ATTACHMENT MH 6

This is the attachment marked "**MH 6**" referred to in the witness statement of Dr Pat Tuohy, Ms Helen Fraser and Ms Miranda Ritchie dated 11 August 2015.

Sharing personal information of families and vulnerable children

A guide for inter-disciplinary groups

Sharing personal information of families and vulnerable children

A guide for inter-disciplinary groups

Introduction

Sharing information about an individual is often essential to their health, safety and wellbeing. It can take the effort of a number of service agencies working effectively together to address the multiple and complex needs of that person or family.

This collaborative approach can not only improve the service provided to the client, but also enhance the working relationships and practice of the professionals involved.

It can be difficult for these agencies to make decisions about whether sharing the information is both appropriate and legal. This guide provides them with the confidence to make sound decisions on the unique circumstances of each case.

This guide is designed to:

- clarify the laws around sharing personal information
- offer practical suggestions and tips for managing information sharing
- explain how Approved Information Sharing Agreements (AISAs) can work
- identify specific information sharing issues that affect children and vulnerable adults.

What is a multi-agency team? (MAT)

In New Zealand, collaborative decision-making processes, such as Family Group Conferences (FGCs) and Strengthening Families meetings, have been around for many years. Over time, similar approaches have been adopted in other sectors to help clients who have issues that require the involvement of multiple agencies.

The core purpose of a multi-agency team is for the agencies involved with a child and family to share information about the child and family, to assess risk and protective factors, and to agree upon a joint management plan.

Wherever possible this will be done with consent. Sometimes that is not possible; the law supports this under certain circumstances, as outlined in this user guide.

How do the teams work?

Usually teams will meet face to face at regular, perhaps weekly, intervals. A Memorandum of Understanding (MoU) is usual for all agencies involved (see page 6).

Who will be a member of the team?

Attendees will usually include senior professionals from agencies such as:

- Police
- district health board professionals (e.g. paediatrics, Child and Adolescent Mental Health, Adult Mental Health, Addictions, Maternity)
- Child, Youth and Family
- Ministry of Education; and
- non-governmental agencies (e.g. Women's Refuge, NGOs specialising in parenting and family violence intervention).

Multi-agency teams can take many forms for example: Children's Teams; Maternal Wellbeing and Child Protection Groups (Vulnerable Pregnant Women's groups); Family Violence Interagency System (FVIARS); Joint Allocation of children with complex behaviours.

Consent to be referred to a MAT

- Consent is usually obtained directly from an adult. Verbal consent is sufficient, but you should document the fact that consent has been given.
- Consent forms should include an up-to-date list of the agencies that may be sharing the client's information.

Always try to get consent

- It's the ethical thing to do (people have a right to know what will happen to their personal information).
- The law requires that you *try* to get consent even if the person is going to say 'no'. Asking them gives them the opportunity to explain their concerns.
- Better outcomes often follow if a patient is engaged in the process and trusts the professionals involved.

What if consent cannot be obtained?

Sometimes consent cannot be obtained (e.g. if a violent partner is always present).

If you are unable to get consent

- Sometimes you need to be pro-active; for instance, by taking the mother somewhere for a private conversation.
- Consider telling the person of your plan to refer.
  - For example: "If we develop concerns about a risk of abuse for your child, we reserve the right to contact the relevant authorities";
  - Or there may be pre-existing concerns: "You've told me… I am concerned for your safety and for your child so what I'm going to do now is to phone Child, Youth and Family".
- Only do this is you are confident there is no risk to adults or children (e.g. of violence to mother or children, or a risk of flight).

If it is impossible to get consent and too risky to even try

- Consider if there is a threat – is the threat sufficiently serious to warrant direct referral to Child, Youth and Family or Police?
  - If so, this should be your first choice.
- If a threat is significant but not at the CYF threshold, consider referring to a MAT anyway.
  - Discuss with a senior colleague.
  - Document your assessment, conclusion, discussion with colleague and plan, including your decision to refer to a MAT.
  - Make the referral in writing. Consider whether you need to discuss verbally with MAT members as well.

