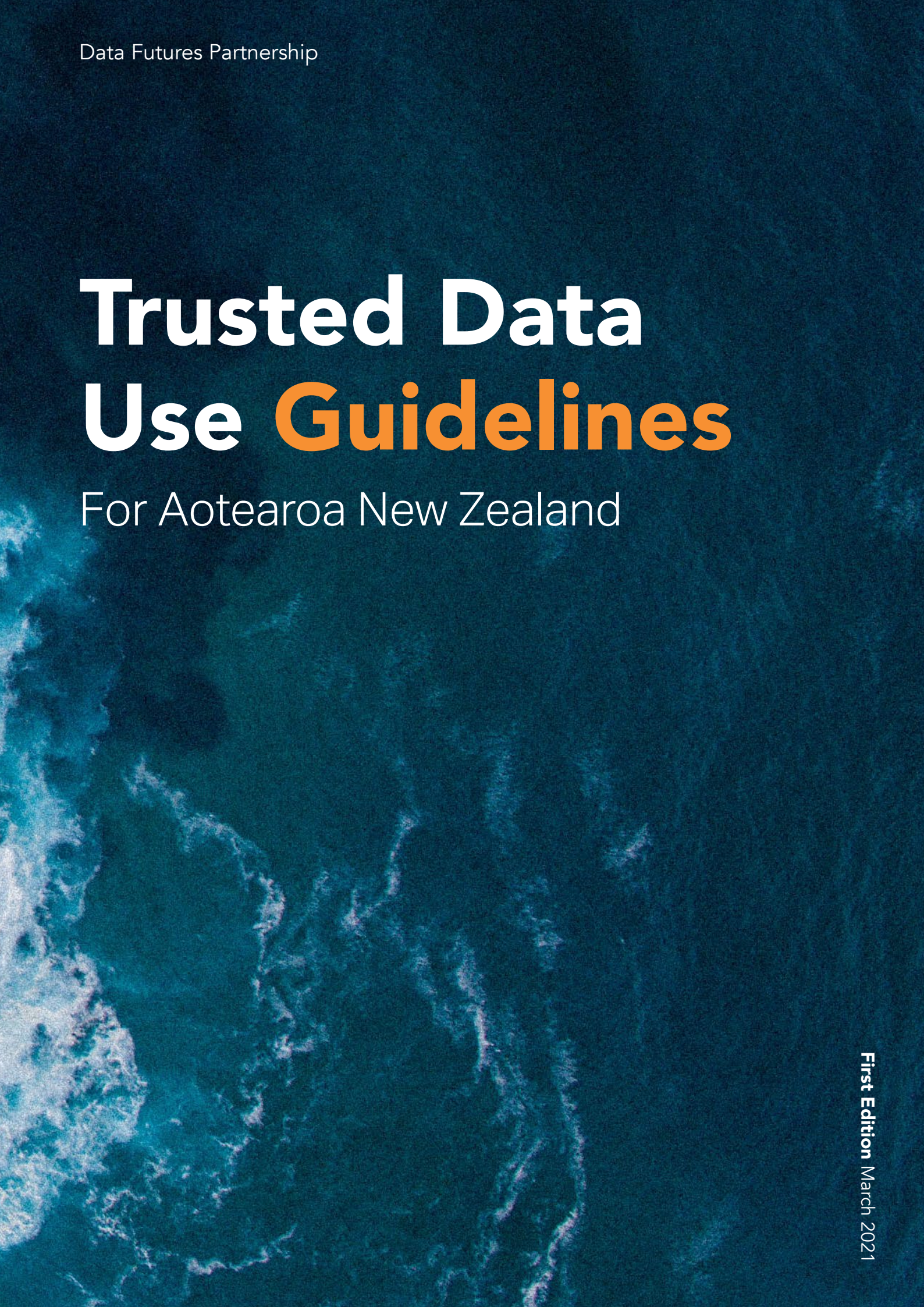
Data Futures Partnership

Trusted Data Use Guidelines

For Aotearoa New Zealand



First Edition March 2021

Contents

01 **Foreword**

02 **Section 1**
Who are the Guidelines for?

03 **Engaging with communities and building trust**

05 **Section 2**
Guidelines for trusted data use

09 **The Data Dial**

16 **Section 3**

18 Te Mana Raraunga — The case for cultural licence
20 Pasifika Futures — Dignity, respect and 'data'
22 HealthOne — Trusted data use

24 **Section 4**
Existing frameworks and useful links

Foreword

A message from the Chair of the Data Futures Partnership, Dame Diane Robertson

As an independent advisory body, the Data Futures Partnership was first tasked by the Government to draft guidelines for private and public organisations seeking to use New Zealand people's personal data.

We resolved it was vital that the draft Guidelines would be informed by the views of New Zealand people. That is why we commissioned open-ended and meaningful conversations with a broad cross section of New Zealand people and communities. This approach enabled us to understand people's levels of comfort with different types, situations and contexts of collection, use and sharing of their personal data — and what was needed in order for them to be more comfortable.

Both Māori and non-Māori frameworks were used to facilitate open conversations. Discussions with different groups of people across the country resulted in common ground being found on some topics — and, in contrast, strongly divergent viewpoints on others. People were generous with their time, and with their openness, frankness and reflection. Thank you.

Subsequently, conversations were had with a range of New Zealand organisations about the usefulness of Guidelines as they began to be used in context. I acknowledge the generous contributions of these organisations and their people, and the relationships that have been formed through this work. In particular, I am very grateful to the contribution made by Pasifika Futures: the Whānau Ora Commissioning Agency for Pacific families, and the partners of HealthOne; Pegasus Health, Orion Health and Canterbury DHB.

This updated edition of the guidelines contributes to a growing number of resources developed in New Zealand concerning data information, sharing and ethics. Many of the resources available have been developed 'for the sector by the sector'. These guidelines specify the questions New Zealand people want answered, the issues that matter to them and provide recommendations for the ways private and public organisations can respond.

There is a reason why the words First Edition appear on the cover. New Zealand people are clear that 'personal data' has many possible ways of being understood and many definitions — and that these are likely to change over time, and in different situations and contexts. They also told us that more work needs to be done to ensure that the needs of bicultural New Zealand, in a time of rapid cultural and demographic change, continue to inform the conditions under which data is collected, used and shared.

We offer these Guidelines as an initial step towards a uniquely Aotearoa New Zealand vision of people being at the centre of deciding how their data may be collected, used and shared. To remain relevant and meaningful, these Guidelines must continue to evolve and grow with us.

He aha te mea nui o te ao?
He tāngata, he tāngata, he tāngata.
What is the most important thing in the world?
It is people, it is people, it is people.

Dame Diane Robertson

Section 1: Who are the Guidelines for?

People of New Zealand

For New Zealand people, these Guidelines are intended as a tool to help them decide on their levels of comfort with any organisation's proposed use of data about them.

What is comfort? Comfort is defined here as a combination of two factors: the level of benefit that people see in a particular use of their data, and the level of trust that people have in the usage. Different people and communities will weigh up these factors according to their own worldviews and situations, but this simple framework has proven to be an accessible, understandable and practical way of finding out what matters to people when it comes to the use of data about them.

These Guidelines list the common ground questions that New Zealand people expect to have answered by organisations seeking to use personal data. The Guidelines also give people and communities an idea of when they should expect an organisation to consult more actively on current or proposed uses of data about them.

In the end, however, every person needs to decide for themselves if a data use provides sufficient levels of trust and benefit for them to be comfortable.

Companies, government agencies and non-governmental organisations

For New Zealand organisations seeking to use personal data, the Guidelines set out to promote practices that will improve levels of comfort among those individuals providing data, as well as in the wider community.

The Guidelines apply equally to:

- **Companies** that collect information about their customers and clients, ranging from, for example, highly personal health information in the case of private hospitals, to confidential financial information in the case of banks, to much less sensitive information about what people are buying at the supermarket.
- **Government agencies** that collect information from, for example, people applying for social welfare benefits, people registering their vehicle, people applying for state housing, or people using public health services.
- **Non-governmental organisations** collecting information on people using their services, such as budget advisory services, women's refuges, homeless support, or victim support services.

Engaging with communities and building trust

In 2016 the Data Futures Partnership sought the views of New Zealanders about data use, applying a social licence approach to understanding 'what matters' when it comes to New Zealand people being comfortable with data use. It defined social licence for data as follows:

> *When people trust that their data will be used as they have agreed, and accept that enough value will be created, they are likely to be more comfortable with its use. This acceptance is referred to as social licence.*

The intention was to understand levels of community acceptance of different kinds of data use, as a means of identifying what matters for data guidelines to cover. This approach yielded much common ground and a range of diverging views, as people were encouraged to consider the value of data use and their levels of trust. The national engagement included discussion about how the term 'people' should be defined for the purposes of social licence.

People: Individuals and communities

In our conversations with the people of New Zealand, they variously defined 'people' to mean the individual and collective, or whānau, or community, or nations of people. This was particularly evident where participants self-identified as Māori; and/or of Pacific descent; and/or people who are vulnerable, disadvantaged or at risk; and/or people who feel that their identities and situations make them more easily re-identifiable from anonymised or aggregated data.

Building community acceptance requires an understanding of how to define community and how communities define themselves. Communities can have a common cultural or historical heritage, or a specific locality. They can share government, social interests, religious proclivity or occupational cohesion, or other common characteristics or interests. Communities can have many different and connected parts.

Communities of New Zealand

In the process of developing the Guidelines, two overarching insights became apparent. First, Māori voiced a need — in accordance with Te Tiriti o Waitangi — to develop data guidelines or protocols using Te Ao Māori frameworks.[1] Second, many communities in New Zealand — including Pacific communities; people who self-identify as disadvantaged, vulnerable or at risk; and people who feel that their identities and situations make them more easily re-identifiable from anonymised or aggregated data — expressed the need for further work to be done to ensure their voices and worldviews are represented and respected in guidelines, protocols or approaches to data collection, use and sharing.

i. Māori

The Data Futures Partnership commissioned Tūhono Trust to undertake an initial engagement with Māori on the concept of social licence. The Trust noted that "implementing social licence would benefit from further research into... benefits to Māori and all New Zealanders of introducing a social licence regime." The Trust's insights, which have informed this first edition of these Guidelines, include the following:

Conditions relating to sharing information

- Māori have a higher level of discomfort when sharing private information compared to anonymised information and a desire to have full control over who private information should be shared with, if at all.

Guidelines and protocols are essential

- A kaupapa Māori framework should be used to develop guidelines and protocols for organisations wanting to use and share information, in accordance with the Te Tiriti o Waitangi.

Collective wellbeing and cultural networks are equally important when sharing information

- Individual and collective wellbeing are equally important for Māori, and sharing information with their cultural networks is important.
- Māori have a higher level of trust and confidence when sharing information with iwi than when sharing with government entities, community organisations and businesses.

[1] P.4 in Sharing Information for Wellbeing: Māori Engagement on Social License (2017) prepared by Tūhono Trust for Data Futures Partnership, June 2017.

Multiple engagement strategies to connect

- To effectively capture the voice of the people, find common ground and key themes, and gauge insights into the thoughts and opinions of people, multiple engagement channels are needed to maximise the opportunity to participate.

In response to these findings it was decided that a formal Crown/Māori conversation around Māori Data Governance in Aotearoa New Zealand should take place. It is hoped this will occur in the near future.

ii. Pacific

People self-identifying as being of Pacific descent who participated in the national engagement programme commonly raised questions about the cultural context of data use, including:

- What 'data' actually means to Pacific people.
- The importance of cultural values and trusted relationships to data collection, use and sharing.
- Concerns about how Pacific data is interpreted outside of a Pacific context.
- Concerns about Pacific data not being used at a local level to benefit Pacific families and/or being used to inform wider deficit approaches to services for Pacific people.

iii. People who are disadvantaged, vulnerable or at risk

People who self-identified as being disadvantaged, vulnerable or at risk commonly raised questions about various contexts of data use, including:

- Concerns about information being used to harm rather than to benefit them and/or their families and communities.
- Concerns about being re-identified from anonymised or aggregated information.

iv. People who feel that their identities and situations make them more easily re-identifiable from anonymised or aggregated data

People self-identifying as having a disability, belonging to a small sub-population, living in less populous settlements, or otherwise perceiving themselves to be easily identified, commonly raised concerns about being re-identified from anonymised or aggregated data.

Each of these New Zealand communities has an expectation that their cultural and/or contextual concerns around data use will be considered by organisations collecting, using and sharing data about them. Future leadership and widespread participation of these communities in forming guidelines, or other protocols designed to alleviate these concerns, is highly recommended.

Building Trust

Building trust goes to the heart of the successful achievement of community acceptance, and to the effective use of these Guidelines. People's comfort with different uses of data about them can change over time as they experience, hear about and discuss real-life instances and outcomes — both positive and negative — of data use and sharing in Aotearoa New Zealand and in the world.

Sometimes, providing answers to the basics around responsible data use — transparency, accountability and control — may not be enough. For instance, the level of trust in data use may be more difficult to obtain when an organisation makes a significant change to the types of data it collects, how it collects it, or how data is used. In these situations organisations should consider proactively engaging with the communities affected.

This community engagement needs to be authentic and involve not just those people whose data is being used, but broader communities who might be indirectly affected by the proposed data use. Organisations need to establish trust, build relationships and listen to what these communities have to say about the current or proposed use of data and make changes if those communities are not comfortable.

It is clear that people in Aotearoa New Zealand feel there are many aspects of data use that are yet to be resolved — and that this process will necessarily be ongoing as data use is changing. These Guidelines should therefore be viewed as a first step along the path of developing guidelines and/or wider protocols that are authentic and relevant to the people of Aotearoa New Zealand.

Section 2: Guidelines for Trusted Data Use

These guidelines have been informed by conversations with New Zealand people and communities, and with different kinds of organisations that collect, use and share data about those people — and with reference to international developments in data guidelines where these apply. The objective has been twofold:

1. To understand common and distinct needs and expectations that New Zealand people have when it comes to organisations collecting, using and sharing data about them.
2. To understand the expectations that different types of organisations have of guidelines which set out to help them use and share data in ways that are acceptable to New Zealand people.

The structure and content of these Guidelines has been built with the findings from open-ended conversations about data. Two programmes of engagement were undertaken — one engaging with Māori, the other engaging a broad cross-section of New Zealand people including Māori. Links to full reports from these engagements can be found on the back page of this document.

New Zealand people told us the features of personal data use and sharing which matter most to them. For people to feel comfortable with current or proposed data use, the eight questions, set out in the guidelines, have been agreed as key areas that need to be responded to.

In conversations with New Zealand people it became clear that comfort with data use goes further than complying with regulations such as the Privacy Act. They want respectful and trusted use of data and information about them. That is why the Guidelines are organised around eight key questions that New Zealand people want answered concerning responsible data use, particularly with regard to expectations of transparency, accountability and control.

The use of the first edition of these Guidelines, set out under each question, will determine how comfortable people are about the use, or proposed use, of their data. Following the guidelines will lead to data practices that are likely to be trusted by most New Zealand people.

Laying the foundation

First explain why it is necessary for the data to be collected, shared or used.

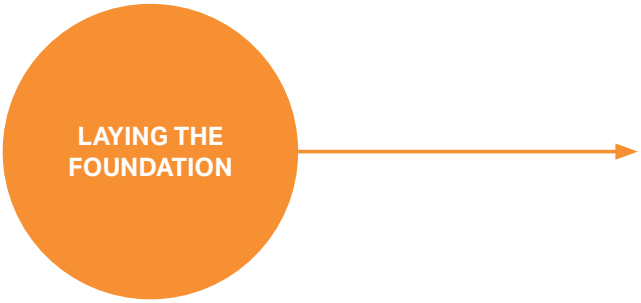
People expect to understand why their data is being collected, shared or used. Organisations need to provide clearly articulated reasons for collecting, sharing or using personal data, and communicate these reasons clearly to the people whose data they are using.

Different organisations will have different purposes for collecting, using and sharing data. These need to be clearly stated in order that New Zealand people can determine how comfortable they feel about data about them being used.

People want to know that by sharing personal data, they (and others) will benefit, and will not be disadvantaged in any way. This requires trust that the organisation collecting their personal information will use it to 'do what is right' by them and their community. When people are comfortable that they can trust an organisation, they are more likely to be comfortable with the collection, use and sharing of data about them.

While individuals expect their data will be treated with privacy and confidentiality they also desire respect and consideration at a human level. When they feel these factors are being acknowledged, they are more likely to have a higher degree of comfort.

An explanation for why the data is being collected, shared or used must be outlined before moving onto the following eight questions.



How to approach the eight questions

Acceptance of current or proposed data use depends on whether it offers sufficient value, protection and choice for those being asked to provide data and for the wider community. New Zealand people and organisations dealing with data about people need to provide accessible, non-legalistic answers to the following questions. Organisations will have different legal requirements and the questions will enable them to explain their responsibilities when dealing with personal data.

The following prompts are suggested when thinking about how to respond:

- To maximise trust in how you are collecting and using personal information, follow the guidance provided under each question as set out below.
- Provide the answers in a way that is simple, straightforward, and easy to access. Do not bury the answers in complex, lengthy Terms and Conditions Statements or Privacy Statements.

Eight Questions

What, who and how

What

1 What will data about me be used for?

Who

2 Who will benefit and in what way?

3 Who will be using data about me?

How

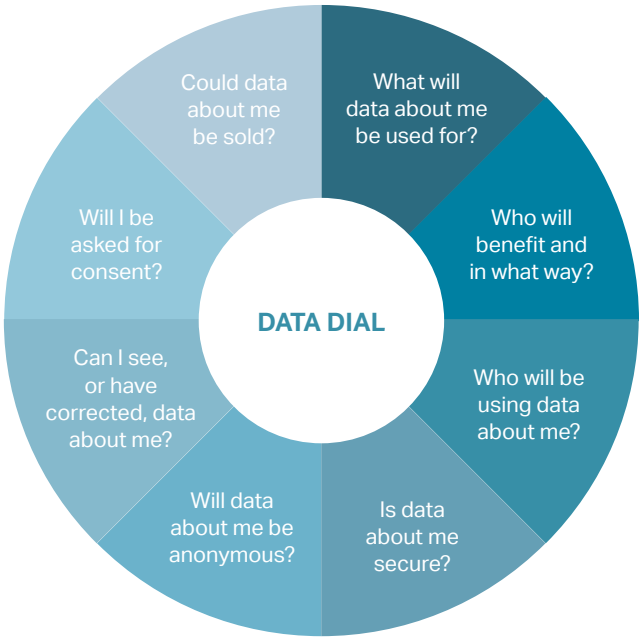
4 Is data about me secure?

5 Will data about me be anonymous?

6 Can I see, or have corrected, data about me?

7 Will I be asked for consent?

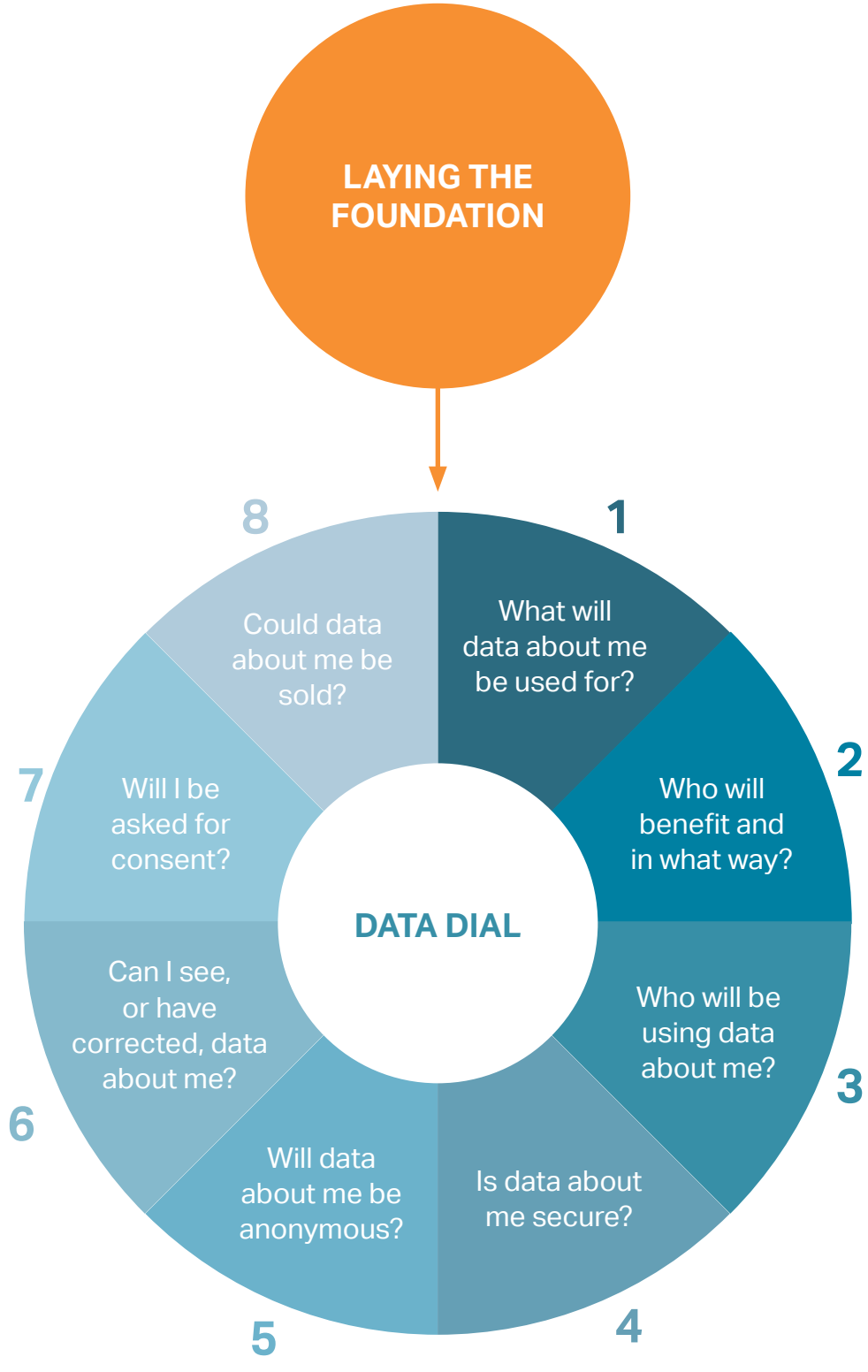
8 Could data about me be sold?



The Data Dial

The Data Dial presents the eight questions in an easily understandable form, and emphasises the importance of first explaining why the data is being collected — 'Laying the foundation' (see page 5).

Detailed explanations of 1–8 are provided on the following pages.



1

What will data about me be used for?

People expect to be clearly informed about the purpose of the data collection in specific and detailed terms. People tend to be more comfortable when data is used in context, as a necessary part of delivering a product or service.

Use of data

A. Explain clearly how the data being collected will be used. For example:

- We will use your information to target marketing to you. We will also share it with the companies in our loyalty programme, and they will use your information to target marketing material to you by email.
- We will provide your information to charities so they can approach you for support.

Provide further detail with concrete examples for people who are interested. Examples might include ways you have used research to improve services in the past. If you can, provide the more detailed information as a click or drill-down option so that it can be skipped by people who are interested in only more general statements about purpose.

When the data is sensitive, or New Zealand people are likely to have a low level of trust in your organisation, explain why it isn't possible to achieve the purpose in any other way (for example, by using anonymous instead of personally identified data).

Data being collected

B. List what data you are collecting. This would encompass all or some of the following:

- Where collection of personal information is required, do so only where it is necessary for a lawful purpose connected with the functions or activities of your organisation or agency.
- Information beyond that needed for service delivery or authorised under legislation (e.g. collected for marketing or research purposes, or for an anticipated future use).

— Describe the purpose.

— Be explicit about any incentives you are offering in exchange for gaining the right to use customer/client information.

— Enable people to easily opt-out of providing this sort of information.

— See Principle 1 of the Privacy Act 2020 for more detailed information.

Linked Data

C. When using linked data, explain what other data will be used and where it comes from.

Data on individuals can be matched across datasets to give a larger, richer set of information (e.g. for research or statistical purposes). Data can also be linked to enable personal identification of an individual, and therefore the ability to approach individuals for a variety of purposes (for instance, offers of services, advertising or requests for donations).

When an organisation intends linking the data being collected with data already held, or data intended to be obtained from another source, explain what other data is intended to be used and where it comes from.

Algorithms

D. If you use algorithms (formula-based decision tools) explain how these work and which pieces of data are used.

Algorithms can be used to make decisions, for example, to determine whether to grant loans, what interest rate to charge, or as part of a recruitment process:

- Advise clients of other inputs to your decision processes (e.g. does a staff member review applications?)
- Offer the applicant the right to contest the decision, including the data that was used in the algorithm.

Future uses

E. State clearly if the data might be used for other purposes in the future and, if so, what other purposes.

If potential future uses are intended, explain what the future use is (or could be) and why it is important.

If you aren't able to be precise or certain about possible future uses, you may still need to consider issues of consent and how you might obtain this.

2

What are the benefits and who will benefit?

People want to know what the benefits are from a particular data use and who benefits. When personal data will be used as a product in its own right for commercial gain, organisations should explain what the person is gaining in exchange, and what the business is gaining.

Expected benefits

A. Explain what benefits the individual, whānau, organisation or iwi can expect. Also explain any wider benefits (e.g. to a larger group such as society in general).

Be specific and provide evidence about how the proposed data use will lead to the benefits claimed.

Proven outcomes are the best way to demonstrate benefits. Provide an example of a similar data use and the resulting benefits or a concrete example of an expected benefit from the proposed use.

Exchange of benefits

B. Explain what benefits are being offered in exchange for the use of personal data (e.g. free services or access to services at a lower charge).

When personally identifiable data is collected to target people for direct marketing and advertising, the benefit accrues mainly to the company as profit. Therefore, people's level of comfort is likely to be less, and people may expect to receive significant personal benefit.

Explain whether other organisations are benefiting from the personal data, including which organisations and how they are benefiting.

Give people the ability to opt out of direct marketing and advertising that uses their data. Make information about this option easy to find and make it easy to opt out.

3

Who will be using data about me?

People want to know who will be using or sharing data about them.

Using data within an organisation

A. Explain which parts of the organisation will be using the information and for what purposes.

Sharing data with another organisation

B. State clearly if you will, or will not, be sharing the data with any other organisations.

Identify any data that will be shared with other organisations; which organisations and for what purposes.

4

Is data about me secure?

People want to know that organisations using and sharing (or intending to use and share) their data have rules and controls to minimise the risk that data is mishandled.

Using data within an organisation

A. Build data protection safeguards into your organisations' use of personal data from the earliest stages of development.

Outline the measures you have to keep data secure and measures taken by the organisations that you will share data with. Where data is sensitive and personally identified, include:

- Which types of personnel will have access to the data and their credentials (e.g. their training, that there were referee checks, and that they have signed declarations of confidentiality).
- The access rules and protocols in place and the consequences for staff who break them.
- Security arrangements that prevent unauthorised access to the data.
- A date for the destruction of data after use.

Inform people what will be done if there is a data breach. Ideally, if there is a data breach, people affected should be informed as soon as possible to give them the best opportunity to protect themselves.

5

Will data about me be anonymous?

In many cases, data must be personally identified in order to achieve the purpose of delivering a service or product. Data which allow the names, addresses, or other identifying information of a person to be readily established are deemed 'personally identified data'. People are willing to have their personally identified data shared in a limited way when they can see significant benefits from the data use and have trust in who will use it.

Anonymising data

A. Unless data needs to be personally identified to achieve its purpose, always use anonymous data.

When you intend that data will be anonymous, rather than a guarantee, many people may be satisfied with a high-level assurance, such as:

> *We use data in a form that does not identify you personally, and we do not use it to target you or other individuals. While it may be theoretically possible to re-identify you from the data we hold, we take several measures to make that highly unlikely.*

For people with a greater level of concern, or where the data is more sensitive, describe the measures you have in place to reduce the risk of individuals being personally identified, but stop short of providing a guarantee. Include:

- Techniques you are using that make re-identification more difficult, such as encryption, pseudonymisation (e.g. where names are converted into unique numbers), data being analysed at an aggregated level, and adding 'noise'.
- Controls on who will be able to access the data and for what purposes.
- Assurances about sharing the data — with whom and for what purpose.
- Assurances about linking the data with other datasets and steps to minimise the risk of re-identification.
- Assurances that the people accessing the data are prohibited from attempting to identify individuals.
- A date for the destruction of data after use.

Provide these details through an online link that allows people to drill down if they want more information. This will avoid your statement appearing too long and complex. People who already have a high level of trust in your organisation and the proposed data use are unlikely to need this further detail.

6

Can I see, or have corrected, data about me?

People want to be able to find out what information is held about them, by whom and for what purpose. If an organisation makes a commitment to providing people with the data it holds about them, trust in the organisation will increase. An ongoing audit trail, showing how information has been shared and used over time, should be available on request.

People also want to be able to correct wrong information about them. Incorrect information in data repositories can be extremely damaging to the individuals or families concerned.

If you have shared the data with another organisation check to see whether you can help with requesting deletion of the data from that organisation.

In other situations, a lower standard of access to and ability to correct or delete data may be acceptable, provided all requirements under the Privacy Act 1993 are met.

People's ability to see data about them

A. Explain how people can find out what data is held about them, by whom, for what purpose and how it is used and shared.

Explain any circumstances in which data held about an individual will not be provided. Rather than list the exceptions in the Privacy Act 1993, explain the circumstances in which your organisation will not provide data.

People's ability to have data about them be transferred

B. Be clear about whether you are willing and able to transfer data to another organisation at an individual's request.

People's ability to have data about them corrected

C. Correct data inaccuracies in accordance with the listed actions.

Recommended actions for correcting inaccuracies are to:

- Provide a phone number that will directly connect an individual with someone qualified to deal with sensitive requests.
- Put suitable safeguards in place to prove that the person requesting the information is the person to whom the data relates.
- Act promptly on requests to correct data.
- Establish a process, with a timeline, for responding to requests for corrections, and share this proactively with people. This process needs to include how data that has been shared with another organisation will also be corrected.
- Explain how you will be accountable for any failures to correct wrong information, including the consequences if your organisation disregards requests to correct information.
- Offer to meet with any person who has requested a correction that you will not or have not acted on. This provides an opportunity for you to discuss your reasons and for the person seeking a correction to explain their situation.

7

Will I be asked for consent?

Consent practices

A. People are likely to expect:

- To be notified before any new data use or sharing occurs.
- Clear time limits on permission.
- To be able to withdraw consent in the future and have their information deleted.

New Zealand law does not depend on consent as the primary authority for collecting, using and disclosing personal information. The main driver is the legitimate business purpose of the holder of the information. Nevertheless people want the ability to give permission for specific data to be used by specific organisations for specific purposes.

It is common for consent to be asked for as part of long, legalistic statements of terms and conditions. Or for Privacy Statements to be in small font at the back of a form. These statements are frequently skipped over by people wanting to access the service or product on offer, raising the question of whether 'consent' in these circumstances is genuine or communication has been clear.

Meaningful consent practices present a valuable opportunity to communicate clearly with those who are trusting you with their personal information.

Obtaining consent

B. It is desirable to explicitly ask for consent to use data about individuals, even when the data is anonymised (in most cases).

- Ask people to give consent through a positive action (e.g. by ticking a box or clicking an 'I agree' statement).
- Do not presume consent simply because an individual has used a service (e.g. used a loyalty card, made a purchase on line, or visited a website). This applies even if you have advised people of your policy on your website or on paper.
- Make the request for consent short and easy to understand and display it separately, rather than as part of a lengthy terms and conditions statement.
- Give people as much choice as possible about which organisations will use the data and for what purpose. Make it easy for people to adjust their choices over time.
- Make it simple for people to tell you if they no longer consent to you having data about them. Be clear about whether you can delete the data or not.
- Where people are in vulnerable situations (for example, a person using a rape counselling service or a women's refuge), it is especially important to limit the initial data collection to the minimum needed for service delivery. Issues of data use and consent should be addressed at a later stage, such as when the client has finished with the service and can feel free to refuse the request.
- When the information being collected relates to a child or a young person ensure they understand and have support to understand (or if they are very young, or unable to understand, ensure that their representative, parent, guardian, or caregiver understands):

— what will be shared and why.
— who it will be shared with.
— any possible decisions that might be made with the information or other outcomes.
— consequences of sharing.

Be clear about the scope of the consent you are seeking

C. Ensure consent is well designed by answering all key questions in the Guidelines and making these answers readily available.

Be clear about when people have a choice and when data provision is a condition of receiving the service or product. Use the following three categories.

- Data you are requiring as a condition of supplying the service or product. In most cases, this should be only the data that is strictly necessary for the service.
- Data elements beyond what is strictly needed for service delivery, but is authorised under legislation. Be explicit about any consequences of not providing this additional information.
- Information beyond that needed for service delivery or authorised under legislation (e.g. collected for marketing or research purposes, or for an anticipated future use).

Consider seeking this information, and consent for its use, separately. In some cases, this might be best done after the service or product has been delivered.

Be explicit about any incentives you are offering in exchange for gaining the right to use customer/client information.

Enable people to easily opt-out of providing this sort of information.

8

Could data about me be sold?

People are concerned about the potential for personal data about them to be sold. Selling personal data without explicit permission can severely undermine trust.

Under the Privacy Act 1993, 'personal information' (that is, information about an identifiable individual) can be disclosed only in limited circumstances. However, even the sale of non-identified information could be of concern, so organisations need to clearly state when they sell data.

If your organisation will under no circumstances sell personal data — information about individuals, whether personally identified or not — state this clearly.

Some organisations, especially government agencies and NGOs, feel that even by raising the issue of the sale of personal data may give the impression that they would sell data, even although such an action would never be contemplated.

In these cases, although reference to the sale of data can be left out, we recommend making it clear that your organisation would never sell any data about its clients.

Personally identified data

A. If the data you collect from people could be sold in an identified form, seek consent unless the sale is part of the sale of a business as a going concern.

If a business is being sold as a going concern, advise customers and provide an opportunity for them to opt out of the customer database.

Non-identified data

B. Data sold in an anonymous form could be linked or matched with other data that could make it personally identifiable.

If you intend selling anonymous data:

- Tell customers who the data is being sold to and for what purposes (for example, marketing).
- Seeking consent first is preferable.

Displaying the answers to the eight key questions

It is recommended that organisations display the answers to the eight key questions (online or on paper) in an easy way for people to find the answers they want.

The consistent use of these eight questions is recommended so that New Zealand people understand how data about them is used and shared and can quickly and easily access the information they want. However, organisations are free to use only some of the questions or add questions they know are important for a particular data use or client group.

Where an organisation uses data in only one way or in very similar ways over time, showing their answers to the eight questions once is sufficient. Organisations using a variety of data sources for varying purposes should complete the eight questions for each distinct use of data, including new uses.

If presented online, answers to the eight questions should allow people to choose what they are interested in and drill down as needed to access second and even third layers of information. At each layer they receive more in-depth information about each specific aspect of the data use.

While most users, in most cases, don't want to know all the ins and outs of how data about them is being used, there is a benefit from the 'visibility' provided by the eight questions. New Zealand people want to be satisfied that if they did want to know all the ins and outs then they would be able to find this information easily. Visibility provides people with the confidence that when and if there are problems with a data use, those will be quickly spotted by journalists, privacy activists, experts or regulators.

Section 3:

This section provides three approaches and contexts to enable these guidelines to be viewed from different cultural viewpoints and organisational structures.

The first approach: Te Mana Raraunga

The first approach offered here is shared by Te Mana Raraunga — the Māori Data Sovereignty Network. The Network comprises a group of researchers and practitioners that advocate for Māori rights and interests in data. It provides another approach — cultural licence — when thinking about group acceptance for data use for Māori. This includes: data rights and interest; governance; storage, security and collection; and access and control. It provides an outline of their Network's purpose, principles and audit tool.

The second approach: Pasifika Futures

The second approach presents a Pacific organisation's experience of applying the data use guidelines. Pasifika Futures — a Whānau Ora commissioning body, offer how they might use and implement these guidelines with communities. They provide a set of cultural expectations, with conditions and obligations around how their stories (data) may be used and shared. They provide a culturally informed framework for data use to provide improved outcomes for Pacific families using the values of respect, dignity, reciprocity and partnership.

The third approach: HealthOne

The third approach is an 'in practice' assessment of the guidelines by HealthOne. HealthOne provides a secure record that stores patient health information currently used in the South Island of Aotearoa New Zealand. HealthOne is operated in partnership by Pegasus Health, Orion Health and the Canterbury District Health Board. This 'in practice' assessment responds to the eight questions laid out in the Data Dial and presents these in an easily accessible language.

Te Mana Raraunga
The case for cultural licence

Cultural licence

Māori, like other indigenous peoples, have often been the targets of exploitative and stigmatising data practices. Te Mana Raraunga asserts that for Aotearoa New Zealand to become a world leader in the trusted use of shared data, it also needs to become a world leader in the trusted use of indigenous (Māori) data. It sees this as a significant opportunity and challenge for government.

Te Mana Raraunga distinguishes between social licence and cultural licence. Their view is that social licence is not a sufficient mechanism for consent in the context of indigenous data. Group acceptance through mandated structures is a more appropriate barometer of trust for data that can be aggregated to represent a group. This is particularly important for any Māori collective (e.g. whānau, hapū, iwi) that has an interest in aggregated data sets as a counterbalance to the significant collective risks.

The role of both individual and collective consent is already a recognised component in the ethical consideration of health and social research in Aotearoa New Zealand. Te Mana Raraunga's view is that while individual views contribute to social licence, cultural licence acknowledges the distinctive rights and interests of iwi/Māori as Treaty Partners, and iwi/Māori aspirations to derive equitable benefits from data.

Māori data governance is one of the key mechanisms through which to address cultural licence. Te Mana Raraunga has developed a number of useful tools and frameworks that can be formally adopted by organisations including a charter, Māori data sovereignty principles, and a Māori data audit tool. The charter and principles provides the key elements to become a Māori data sovereignty organisation, and the data audit tool provides a way to assess organisational responsiveness.

The charter was formally approved by the network in 2016. The charter's preamble and statement of purpose frame Māori rights in relationship to data.

Preamble

With respect to the inherent rights that we as Māori have by virtue of our inalienable relationships with the land, water and the natural world, we assert that:

- Data is a living tāonga and is of strategic value to Māori.
- Māori data:
  - refers to data produced by Māori or that is about Māori and the environments we have relationships with;
  - is subject to the rights articulated in the Te Tiriti o Waitangi and the United Nations Declaration on the Rights of Indigenous Peoples, to which Aotearoa New Zealand is a signatory.
- Data sovereignty typically refers to the understanding that data is subject to the laws of the nation within which it is stored.
- Indigenous data sovereignty perceives data as subject to the laws of the nation from which it is collected.
- Māori data sovereignty:
  - recognises that Māori data should be subject to Māori governance;
  - supports tribal sovereignty and the realisation of Māori and Iwi aspirations.

Charter available at:
www.temanararaunga.maori.nz

Te Mana Raraunga: Māori Data Sovereignty Network is an independent group of Māori researchers and data practitioners that advocate for Māori rights and interests in data. The network is open to participation from Māori and iwi data users, ICT providers, researchers, policymakers and planners, businesses, service providers and community advocates that share their charter.

TE MANA RARAUNGA
Māori Data Sovereignty Network

Purpose

Te Mana Raraunga advocates for resources to support the development of capacity and capability across the Māori data ecosystem including:

- Data rights and interests; establishing the nature of Māori rights and interests to government collected administrative data, survey, census and research data derived from indigenous tāonga is central to realising aspirations in the Mataatua Declaration, the WAI262 claim, and the United Nations Declaration on the Rights of Indigenous Peoples.
- Data governance; ensuring Māori involvement in data governance and data management, which is essential to ensure data is used for projects that support beneficial outcomes for Māori.
- Data storage and security; supporting the development of Māori data infrastructure and security systems to support the realisation of Māori data sovereignty.
- Data collection, access and control; Māori should be involved in decisions about the collection of and access to Māori data, analysis and interpretation.

M□ori data sovereignty principles

Te Mana Raraunga has also published Māori data sovereignty principles to guide the ethical use of Māori data. There are 16 specific principles underpinned by six broader Māori values of rangatiratanga (authority), whakapapa (relationships), whanaungatanga (obligations), kotahitanga (collective benefit), manaakitanga (reciprocity) and kaitiakitanga (guardianship). Of particular relevance here are the principles relating to control, balancing individual and collective rights, accountabilities and consent.

Principles available at:
www.temanararaunga.maori.nz

M□ori Data Audit Tool

The Māori data audit tool helps organisations assess their responsiveness to Māori data through the following questions;

1. Does the agreement recognise Māori data (what Māori data encompasses)?
2. