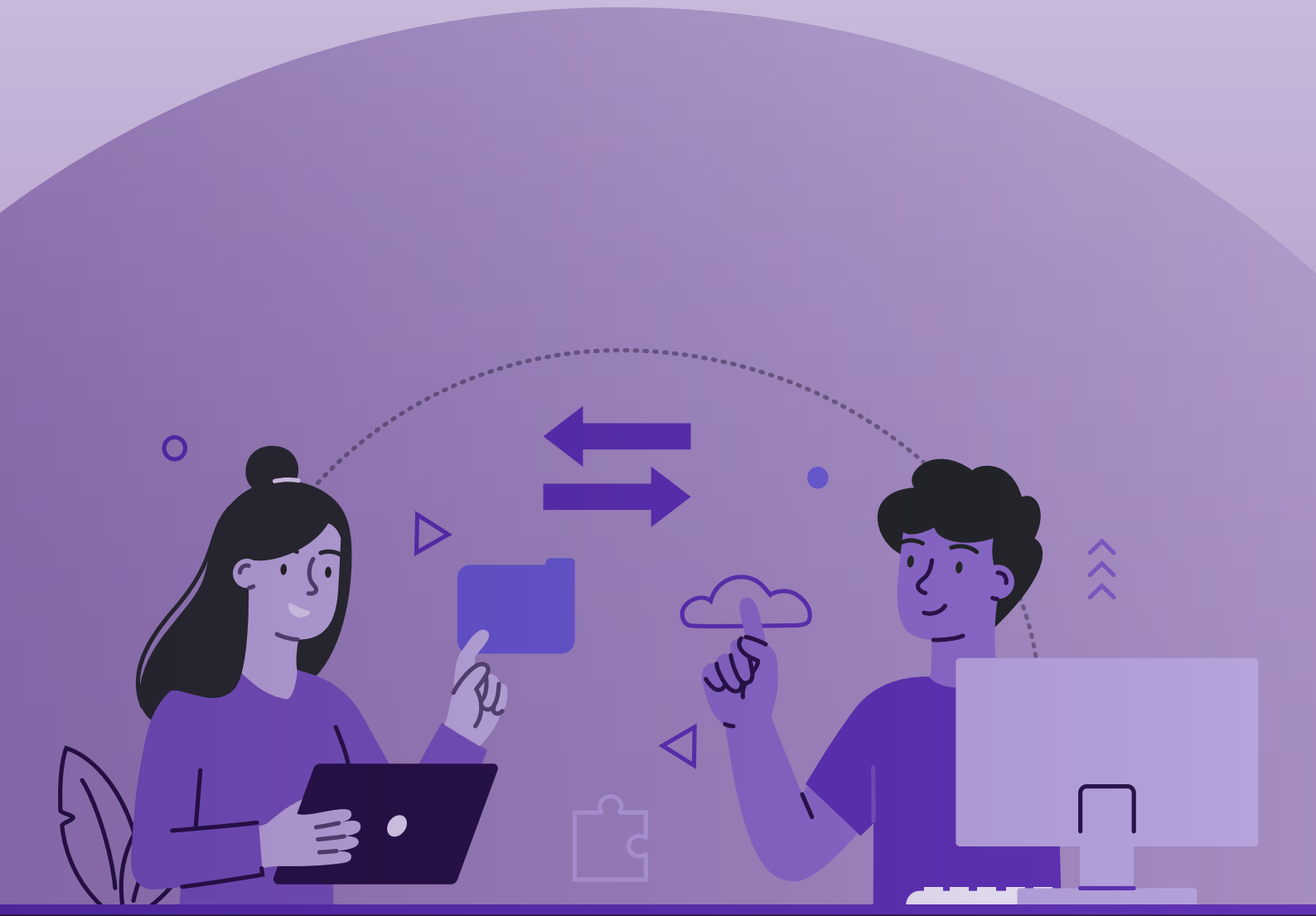
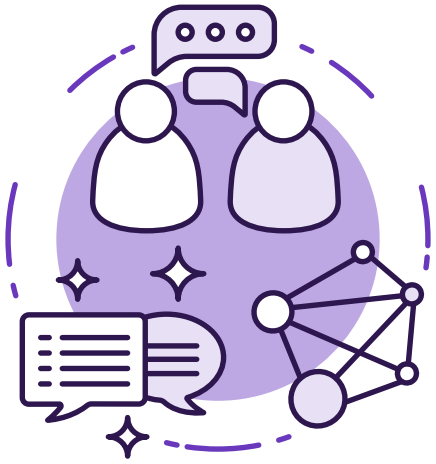
Te Kāwanatanga o Aotearoa
New Zealand Government