Sharing personal information of families and vulnerable children

Privacy Commissioner
Te Mana Matapono Matatapu

The Escalation Ladder

Sharing information involves both the collection and disclosure of personal information. Deciding which laws apply and what information to share can be complicated, but there are some guiding rules.

How to use the Escalation Ladder

Work through from question 1 to question 5 and stop when you can answer 'yes'. If the answer to all of the five questions is 'no', then disclosure should be unnecessary and should be avoided, at least for now.

Remember that the proportionality principle always applies – you should only provide as much information as is reasonably necessary to achieve your objectives.

1 Can we get by without naming names?

YES

- Use anonymous information where practical.
- Disclosing anonymous information is always OK. (For example, if you have professional supervision, you might be able to discuss a case without referring to any names.)

NO

2 Have they agreed?

YES

- If information is not able to be used anonymously, the best thing is consent from the parties concerned.
- Consent does not need to be written.
- Always record the fact that parties have agreed. Record any limitation or qualification of consent e.g. 'please don't involve the church".

NO

3 Have we told them?

YES

- If it is not practicable or desirable to obtain consent, the information may be used or disclosed if it is in line with the purpose for which it was obtained.
- Inform the person affected of this where possible – ideally at the time the information was first collected from them, or soon after that.
- If informing the person would prejudice the purpose of collection, or would be dangerous to any person, then telling the person concerned may be waived in that instance.

NO

4 Is there a serious threat here?

YES

- Information may be used or disclosed where there is a serious threat.
- 'Serious' depends on:
  - how soon the threatened event might take place,
  - how likely it is to occur, and
  - how bad the consequences of the threat eventuating would be.

NO

5 Is there another legal provision we can use?

YES

Many different laws allow personal information to be shared. For instance:

- information about the health/safety of a child or young person can always be disclosed to a police officer or social worker
- health information can be requested by someone who needs it to provide health services
- information can be disclosed where necessary to avoid prejudice to the maintenance of the law.

NO

If the answer to all of the five questions is 'no', then disclosure should be unnecessary, and should be avoided, at least for now.

The Privacy Commissioner operates a free phone line (0800 803 909) that can be used to help with questions around disclosing information.

Suggestions for best practice in information sharing

Disclosing information about children

The Privacy Act generally does not draw a distinction between the privacy rights of adults and those of children.

The only area where there is a difference is when a person asks for access to their own personal information. An agency may refuse a child's request for access to his or her own personal information if the child is under 16 years and the agency believes supplying the information would be contrary to that child's interests (Privacy Act, section 29(1)(d)).

The Children, Young Persons, and Their Families (CYPF) Act allows information held about children to be disclosed if where there is any concern for the welfare and wellbeing of that child. CYPF Act disclosures can be made to a CYF social worker or a police officer. Health information about a child may also be disclosed upon a request by CYF or Police under section 22C of the Health Act 1956.

Groups that are considering sharing personal information about children or developing an AISA or MoU should consider whether:

1. the information sharing practice is in best interests of the child or children concerned
2. the child (subject to their age and capability) has been consulted or informed, their views obtained and whether the information sharing practice adequately takes their views into account
3. there is a sufficient legal basis for their information sharing practice.

Informing the child's parents or legal guardian

Apart from section 22F of the Health Act (see page 16), privacy law provides parents with few additional legal rights to access, use and disclose personal information about their children. But this does not mean that agencies should disregard the role parents have.

The Care of Children Act provides legal guardians with rights and obligations concerning:

- the role of providing day-to-day care for the child
- the child's intellectual, emotional, physical, social, cultural, and other personal development
- important matters affecting the child. These include:
  - (a) the child's name (and any changes to it)
  - (b) changes to the child's place of residence that may affect the child's relationship with his or her parents and guardians
  - (c) medical treatment for the child (if that medical treatment is not routine in nature)
  - (d) where and how the child is to be educated
  - (e) the child's culture, language, and religious denomination and practice.

It is important for agencies to consider what steps have been taken to inform or consult a child's parent or legal guardian about the use of their child's personal information.

Obtaining the parent/guardian's consent is not necessary where to do so would be contrary to the child's safety or best interests, or would be contrary to the law.

Have written "ground rules" – using a Memorandum of Understanding

In order to work well together, group members will often need to share personal information about clients with other group members. Sharing information in this way means that group members are collecting *and* disclosing personal information.

There are many legal rules covering this process which can lead to confusion about which rules should apply and to whom.

Even where the rules appear relatively clear, there may be uncertainty among group members about how those rules should be interpreted.

One way for inter-disciplinary groups to make things clear is to set guidelines about the way they will share personal information between group members.

These agreed practices should be in writing and could take the form of an MoU between the group members.

The Privacy Commissioner's Office is available to help agencies as they develop an MoU.

What should be in an MoU?

The purpose of the information sharing

The MoU should explain why it is necessary for information to be shared amongst the group; i.e.

- case management purposes
- to improve the delivery of services and to achieve better outcomes
- to identify the clients who are most at-risk in the community
- enable best practice setting out how these outcomes can be achieved by better information sharing.

NOTE: A written statement of purpose will help to ensure that inter-agency information collection and disclosure practice complies with the Privacy Act.

Principle 11 allows personal information to be disclosed where:

- disclosure of the information is one of the purposes in connection with which the information was obtained; or
- disclosure of the information is directly related to one of the purposes in connection with which the information was obtained.

The scope of the information sharing

The MoU should set out the extent of the information sharing; i.e.

- Is the shared information to be used solely for the purposes and work of the inter-agency group?
- On what occasions, if any, can group members use the information they receive for wider purposes?
- When, if at all, can the information be disclosed to other parties?

The role that each agency plays in the group

The MoU should reflect the different roles and legal functions/duties of group members. It should also clearly set out mutual obligations and expectations concerning the use of shared client information.

Ways of resolving problems/complaints and disputes

The MoU should set out agreed procedures to deal with problems arising from the information sharing.

There should be a process for dealing with complaints from people or clients affected by the group's information sharing. There should also be a process for dealing with internal disputes or problems concerning the use of shared information by group members.

When you get stuck

From time-to-time, dilemmas about whether to share information will still arise even if agreed information sharing practices have been developed.

Where following agreed practices are not enough to resolve an information sharing dilemma, or where the agreed practices are yet to be formally developed, you can use the escalation model to help in your decision making. The escalation ladder (on page 4) will help you to disclose the information you need to, after considering a series of questions.

When an MoU doesn't go far enough

A set of agreed ground rules in an MoU can help to clarify understanding between group members. But it does not allow disclosure of information that would otherwise be illegal under the Privacy Act or other statutes.

There are circumstances when information cannot lawfully be disclosed under the Privacy Act or other statutes. To get around this, the Privacy (Information Sharing) Amendment Act 2013 enables agencies to enter into Approved Information Sharing Agreements (AISAs).

What is an AISA?

AISAs are agreements that can be formed between government departments; or between government departments, private sector agencies and NGOs.

Each AISA must include a government department as the 'lead agency.' AISAs cannot be made solely between NGOs.

An AISA must be reviewed by the Privacy Commissioner and approved by a government Minister before they take effect.

What does an AISA do?

AISAs provide agencies with a clear legal basis under which information sharing practices may occur.

The Ministry of Social Development is currently working on developing an AISA to improve information sharing around child safety.

Further help

The Privacy Commissioner's Office has an 0800 free phone line (0800 803 909) that can be used to help with questions you might have around sharing information or AISAs.

Information sharing scenarios

Example	Scenario	Questions
1. **Miss S:** 18 year old woman, 16 weeks pregnant, previous CYF involvement as a child. • Partner supportive, both excited about pregnancy, but lack parenting skills. • No family support. This couple have moved to a new area and family are distant. **Assessment:** Low to moderate risk. MAT would be useful.	**A.** Consent is given for their case to be handled by a Multi Agency Team. The midwife makes a referral.	**Escalation Ladder Step 2: Have they agreed?** The answer is yes.
	B. Consent is not given for their case to be handled by a MAT but consent is given for them to be referred to an NGO. Lead Maternity Carer (LMC) and NGO social worker work together on the case.	**Escalation Ladder Step 2: Have they agreed?** The answer is no. The NGO should explain how it plans to use the information in keeping with Escalation Ladder Step 3: Have we told them?
	C. GP makes referral to a MAT prior to discussion with Miss S. GP believes the couple are "not telling the whole story". The GP sought their consent to refer them to a team but consent was not given. The MAT identifies other risks – absconding, drug and alcohol abuse, partner convicted of assault. It refers the case back to the Lead Maternity Carer for further assessment and recommends referrals to other supportive agencies.	**Escalation Ladder Step 1: Can we get by without naming names?** This is an example of where an initial Step 1 approach by the GP could be used. If a referral is deemed appropriate, then it could be justified by either: **Escalation Ladder Step 3: Have we told them?** **Or** **Escalation Ladder Step 4: Is there a serious threat here?** *Should the MAT accept a referral without the woman's consent from a GP?* Yes. The main obligation is on the GP who would be breaching clinical confidentiality but circumstances such as a serious threat could justify breaching that confidence.

Information sharing scenarios

Example	Scenario	Questions
2. **Miss B:** 18 year old woman, 16 weeks pregnant, previous CYF involvement as a child. • Partner unsupportive, unhappy about pregnancy. • Partner drinks to excess regularly, and uses drugs occasionally. • Miss B has disclosed one episode of being physically assaulted by her partner. He held and punched her head and abdomen repeatedly with his fists. • No family support. The couple have moved to a new area and family are distant.	**A.** Consent is given to take the case to a Multi Agency Team and the midwife makes a referral.	**Escalation Ladder Step 2: Have they agreed?** The answer is yes.
	B. Consent is declined to refer the case to the MAT (or unable to obtain consent due to the risk of violence to Miss B). The midwife forms the view that the threat is serious and refers the case to the team. At the MAT, the Police note attending multiple assault incidents at the couple's address. The partner has two recent convictions for assaulting women prior to the current relationship.	**Escalation Ladder Step 4: Is there a serious threat here?** Yes. The midwife makes a referral to the MAT without Miss B's consent. *Is this defensible under the Privacy Act with a memorandum of understanding for the MAT?* Yes. Disclosure of information in this case is to prevent or lessen a serious threat and is permissible.

Information sharing scenarios

Example	Scenario	Questions
3. **Miss A:** 16 years old, 25 weeks pregnant, with no Lead Maternity Carer but meets with a school nurse. • She has had mental health involvement two years ago and attempted suicide. • Her 17 year old boyfriend is unsure of becoming a father. • She is transient with no fixed address and is temporarily living with friends.	**A.** Miss A consents to school nurse referring her case to a Multi Agency Team and the referral is made.	**Escalation Ladder Step 2: Have they agreed?** The answer is yes.
	B. Miss A declines consent to be referred to a MAT. The school nurse assesses the threat as serious and makes the referral. At the MAT, CYF note multiple breakdowns of care due to behaviour and recent Youth Justice involvement for violent assault. Police intended to charge her but she ran away and was unable to be located. Child, Adolescent and Family Service (CAFS) also had serious concerns about her mental health after diagnosing early psychosis which wasn't followed up because she failed to appear at subsequent appointments.	**Escalation Ladder Step 4: Is there a serious threat here?** The answer is yes. A referral is made to the MAT without her consent. *Is this defensible under the Privacy Act with an MoU for the MAT?* Yes, if the nurse believes on reasonable grounds that there is a serious threat and making the referral will either prevent or lessen it.

Information sharing scenarios

Example	Scenario	Questions
4. **Miss D:** 24 years old, fourth pregnancy. • She abuses alcohol, together with her partner. • All previous children have been taken into CYF care. • She has suffered from partner violence recently and in the past. Police have attended at least one domestic incident involving physical violence to her. • She has not engaged a midwife.	Police make a referral to the Multi Agency Team without her consent. The team considers her to be a high risk pregnancy and Miss D is offered midwifery services and informed of her referral to the MAT. CYF also runs a report on her history and reports back to the team. An addictions clinician is engaged to investigate whether any assistance has been given in the past. The background check is followed up and other actions are taken in response to the information gathered.	The Escalation Ladder may be helpful in clarifying what information can be requested or sourced about Miss D and her partner and the risks posed by alcohol and drug misuse and mental illness. **Escalation Ladder Step 1: Can we get by without naming names?** No. Proceed to the next stage. **Escalation Ladder Step 2: Have they agreed?** No. Proceed to the next stage. **Escalation Ladder Step 3: Have we told them?** Yes. This is permissible with an MoU. If there is no MoU, given the current and past violence, go to the next stage. **Escalation Ladder Step 4: Is there a serious threat here?** The answer is yes. But the earlier options should be exhausted first.

Information sharing scenarios

Example	Scenario	Questions
5. **Baby J:** Aged eight weeks. • Brought in to a hospital emergency department and admitted to the children's ward, for 'failing to thrive' (i.e. insufficient weight gain or inappropriate weight loss) and with evident bruising on his back. • Mother is an 18 year old woman with previous CYF involvement as a child who admits to being a heavy binge drinker. She has had previous referrals to alcohol and drug addiction services. While in the ward, she is questioned about family violence and discloses there has been violence during her pregnancy and that she had told her midwife. • Father is in his early 20s and has a history of alcohol and substance abuse. • The couple has no family support. They have moved to a new area and family members are distant.	The mother consents to the family's case to be referred to a Multi Agency Team but she does not consent to access to any clinical files. This includes paediatrics and addictions service.	*What information can be requested or sourced without consent about Baby J relating to the baby's maternal care, delivery and post natal information?* **Escalation Ladder Step 4: Is there a serious threat?** Yes. Preferably in conjunction with an MoU defining what the trigger factors are in this context (i.e. is it just the baby's failure to thrive? Or is it that plus other markers of concern?) *What information can be requested or sourced without consent in relation to the mother and the father?* **Escalation Ladder Step 3: Have we told them?** Yes. This should be in accordance to the MAT's agreed practices of information sharing as set out in its MoU.

Information sharing scenarios

Example	Scenario	Questions
6. **Baby AJ:** Four month old boy. • Admitted to a hospital children's ward with severely infected, poorly managed eczema. • His mother has had considerable advice and support but has been unable to apply the advice. • The boy has had poor weight gain and is developmentally delayed but has no injuries or other signs. • The mother is suffering from postnatal depression and increasing alcohol abuse. • She denies that any family violence has occurred, including anyone hitting her children.	**A.** The baby has no other siblings. The mother says she has good support around her but that she "shuts them out". She accepts the children ward social worker's offer to involve other family members and a referral to mental health and addiction services.	**Escalation Ladder Step 2: Have they agreed?** Yes. Consent has been given.
	B. The baby has a five year old brother. The mother reveals that the boy is often kept at home for minor illness "but he's doing really well". The mother declines support that's offered as well as permission to contact other agencies.	*Can a clinician contact the brother's school without the mother's consent to obtain the child's attendance records as well as find out if there are concerns about the boy's wellbeing?* **Escalation Ladder Step 3: Have we told them?** Yes. The information may be disclosed if it is in line with the MoU. *Can a clinician contact a GP, midwife or Plunket nurse without the mother's consent?* **Escalation Ladder Step 5: Is there another legal provision we can use?** Yes. The information may be disclosed under section 22F of the Health Act. Health information can be requested by someone who needs it to provide health services.

Information sharing scenarios

Example	Scenario	Questions
7. **Boy AB:** Eight year old boy. • Referred to a paediatrician for increasing violence and deteriorating learning. • No relevant medical history, no medical issues, normal examination. • Mild learning difficulties and normal level of concentration.	**A.** Mother reveals there has been domestic violence in the past. She has been to court and the boy's father was convicted. The father has attended a stopping violence course and is no longer violent. The children were never hit. When he loses patience with the son, he now walks away. Mother accepts that previous family violence is the likely cause of the boy's behaviour. She accepts a referral to the Child, Adolescent and Family Service.	**Escalation Ladder Step 2: Have they agreed?** Yes. Consent has been given.
	B. The mother reveals current violence towards her on about a monthly basis. She has suffered bruising but no fractures. The severity of the violence is increasing but she does not believe she will be seriously hurt. Her partner's behaviour is increasingly bizarre. He has previous mental health history. The children are never hit but witness the violence towards the mother. She agrees this is a likely cause of the boy's behaviour. The mother declines a referral to a family violence agency. She says the partner is very unlikely to come to a conference.	**Escalation Ladder Step 4: Is there a serious threat here?** Yes. The threshold is serious threat which requires consideration of imminence, likelihood and severity. This example would tick all three criteria as it is relatively imminent (monthly), likely (is happening regularly) and relatively severe. *Can a paediatrician access the father's mental health record without his consent?* **Escalation Ladder Step 1: Can we get by without naming names?** No. **Escalation Ladder Step 2: Have they agreed?** No. **Escalation Ladder Step 3: Have we told them?** Probably not. If informing the person would be dangerous to any person, then telling the person concerned (the partner) may be waived in that instance. **Escalation Ladder Step 4: Is there a serious threat here?** Possibly, but it would need a mental health agency to be confident that disclosing the mental health information would prevent or lessen the threat.

Relevant legislation

Privacy Act 1993

The Privacy Act regulates how public and private sector agencies (such as schools, NGOs, government departments, small and large businesses) may collect, hold, use and disclose personal information about identifiable individuals.

At the heart of the Privacy Act are *12 information privacy principles*, which apply without distinction to children, adults and vulnerable adults. The Office of the Privacy Commissioner (OPC) has summarised these principles as:

1. only collect information if you really need it
2. get it straight from the people concerned where possible
3. tell them what you're going to do with it
4. be considerate when you're getting it
5. take care of it once you've got it
6. people can see their information if they want to
7. they can correct it if it's wrong
8. make sure information is correct before you use it
9. get rid of it when you're done with it
10. use it for the purpose you got it
11. only disclose it if you have a good reason
12. only assign unique identifiers where permitted.

Principles 1-4 cover the **collection of personal information**

Agencies have to be clear about why they are collecting personal information and to explain these reasons to the individual (unless there is a good reason why they can't). Agencies can't collect information in ways that are unfair, unlawful or unreasonably intrusive.

Principle 5 governs the way personal information is **stored.**

It is designed to protect personal information from unauthorised use or disclosure. Agencies also have to take reasonable steps to keep information they hold safe against loss, destruction and unauthorised modification.

Principle 6 gives individuals the **right to access information about themselves**. Information requests can be made for any reason, and must be responded to within 20 working days.

Principle 7 gives individuals the **right to seek correction of information about themselves**. If the correction isn't made they can demand that a statement of correction is attached to the information they disagree with.

Principles 8-11 place restrictions on how people and organisations can **use or disclose personal information**.

These include ensuring information is accurate and up-to-date, and that it isn't improperly used or disclosed. The use and disclosure principles have a number of important exceptions – for instance, disclosure with authorisation is always acceptable, as is disclosure to prevent or lessen a serious threat.

Principle 12 restricts the use of unique identifiers

Unique identifiers include IRD numbers, bank client numbers, driver's licence and passport numbers – to the agency that initially created them, with a few specific exceptions (such as the NHI, which can used across the health sector).

The Privacy Commissioner has produced a factsheet on the information privacy principles which sets out in detail how agencies should apply the principles (www.privacy.org.nz).

Health Information Privacy Code 1994

The Health Information Privacy Code modifies the 12 information privacy *principles* under the Privacy Act into 12 health information privacy *rules*. The Code's 12 rules regulate how health agencies (such as doctors, health insurers and district health boards) may collect, hold, use and disclose health information about identifiable individuals.

The biggest difference between the *rules* of the Code and the *principles* of the Act concern the disclosure of personal information, which is regulated by rule 11.

Rule 11 of the Code sets out provisions that have specific application to the health sector. For instance, doctors may disclose health information to family members or caregivers when necessary, and hospitals may provide basic information about current patients on request.

Health Act 1956

Section 22C of the Health Act allows (but does not require) anyone holding health information to disclose that information, upon request, to people acting in specified official capacities, namely:

- a probation officer or prison medical officer
- a social worker or a care and protection co-ordinator
- an MSD employee for the purpose of determining benefit payments in hospital
- a member of the New Zealand Defence Force, for the purposes of administering the Armed Forces Discipline Act 1971 or the Defence Act 1990
- a police constable, for the purposes of performing his or her official functions
- any employee of the Ministry of Health, for the purposes of administering the Health Act or the Hospitals Act or compiling statistics for health purposes
- an employee of a district health board, for the purposes of exercising or performing any of that board's functions under the New Zealand Public Health and Disability Act 2000.[1]

Section 22F is also relevant. It gives the representative of a person (which includes the parents or guardians of children under 16) a legal right of access to their child's health information except where contrary to the child's wishes or interests.

This right also applies to anyone that is or is going to be providing health care to a person; so an individual's new doctor could legally enforce a demand for access to that person's old health records by complaining to the Privacy Commissioner, as could the parent or guardian of a child under 16.[2]

1 Identifiable information may only be provided where it is essential to that function
2 See also rule 11(4) of the Health Information Privacy Code 1994

Children, Young Persons and their Families Act 1989

The Children, Young Persons and their Families Act 1989 governs New Zealand's child protection and youth justice jurisdictions. The CYPF Act allows (and sometimes requires) disclosure of personal information in certain circumstances:

Section 15 enables any person who is concerned for the well-being or welfare of a child or young person to report those concerns to a Child, Youth and Family social worker or the Police.

Section 16 protects that person from any liability in civil, criminal or disciplinary proceedings regarding any disclosures they make, unless those disclosures are made in bad faith.

Section 66 requires any government department, crown entity or agent to supply information held about a child, upon the request of a CYF social worker, care and protection co-ordinator or police constable. A section 66 request may be made for the purposes of determining whether a child is in need of care and protection, or where proceedings are occurring under the Act.

There are currently a number of developments planned for improving outcomes for vulnerable children.

- The development of a *Vulnerable Kids Information System* which enables front-line professionals to share information about children at risk of abuse or neglect. This will include built-in safeguards, including a code of conduct and auditing requirements (scheduled for implementation in 2014/15).
- The introduction of legislation to support greater scope for information between government departments, agencies and NGOs that deliver social services (scheduled for implementation at the end of 2014).
- Providing those who deliver services and programmes to vulnerable children and families, with access to personal information held on the children they are working with (scheduled for implementation at the end of 2014).

Relevant international law

New Zealand is a ratified signatory to the UN Convention on the Rights of the Child (UNCRC). **Article 16** provides the child the right to protection of the law against any arbitrary or unlawful interference with their privacy.

Article 3.1 provides that in all actions regarding children by public and private social welfare institutions, courts, administrative authorities and legislative bodies, the best interests of the child must be a primary consideration.

Article 12 provides that the child who is capable of expressing his or her own views has a right to express those views, which must be given due weight in accordance with their age and maturity.