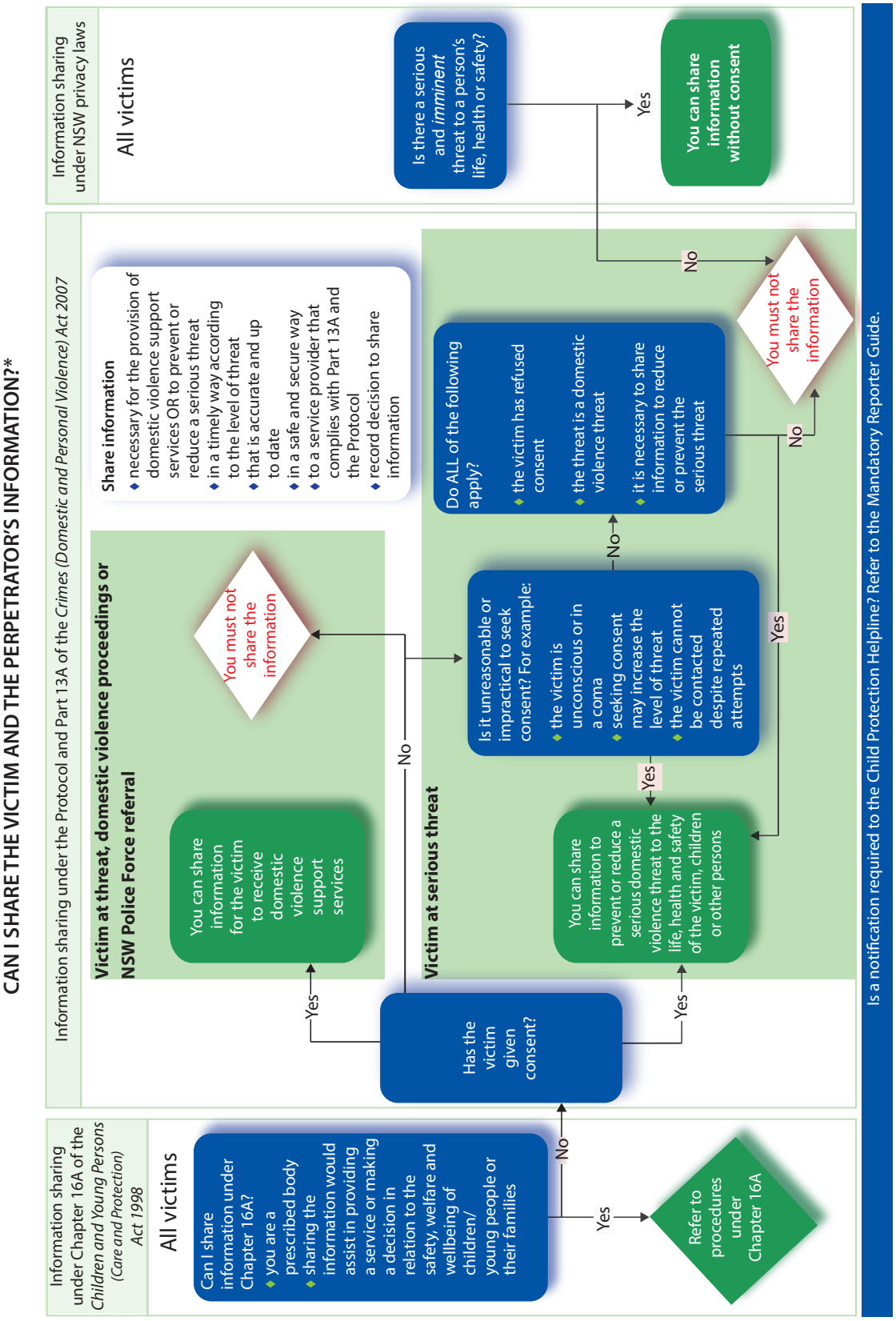
Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* and Information Sharing Protocol Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and other relevant legislation



Appendix 2

Information sharing process flowchart

Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* and related Protocol
Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and other relevant legislation

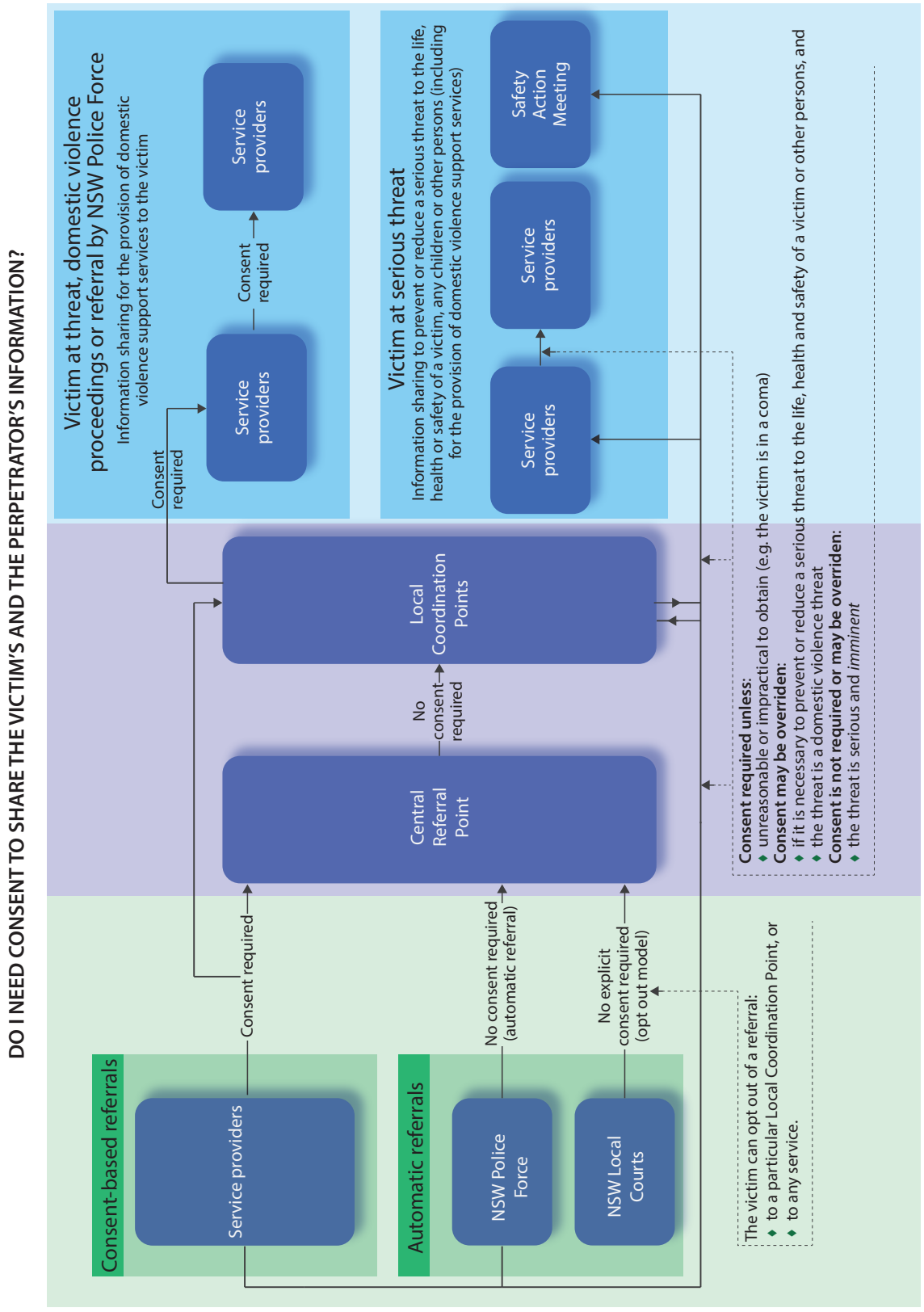


* NSW Police Force and NSW Local Courts refer to the Consent Flowchart at Appendix 3

Appendix 3

Information sharing consent flowchart

Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* and related Protocol
Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and other relevant legislation



Appendix 4

Information sharing compliance checklist

If you or your organisation wish to share information under Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* (Part 13A), you must comply with the *Domestic Violence Information Sharing Protocol* (Protocol). Compliance with the Protocol must be determined using this Compliance Checklist. The checklist should be read in conjunction with chapter 18 Compliance located in the Protocol.

Service providers must use the checklist to:

- Assess their state of readiness to share information under the Protocol
- Conduct annual compliance self-assessments
- Report on compliance to their funding body if applicable, and
- Report on any remedial action.

Funding bodies must use the checklist to:

- Assess and monitor a service provider's state of readiness to share information under the Protocol
- Monitor a service provider's ongoing compliance with the Protocol
- Determine and monitor any remedial actions necessary to ensure future compliance with the Protocol, and
- Conduct formal audits.

Instructions

State of readiness to share information under the Protocol:

- You must be compliant or partially compliant in each section in Part A, and if partially compliant, set out the steps and time frames for full compliance. Where the section is not relevant at the time of completion of the checklist, select N/A and provide a brief explanation.

Self-assessment by service providers:

- Rate your level of compliance against each of the sections in Part A (compliant, partially compliant or non-compliant), and
- Provide any relevant additional information in Part B.

If compliant	If partially compliant or non-compliant
• Submit for review and endorsement by senior staff • Maintain on a compliance file • Submit copy to the funding body as requested	• Describe how you or your organisation are not fully compliant • Explain the reason(s) why you are not fully compliant (if you are subject to a compliance improvement plan, indicate any progress since the last completion of the checklist) • Describe remedial action(s) that will be taken to prevent future non-compliance • Submit for review and endorsement by senior staff • Maintain on a compliance file • Submit copy to the funding body • Submit copy to the NSW Department of Justice as required • Participate in the development of a compliance improvement plan and any other actions as required under the Protocol

Desktop review by funding body:

- Review self-assessment ratings and any explanation/remedial action listed in Part A
- Seek further information/clarification if required
- If the checklist indicates partially compliant or non-compliant, provide guidance and corrective feedback or develop a compliance improvement plan with the service provider
- Monitor the compliance improvement plan until full compliance is achieved
- Undertake any other actions as required under the Protocol
- Complete Part C, and
- Provide any feedback from Part B to the Department of Justice (cpd_unit@adg.nsw.gov.au) as required.

Compliance checklist

Name of service provider			
Address/contact details			
Checklist completed by (name, position)			
Assessment date (start, finish)			
Endorsed by (name, position)		Signature	
Submitted to monitoring body (date, details)			

Part A – Organisation Compliance

Legend: C: Compliant; PC: Partially compliant; NC: Non-compliant

Requirements	Evidence	Rating	Explanation/remedial action required
Organisational practice	The service provider can demonstrate that: • organisational policies and procedures comply with the Protocol • quality assurance processes include a review of internal information sharing policies and procedures • staff training manuals incorporate information sharing procedures under the Protocol	☐ C ☐ PC ☐ NC	
Policies, procedures and processes	The service provider can demonstrate policies and procedures that set out: • how to identify and manage a conflict of interest • when and how client consent to share information must be sought • decision pathways for approval of information sharing without consent or overriding a refusal of consent • client complaint handling procedures • management of breaches and non-compliance of information sharing under the Protocol	☐ C ☐ PC ☐ NC	

Requirements	Evidence	Rating	Explanation/remedial action required
Staff	The service provider can demonstrate that: • all relevant staff have received induction and/or training on the Protocol • senior staff with responsibility for supporting and approving information sharing decisions are identified and have received appropriate training • information is available to direct staff to the Protocol	☐ C ☐ PC ☐ NC	
Record management	The service provider can demonstrate safe and secure methods for: • collection, use and sharing of personal and health information • recording the collection, use and sharing of personal and health information • storage and disposal of personal and health information	☐ C ☐ PC ☐ NC	
Monitoring and compliance	The service provider can demonstrate: • completion of annual self-assessments • processes to monitor/review information flows • timely completion of any compliance improvement plan • systems to monitor access to electronic client information database	☐ C ☐ PC ☐ NC	
Complaints	The service provider can demonstrate in relation to any complaint: • timeliness in dealing with the complaint • documentation of the complaint and the resolution • evidence of notification of the complaint to the funding body	☐ C ☐ PC ☐ NC ☐ NA	
Breaches and non-compliance	The service provider can demonstrate in relation to any breach or non-compliance: • that the non-compliance and/or breach of the Protocol and/or the Act was identified rapidly and appropriate actions taken as specified in the Protocol • remedial action was commenced immediately to meet full compliance • appropriate action was taken to reduce any threat to the victim or any other persons • victims are informed of the breach or non-compliance as required by the Protocol	☐ C ☐ PC ☐ NC ☐ NA	

Compliance checklist, cont.

Requirements	Evidence	Rating	Explanation/remedial action required
Breaches and non-compliance	The service provider can demonstrate in relation to any breach or non-compliance: • that the non-compliance and/or breach of the Protocol and/or the Act was identified rapidly and appropriate actions taken as specified in the Protocol • remedial action was commenced immediately to meet full compliance • appropriate action was taken to reduce any threat to the victim or any other persons • victims are informed of the breach or non-compliance as required by the Protocol	☐ C ☐ PC ☐ NC ☐ N/A	
Victim's rights	There is evidence that: • victims are informed of their right to give or refuse consent to share their information • victims are informed of their right to access their information and amend any inaccuracies • victims are informed of their right to make a complaint and how to do so if they believe their information has been inappropriately disclosed	☐ C ☐ PC ☐ NC ☐ N/A	
Victim consent	There is evidence of: • documenting consent (when and how it is sought) • decisions to share information without consent • safe and secure disposal of information if a referral is refused or consent is refused	☐ C ☐ PC ☐ NC ☐ N/A	

Part B – General feedback

List any comments about the compliance checklist or about any aspects of the Protocol that may help improve the compliance monitoring process.

Part C – Desktop review

To be completed by the funding body

Name of funding body		Region	
Name of person completing the review		Contact details	
Actions required	Examples: ☐ Request prior/new self-assessment compliance checklist(s) ☐ Develop compliance improvement plan with service provider ☐ Review compliance improvement plan ☐ Finalise compliance improvement plan ☐ Advise service provider to cease sharing information under the Protocol ☐ Notify the NSW Department of Justice ☐ Notify the NSW Privacy Commissioner ☐ Other (list)		Due date
Endorsement (name, position, signature, date)			

Appendix 5

Information sharing consent form

Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007**

Why is it important to share information?

Sharing information in cases of domestic and family violence is important so that we can help you stay safe and connect you to the support services that can help you.

Why am I being asked to complete this consent form?

Because we have concerns for your safety and wellbeing, we would like to refer you to domestic violence support services that can address your needs. These services may help you with safety planning, emergency accommodation, counselling, court support and other services.

If you are at serious threat of domestic violence, we may also need to share your information with other services to prevent or reduce a serious threat to your life, health or safety.

By signing this form you give us permission to share your information. Your information will be kept confidential and will only be shared with services who will make sure it is kept securely. It will never be shared with the person who hurt you.

I, ... (name) of

..... (address)

consent to the collection, use and sharing of my personal or health information with other services to receive domestic violence support services (please see other side of this form).

I understand that if there are serious threats to my life, health or safety of my family or other persons, in some cases information may be shared without my consent to protect me, my family or others.

Signature ..... Date .....

Staff name ..... Service provider .....

Signature ..... Date .....

Note to staff: Where verbal consent was obtained, record the circumstances of the verbal consent below:

* The service provider is subject to Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* and the Information Sharing Protocol.

Information sharing consent form

Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007*

If there are threats to your life, health or safety we can refer you to support services that can help you. The support worker will talk to you about your safety needs and referrals that can be made to help you.

Note to staff: With the client, identify safety needs and list in the table below and complete as indicated.

My needs	Name of agencies or services	Information shared

Signature ..... Date .....

Staff name ..... Service provider .....

Signature ..... Date .....

Appendix 6

YOUR INFORMATION AND YOUR SAFETY

Your safety is very important to us.

We want to help you secure your ongoing safety from domestic violence.

Working out your safety needs

To know how we can help you we need to work out the level of threat to your safety.

We do this by asking some questions about what has happened in the past and your current circumstances. We will also ask you about your fears and concerns. Your answers will give us a clearer picture of your situation and needs. This is called a threat assessment.

A threat assessment can be done by a support worker, your doctor, someone from Health, Housing or Education, a police officer or another professional person.

Referring you to support services

After working out the level of threat to your safety, one way for us to help you is to make a referral to a support service.

A referral includes information about you, for example: your name, phone number, what has happened, information about any court notices or protection orders, and a copy of any threat assessment. The referral includes information about the person who hurt you, so that the service understands your situation and needs.

A referral is automatic when police officers attend a domestic violence incident or where there are domestic violence proceedings in court.

Keeping your information secure

Your information is strictly confidential and will only be shared with a support service that is bound by law to keep it secure.

Your information will never be shared with the person who hurt you.

A safe method of contacting you

If we make a referral to a support service, we want to make sure that the service contacts you in a way that does not make you unsafe at home.

For this reason, we will ask you for a safe method and time to contact you.

The support service will follow your instructions when contacting you.

Support services for you and your family

After the referral is made, a support service will contact you and offer you help with different issues you may face.

Support may include:

- safety planning
- emergency accommodation
- counselling
- access to financial assistance
- court support, or
- other services you may need to increase your safety.

Working with you

Important decisions about your safety should be made by you and in most cases we will seek your consent before making a referral to a support service.

Where an automatic referral is made by the police or the court, your consent will be sought straight afterwards, when the support service contacts you.

You can also choose to opt out of a referral made by the court when the court officer talks to you.

Keeping you safe

Generally, we will seek your consent to share your information. But if you are at serious threat of further violence there may be times when we need to share information without your consent. Services will only do this to take actions to protect your life, health or safety or that of other persons.

If this happens, we will let you know, where possible before or as soon as possible after. We will also tell you why we shared the information and who it was shared with.

Making sure your information is correct

If you think that some of the information held about you by a service is incorrect, you can ask to look at your file and ask that the information is corrected. You should talk to your support worker about this.

Making a complaint

If you believe that your information has been shared inappropriately you should speak to your support worker or the manager of the support service and ask how you can make a complaint.

You can also contact:

- Information and Privacy Commission NSW on 1800 472 679
- Victims Access Line on 1800 633 063
- Aboriginal Contact Line on 1800 019 123.

More information

You can find out more information about:

- what information can be shared
- how your information can be used
- how your information will be stored and protected
- how you can correct your information it if it is wrong
- how you can make a complaint about a possible breache of your privacy.

An information sharing protocol is located at:

www.domesticviolence.nsw.gov.au

Appendix 7

Memorandum of Understanding template

BETWEEN

Agency 1 .....

Agency 2 .....

Agency 3 .....

Agency 4 .....

(Purpose for sharing information under Part 13A of the
Crimes (Domestic and Personal Violence) Act 2007 and the Information Sharing Protocol)

1. Project name: Safer Pathway

The introduction of *It Stops Here: Safer Pathway* (Safer Pathway) reflects a shared commitment to improving the response to domestic and family violence through collaborative, integrated service provision and improved information sharing.

To support Safer Pathway, legislative amendments were made that create exceptions to NSW privacy laws and allow service providers to share information about victims, perpetrators and other persons in defined circumstances.

The legislative amendments are contained in Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007*.

The Domestic Violence Information Sharing Protocol

The commitment to improving the response to domestic and family violence requires service providers to have a shared understanding of and to comply with the standards and processes relating to information sharing under Part 13A. The *Domestic Violence Information Sharing Protocol* (Protocol) explains information sharing under Part 13A. It sets out the procedures for service providers to share information, including consent and referral practices, and outlines their information management obligations. It also outlines procedures for access and amendment of information, the management of complaints, and the compliance framework.

The Protocol is made by an order of the Minister for Justice under section 98O of Part 13A. Service providers must adopt the provisions and standards set out in the Protocol to share information under Part 13A and the Protocol. Importantly, in the interests of victim safety, information sharing needs to be supported by processes and applications that promote strong information management principles and secure storage and transfer of personal and health information.

2. Purpose of this MOU

This MOU provides a formal structure for service providers who wish to share information under Part 13A and agree to adopt and comply with the Protocol and the compliance framework.

3. Objectives of the MOU

The objectives of the MOU are to:

- Facilitate information sharing between the parties in compliance with Part 13A and the Protocol
- Establish cooperative working relationships between the parties in order to facilitate information sharing
- Improve victims' confidence in the information sharing process.

4. Status of this document

The MOU is an expression of the purpose and intention of the parties, which is binding in honour only. This MOU does not give effect to any legal relationship or obligations other than those already in existence under any written law. It is not intended to give rise to any consequences or be the subject of litigation, nor is it intended to subjugate the rights, duties or responsibilities of the parties arising from the provision of information about their clients.

5. Shared principles

Parties to the MOU agree to adopt and maintain information sharing standards in accordance with Part 13A and the Protocol and to:

(i) commit to protect the privacy and confidentiality of the information obtained in the provision of their respective services

(ii) commit to the safety of victims of domestic violence and privacy principles to safeguard individuals' personal and health information

(iii) take reasonable steps to assist one another to achieve the objectives of this MOU

6. Legislation

Parties agree to abide by privacy and information sharing standards and legislative instruments including the:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Crimes (Domestic and Personal Violence) Act 2007*
- Any other laws they may be subject to.

7. Roles and responsibilities of parties

Agencies are partners in this MOU because of their key role in the delivery of services to victims and perpetrators of domestic violence. In agreeing to be a partner in the MOU, agencies are responsible for promoting, monitoring and implementing the standards of the Protocol.

Parties agree to share and exchange information according to the Protocol and any additional principles and procedures specified in this MOU, and applicable laws and to:

(i) act within the limits of relevant legislation

(ii) adhere to information sharing and management principles contained in the Protocol

(iii) adhere to the compliance monitoring framework

(iv) verify that their information management policies and processes are consistent with the Protocol

(v) monitor their compliance with the Protocol according to the compliance framework

8. Dispute resolution

Parties will work together to resolve issues as they arise relating to this MOU. Where parties are unable to resolve disagreements, the matter will be managed within internal dispute resolutions process.

Where issues relate to information sharing under Part 13A or the Protocol, the Information Sharing Protocol is the final authority. Where parties are unable to resolve disagreements, the matter will be referred to the Department of Justice whose determination of the issue will be accepted by the parties.

9. Endorsement

The parties, through the undersigned delegates below, sign off to the Memorandum of Understanding.

Name/Title.....	Name/Title .....
Agency.....	Agency .....
Signature.....	Signature .....
Date	Date.....

10. Effective date

This MOU shall be effective from the.....until .....


NSW
GOVERNMENT