# GCPO Guidance

## Legal authority to share information



Version 1.00 | March 2024



**A legal authority should exist for all information sharing activities to give everyone confidence you are sharing personal information legally and appropriately.**

# Contents

## Purpose of guidance

The purpose of this guidance is to help you understand:

- what a legal authority is
- the different types of legal authorities for information sharing
- what legal authority may be appropriate for your information sharing activity

This guidance does not cover the sharing of information to an individual who is exercising their rights under Information Privacy Principle (IPP) 6, the Official Information Act 1982, or an agency's enabling legislation.

## Audience for guidance

This guidance can be used by:

- Public sector agencies, including:
  - Regional staff
  - National Office staff
- Organisations working with government agencies

### Questions about this guidance

If you have any questions about this guidance please contact GCPO at GCPO@dia.govt.nz.

## What is a legal authority?

All information sharing must be permitted by legislation.

Where a legislative provision permits the sharing of information that legislative provision is referred to as the legal authority.

It is important to ensure that a legal authority exists for your proposed information sharing. This gives everyone confidence that you are sharing personal information legally and appropriately - that is, yourself, your agency, the receiving agency/organisation, and the public.

## What legal authority to use

There are various legislative provisions that permit the sharing of information. Each provision permits the sharing of information for a specific purpose. More than one provision may permit your intended information sharing activity — you'll need to identify the legal authority that best fits your information sharing activity.

Some legal authorities have specific parameters and restrictions for the information sharing they permit, such as:

- only between specific types of agencies
- restricted categories of information
- for specific purposes only.

**Before you share information, check with your privacy, information sharing or legal team who will provide specialist advice on the appropriate legal authority for your proposed information sharing activity**

The following sections break down the main Acts and legislative provisions that authorise or enable the sharing of information.

# Privacy Act 2020 for sharing information

The Privacy Act is the main legislation governing the sharing of personal information in New Zealand.

## Information Privacy Principles 2 and 11

### Disclosures and collections

Sharing personal information with another agency is a “disclosure” under the Privacy Act. An agency can only disclose personal information if the proposed disclosure satisfies one of the exceptions listed in Information Privacy Principle (IPP) 11.

Receiving personal information that another agency shares is a “collection” under the Privacy Act. An agency should generally collect personal information from the person concerned, but there are exceptions in IPP 2 that allow agencies to collect personal information indirectly.

It does not matter how that information is shared. Information may be physically sent, transmitted digitally, your agency may allow another agency to extract information from your systems or view and use information within your systems. All of these are disclosures and collections.

### IPP 11 exceptions

Commonly used exceptions include where the:

- individual gives authorisation
- disclosure is for one of the purposes, or a directly related purpose, for which the information was initially collected
- information is used in a form that does not identify the individual
- information is used for research and statistical purposes and will not be published in a form that could reasonably be expected to identify an individual
- disclosure is necessary to prevent or lessen a serious threat to health and safety, or to avoid prejudice to the maintenance of the law.

You will need to assess the circumstances of your sharing activity to determine whether an exception applies.

The collecting agency has to ensure that it genuinely needs the information and that it's allowed to collect it. However, there is a higher risk associated with disclosing information, as it is important to make sure people's information is not improperly exposed. The agency disclosing the information should therefore check carefully that one of the exceptions is satisfied before sharing any personal information either in response to a request or proactively.

Examples of sharing personal information using IPP 11 exceptions include:

### Threat of Harm

You are a case manager for a government agency. You are working with an individual who has recently been made redundant to identify appropriate government agency services that may be able to support the individual and their family through this rough time. In a meeting with the family, an adult family member makes a comment about his anger at the individual's employer and that he intends to make them pay for the harm they have caused the family. You are concerned that the family member will carry out his threats.

**Can you share your concerns with anyone?**

You should always inform and talk to your manager in the first instance. The **IPP 11 (1)(f) serious threat exception** permits you to share information to lessen or prevent a serious threat to the life or health of another person, or to public health and safety. When using this exception, you should believe on reasonable grounds that the sharing is necessary to lessen or prevent the threat, and only share relevant information with a person or agency that is able to do something to lessen the threat.

In this case, you could share information with Police about the family member who made the threatening comments, the threat that was made, and about whom the threat was made.

## Police investigation into criminal offending

Police have approached your agency seeking information about a 30-year-old individual. Police have advised that they are undertaking an investigation into allegations of criminal offending. They have requested contact information your agency holds in relation to the named individual.

**Can you share the individual's contact information with the Police?**

The IPP 11 (1)(e) **maintenance of the law exception** permits you to share personal information if you believe on reasonable grounds that the disclosure of the personal information is necessary to avoid prejudice to the maintenance of the law.

Before you can disclose personal information, you must be satisfied that Police are investigating a potential breach of the law, and that the disclosure of the personal information is necessary for the purpose of maintaining that particular law. For example, if the contact details you hold about the individual are several years old and potentially out of date, it may be harder to say it is necessary in the circumstances to disclose that information.

## Student conducting research for their thesis

A university PhD student has approached your agency requesting a data set containing personal information to enable the student to undertake data analysis to support their thesis.

**Can you share the data set containing personal information with the student?**

The IPP 11 (2)(g) **research and statistics exception** permits the sharing of personal information where you believe on reasonable grounds that the information will not be used in a form in which individuals could be identified or will be used for research and statistical purposes and will not be published in a form that could reasonably be expected to identify the individuals.

You should satisfy yourself that the conditions of IPP 11 (2)(g) will be met by the student before you disclose the personal information. You should also determine whether the needs of the student can be met by providing non-identifying information. You should consider documenting the sharing in an Information Sharing Agreement, which will include controls such as rules about storage or retention of the information. Depending on the type of research being undertaken you may also want to confirm whether the student has obtained ethics approval to complete the research.

## Approved information sharing agreements (AISAs)

The Privacy Act enables the development of approved information sharing agreements (AISAs). AISAs are a legal instrument, as they are approved by an Order in Council. AISAs provide the legal authority for the sharing of specified information between specified agencies for specified purposes.

AISAs are used when a modification to the IPPs is required to enable the information sharing activity. Schedule 2 of the Privacy Act 2020 lists:

- all AISAs
- the agencies that are party to the AISAs
- the information that can be shared
- the purpose for sharing under the AISA.

Further information about AISAs is available from the Privacy Commissioner's website.

## Privacy Act codes of practice

The Privacy Commissioner has the power to issue codes of practice. These codes modify the operation of the Privacy Act and set rules for specific industries, organisations, or types of personal information.

### Health Information Privacy Code

If you are wanting to share health information about an individual, you will need to consider whether the Health Information Privacy Code (HIPC) 2020 applies. The HIPC sets specific rules for agencies in the health sector, including rules for sharing health information.

The HIPC applies to:

- health or disability services such as primary health organisation, rest homes, supported accommodation, doctors, nurses, dentists, pharmacists, and optometrists
- listed agencies that are part of the health sector, such as ACC, Ministry of Health, Te Whatu Ora, Health Research Council, health insurers and professional disciplinary bodies.

The HIPC rules align closely with the information privacy principles. So, for example, a health agency can only disclose health information if the proposed disclosure satisfies one of the exceptions listed in Rule 11. While it's not always required, authorisation plays a stronger role in the health sector than it does in non-health contexts.

Examples of sharing personal information using Rule 11 exceptions include:

### Researcher seeking health information

A researcher has approached your agency seeking health and wellbeing information about a cohort of individuals to enable research into the impacts of physical activity on the health and wellbeing of children at school. The research project has ethics approval as information will also be collected directly from the children and their parents.

**Can you share this information with the researcher?**

Rule 11(2)(c)(iii) permits a Health Agency to disclose health information if it believes on reasonable grounds that the information will be used for research purposes (for which ethics approval has been provided if required) and will not be published in a form that could reasonably be expected to identity individuals. If you are not a health agency but hold health information in relation to the cohort of individuals, you cannot use the HIPC exceptions. You will need to consider the IPP 11 research exception. You may also want to consider documenting the sharing of the information in an Information Sharing Agreement.

### Doctors sharing with other health providers

An individual has suffered an injury to their ankle. They have an appointment with their GP where the GP collects information about the injury.

**Can the GP pass this information on to an orthopaedic specialist?**

Section 22F of the Health Act 1956, supported by rule 11(1)(c) of the HIPC, permits the disclosure unless the GP considers that the patient would not want that information to be disclosed. The GP will not generally need to seek the permission of the patient to disclose the information to the specialist as the referral was one of the purposes for which the information was collected and the specialist is providing health services to the patient. However, at the time of the consultation, the GP should advise the patient what information will be provided to the specialist for the purposes of supporting the referral (Rule 3).

## Agencies not covered by HIPC rules

Many agencies hold health information but are not "health agencies" as defined by the HIPC. If you are **not** a health agency, then the HIPC rules are not relevant to you.

Instead, you will need to consider the exceptions in IPP 11 or other legal authorities such as the Oranga Tamariki Act or Family Violence Act before you share health information.

**You should seek advice from your privacy, information sharing or legal teams if you think your information sharing activity could be authorised by the HIPC, so that you can be aware of any special obligations that may apply.**

## Other codes of practice

There are five other codes of practice:

- **Civil Defence National Emergencies (Information Sharing) Code 2020**
  This code provides agencies with a broader discretion to collect, use and disclose information provided that a state of national emergency is in place (and for 20 working days after the state of national emergency is lifted). It facilitates the sharing of information to assist in the response to the national emergency.

  For example, it permits sharing information to help:

  - identify individuals who are caught in the emergency
  - identify people that may need specialist assistance
  - coordinate the management of the emergency

- **Telecommunications Information Privacy Code 2020**
  This code applies specific rules to telecommunications agencies to better ensure the protection of individual privacy. The code applies to telecommunications information collected, used, and disclosed by telecommunications agencies.

  Most of the code is not relevant to public sector agencies, except for the purposes of general knowledge. However, relevant agencies should be aware of the provision that allows sharing of emergency location information to facilitate a response to an emergency call or to prevent or lessen a serious threat to an individual's life or health.

- **Credit Reporting Privacy Code 2020**
  Applies to credit reporting companies to ensure the protection of individual privacy. Credit reporting companies must display a summary of the rights under this code on their websites and when responding to a person's request for a copy of their credit report.

While the code does not apply to government agencies, finance and HR advisers may need to be aware of some of the rules so they are clear about what credit reporting companies can and cannot do.

- **Justice Sector Unique Identifier Code 2020**
  This code provides a partial exemption from IPP 13 for specific agencies within the Justice sector when those agencies reassign a unique identifier to people proceeding through the justice system. It does not affect the operation of the other information privacy principles.

  Agencies subject to the code include Police, Department of Corrections, Waka Kotahi, Ministry of Social Development, Ministry of Justice, the Registrar of Motor Vehicles, and Road User Charges Collectors.

- **Superannuation Schemes Unique Identifier Code 2020**
  This code provides a partial exemption from IPP 13 for agencies with certain superannuation schemes. It does not affect the operation of the other information privacy principles.

  Those who need to provide advice in this specialist area may need to consult the code.

**You should seek advice from your privacy, information sharing or legal teams if you think your information sharing activity could be affected by a code of practice.**

## Law enforcement information

There are general exceptions in some of the information privacy principles (including IPP 11) that permit information sharing if the agency reasonably believes this is necessary for the maintenance of the law.

However, Schedule 4 of the Privacy Act also authorises specified public agencies to have access to listed types of law enforcement information that is held by other specified agencies. This Schedule covers some of the most common sharing needs, to make it easier to determine if the sharing is allowed.

Specified agencies include:

- Police
- Serious Fraud Office
- Department of Corrections
- Ministry of Justice
- Ministry of Business, Innovation and Employment
- NZ Transport Agency

- Ministry for Primary Industries
- NZ Customs Service
- WorkSafe NZ

Each specified agency will have its own internal policy and procedures for accessing and sharing law enforcement information under the Privacy Act.

**You should seek advice from your privacy, information sharing or legal teams if you think your information sharing activity involves law enforcement information under section 172 and Schedule 4 of the Privacy Act.**

## Identity information

The Privacy Act authorises specified public agencies to have access to identity information about individuals held by other agencies (holding agencies).

Schedule 3 of the Privacy Act sets out which agencies can access specified types of identity information held by listed agencies for specific purposes. In most cases, the purposes for accessing identity information relate to verifying the identity of a person.

Each agency authorised to access identity information held by another agency will have its own internal policy and procedures for accessing that information.

**You should seek advice from your privacy, information sharing or legal teams if you think your information sharing activity involves accessing identity information under section 165 and Schedule 3 of the Privacy Act.**

## Section 30: Privacy Commissioner authorisation to share

The Privacy Act provides the Privacy Commissioner with the power to authorise a one-off disclosure of personal information that would otherwise breach IPP 11, provided that either:

- the public interest in the disclosure outweighs the privacy interests of the individual, or
- the benefit of the disclosure to the individual outweighs the privacy interests of the individual (for example, where there's a direct financial benefit associated with the disclosure to the individual).

**You should seek advice from your privacy, information sharing or legal teams if you think your information sharing activity could be authorised by section 30.**

Further information about how to make applications, and what information to include, is available on the Privacy Commissioner's website.

## Information Matching Programmes

All information matching programmes set out in Schedule 5 of the Privacy Act are authorised under specific statutory provisions.[1]

Since the new Privacy Act came into force in 2020, no new information matching programmes can be established. Other forms of information sharing, including AISAs, need to be considered instead.

However, there are still some programmes in operation. Those programmes are governed by the rules set out in the Privacy Act. Relevant staff in agencies (for example staff who compile data to be able to report to the Privacy Commissioner) will need to be aware of those rules.

## Additional Privacy Act guidance and resources

The Office of the Privacy Commissioner has the following guidance on sharing information under the Privacy Act 2020:

- IPP 11: Office of the Privacy Commissioner | IPP 11 Guidance
- Maintenance of the law and serious threat guidance: Final-Guidance: Releasing-personal-information-to-Police-and-law-enforcement-agencies
- Section 30: Office of the Privacy Commissioner | Section 30 Special Circumstances
- Heath Information Privacy Code 2020: Office of the Privacy Commissioner | Health Information Privacy Code 2020
- Codes of Practice: Office of the Privacy Commissioner | Codes of practice
- List of provisions and authorised information matching programmes: Office of the Privacy Commissioner | Information matching provisions

1 See Schedule 7 of the Privacy Act 2020.

# Primary legislation for sharing information

Primary legislation may authorise or enable agencies to collect, use, and disclose personal information for specified purposes.

## How primary legislation affects sharing

Primary legislation that authorises the collection, use and sharing of information will override the Privacy Act with regard to collection, use and sharing, although only to the extent that the primary legislation cannot be read consistently with the IPPs.

However, the remaining IPPs covering security, storage and accuracy will still apply to your information sharing activity.

The following sections set out some of the most common primary legislation used across the government sector to facilitate information sharing.

The first group of statutory provisions do not require agencies to share information, but they provide discretion to do so in appropriate circumstances, for sound public interest reasons.

Some provisions make it compulsory to share information when approached by the appropriate authority: see "Legislation requiring the sharing of information" section.

**Seek advice from your privacy, information sharing or legal teams on whether your agency has primary legislation that enables the sharing of information with other agencies, organisations, or individuals and how that legislation is applied in practice.**

## Oranga Tamariki Act 1989

The Oranga Tamariki Act authorises the sharing of information between agencies within the child welfare and protection sector and with 'Independent Persons' - those working within the child welfare and protection sector.

### Section 15

If you become aware that a child or young person has been, or is likely to be, harmed, ill-treated, abused, neglected, or deprived, or have concerns about the wellbeing of a child or young person, section 15 permits you to share information in good faith about your concerns with Oranga Tamariki.

You do not need to be working for a child welfare and protection agency or have the consent of the child or their parents/whānau to make a report of concern.

For more information about how to make a report of concern see: Report of concern | Oranga Tamariki.

### Section 66C

If you work in the child welfare sector you can use section 66C of the Oranga Tamariki Act to request and disclose information to support safety and wellbeing for children or young people (tamariki or rangatahi) to:

- prevent or reduce the risk of harm, ill-treatment, abuse, neglect, or deprivation for tamariki
- make or contribute to an assessment of risk or needs of tamariki
- make, contribute, or monitor any support plan for tamariki that is managed by Oranga Tamariki
- prepare, implement, or review any prevention plan or strategy made by Oranga Tamariki
- arrange, provide, or review services facilitated by Oranga Tamariki for tamariki or their whanau
- carry out any function in relation to a family group conference for tamariki in care or anything else related to the care and protection of tamariki.

You do not need the consent of the individual to share the information if the sharing is for one of the specified purposes under section 66C. Section 66K does require consultation with tamariki and rangatahi whenever practicable or appropriate to do so.

When sharing information using section 66C as the legal authority, you must believe on reasonable grounds that the sharing of information will assist the receiving agency for any or all of the purposes provided above. This applies whether you are sharing information proactively or whether you are responding to a request for information from a child welfare and protection agency or an Independent Person.

If you have received a request for information under section 66C but require more information before you can believe you have reasonable grounds to share, contact the requestor and ask for more information. If you are still unsure about whether you should share information using section 66C you should seek support from your privacy, information sharing or legal team.

It is important to remember that while section 66C authorises the sharing and use of information, the Privacy Act IPPs relating to security, accuracy, storage, and unique identifiers still apply.

### Guidance and resources

Oranga Tamariki has further guidance on sharing information using section 66C: Information sharing | Oranga Tamariki — Ministry for Children

## Family Violence Act 2018

The Family Violence Act authorises the sharing of information between agencies within the family harm sector.

If you work in the family harm sector you can use section 20C of the Family Violence Act to request and disclose information to:

- make or contribute to a family violence risk or need assessment
- make or contribute to making or carrying out of a decision or plan that is relation to or that arises from or responds to family violence
- help ensure that a victim is protected from family violence.

You do not need the consent of the individual to share the information if the sharing is for one of the specified purposes under section 20. However, provided it is safe to seek consent, it is often best practice to do so.

When applying section 20, you must believe on reasonable grounds that sharing information will or may help the receiving agency achieve one or more of the purposes above.

If you require more information before you can form a reasonable belief that the information sharing will fit with section 20, contact the requestor and ask for more information. If you are still unsure about whether you should share information using section 20 you should seek support from your privacy, information sharing or legal team.

While section 20 authorises the sharing and use of information, the IPPs relating to security, accuracy, storage, and unique identifiers still apply.

### Guidance and resources

The Ministry of Justice has further guidance on sharing information using section 20:
Information Sharing Guidance | New Zealand Ministry of Justice

## Sharing to support enforcement and regulatory functions

Primary legislation can also facilitate the sharing of information to enable agencies to undertake enforcement or regulatory functions.

In some cases, these legislative provisions will require an agency to create an agreement that documents the details of the sharing.

The Immigration Act 2009 is a good example of primary legislation that contains provisions facilitating the sharing of information for enforcement and regulatory purposes. Sections 301 to 306 set out when Immigration New Zealand can disclose immigration information, who it can be shared with and for what purpose.

The example below illustrates the Immigration Act provisions in practice:

### Passenger information collected by airlines

Airlines provide Advance Passenger Processing (APP) information about every passenger and crew member on their flights coming to or leaving New Zealand, including passengers who are only in transit. The information the airlines collect is shared with Immigration New Zealand (INZ). The sharing is authorised under section 303A of the Immigration Act 2009 and allows INZ to compare personal information it holds with APP information and load alerts into the system.

On this particular day at a check-in desk in Singapore a traveller has triggered an alert during the APP check as they have been found to have attempted to travel on false documents in the past. This has informed a 'do not board' message and the airline agent calls an Immigration Border Officer. The officer checks the documents, but it is not immediately clear they are false and she lets the traveller board. On arrival with increased scrutiny at the border it appears the traveller's documents are false and they are declined entry into New Zealand. The traveller is held until they can be put on a plane back to their country of origin.

At the time of the traveller's turn-around, biometrics are taken (fingerprints and face images) so that fingerprint checks can be done with other Five Eyes Partners. This prevents travellers excluded from one country from gaining entry to another country through false pretences.

## Legislation requiring the sharing of information

An agency's primary legislation may require you to share personal information for specific purposes.

Some examples of these types of legislative provisions include:

- Section 17B of the Tax Administration Act
- Section 66 of the Oranga Tamariki Act 1989
- Section 23 of the Data and Statistics Act 2022
- Section 619 of the Education and Training Act 2020
- Schedule 6 clause 2 of the Social Security Act 2018
- Section 20(1)(a) of the Children's Commissioner Act 2003
- Schedule 5 of the Pae Ora (Healthy Futures) Act 2022
- Section 20 of the Inquiries Act 2013

A notice requiring the provision of information:

- should be made in the prescribed form
- clearly identify the legal authority under which the notice has been issued
- clearly state the information you are required to provide and for what purpose(s).

When you receive a notice, you must provide the information requested to the issuing agency within the specified timeframe.

Record the notice and your response to the notice in the appropriate register.

**You should always seek advice from your privacy, information sharing or legal team if you have received a notice requiring you to provide information.**

The examples below illustrate when you may be required to share information.

Stats NZ are producing official statistics about child poverty. They have approached your agency because they need personal information you hold to produce these statistics.

**Do you need to provide this information?**

Yes you can. The Government Statistician can make mandatory requests for data if the data is necessary or desirable for official statistics. Your agency must comply with this request. Stats NZ has high standards for keeping information private, secure, and confidential. This includes enforceable requirements to keep data confidential, ensuring that Stats NZ won't publish statistics in a form that could reasonably be expected to identify the individual concerned.

Stats NZ will undertake a Privacy Impact Assessment (PIA) before they collect the data from your agency. The PIA will identify and assess privacy risks and ensure there are good practical measures in place to protect the personal information.

You have received a request for information about an individual from the Abuse in Care Royal Commission. The information requested includes personal information about the individual.

**Can you share this information with the requestor?**

Yes you can. The Abuse in Care Royal Commission has powers under section 20 of the Inquiries Act 2013 to collect information appropriate for the purposes of the inquiry. This means they can require any person to produce documents and provide information necessary for the Abuse in Care inquiry to identify, examine and report on matters in scope of the inquiry.

Given the sensitive nature of the information you should ensure that you share the information using a secure method to protect the personal information.

You have received a request for information about a number of individuals from the Chairperson of a Mortality Review Committee. The request is for personal information, including health information about the individuals listed in the request.

**Can you share this information with the Chairperson?**

Yes you can. Mortality Review Committees are set up under the Pae Ora (Healthy Futures) Act 2022, and Schedule 5 of that Act grant the Mortality Review Committee (or their appointed agent) the power to source any information relevant to their purpose.

Given the sensitive nature of the information you should ensure that you share the information using a secure method to protect the personal information.

# Document your legal authority

## Why you need to document your legal authority

Documenting the legal authority:

- ensures all agencies understand the lawful basis for the sharing
- allows others to raise queries if they think you're incorrect
- gives context for the other information in your documentation about what you're sharing, who you're sharing with and for what purpose.

## Check if you need an information sharing agreement

Some legal authorities require or permit sharing in very specific circumstances on an ad hoc basis. In these instances, it may not be necessary to have a full information sharing agreement. You can document your use of the legal authority in a different way.

For example, where information is being shared under section 66C of the Oranga Tamariki Act, it may well be sufficient to use the Oranga Tamariki section 66C request for information templates and to record your requests and disclosures in an appropriate register.

## Set up an information sharing agreement

If you're setting up an information sharing agreement to document your sharing, the legal authority is recorded in that agreement.

For guidance on how to develop an information sharing agreement see: https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/information-sharing/information-sharing-agreement/develop-an-information-sharing-agreement/.

**Remember, an information sharing agreement is not a legal authority to share information.**

# Consider if sharing is appropriate

## Consider whether you should share information

Once you have identified a legal authority that permits (but does not require) you to share information, stop and consider whether you should share.

Usually, the answer will be yes. However, it's worth asking the question. Some sharing may be legally permitted but still inadvisable or even unethical. For example:

- it may break promises
- damage trusted relationships
- cause unjustified distress.

## Help deciding whether to share

If you're concerned that sharing may create these kinds of problems, check with your privacy, information sharing or legal teams to help you make the right judgment call.

The Data Protection and Use Policy (DPUP) principles can help you to determine whether you should be sharing personal information for your intended purposes.

Your agency may also require your proposed information sharing activity to be subject to review, assessment and approval by an ethics committee. This usually happens when you want to collect and share personal information to support research and evaluation activities.

The following sections provide more information about DPUP and ethics committees and approvals.

## Data Protection and Use Policy

The Data Protection and Use Policy (DPUP) describes what 'doing the right thing' looks like when collecting or using people's data and information.

DPUP provides 5 principles and 4 guidelines. The guidelines describe good practice and ways you can apply the principles in practice. You can use the DPUP principles and guidelines to help you determine whether you **should** share a person's information.

You can learn more about DPUP and its application to sharing information here:

Data Protection and Use Policy (DPUP) | NZ Digital government

## Ethics approval

In some cases, projects will require an ethics approval. This is particularly common for research projects.

Research that is conducted unethically, including the unethical collection and use of information, can have harmful consequences for those involved. An ethics approval demonstrates that the research project is unlikely to have negative effects on people.

When you receive a request for personal information for the purposes of research (internally or externally) you should confirm whether the researcher has obtained approval from the relevant ethics committee.

There are several ethics committees in New Zealand and some agencies may have their own internal ethics committee and ethics approval processes.

### The Health and Disability Committees (HDECs)

The health and disability committees (HDECs) are Ministerial Committees whose function is to secure the benefits of health and disability research by checking that it meets or exceeds established ethical standards.

See: About the HDECs | Health and Disability Ethics Committees

### Institutional Ethics Committees

Institutional Ethics Committees are established and supported by the institution to which they belong, and they review research that is occurring within that institution. There are currently 13 Institutional Ethics Committees in New Zealand. These committees are approved by the Health Research Council.

See: Health research saves lives | Health Research Council of New Zealand (hrc.govt.nz)

### Government agency ethics committees

The following government agencies have have research ethics committees, lead data ethics advisory groups or provide guidance relating to ethics:

- Statistics New Zealand - Data Ethics Advisory Group - data.govt.nz
- Statistics New Zealand: The Interim Centre for Data Ethics and Innovation - data.govt.nz
- MSD - Research ethics - Ministry of Social Development (msd.govt.nz)
- Oranga Tamariki - How to access data for your research | Oranga Tamariki — Ministry for Children
- Te Whatu Ora Auckland - Ethics and regulatory | Te Whatu Ora Te Toka Tumai Auckland (adhb.health.nz)

Te Kāwanatanga o Aotearoa
New Zealand Government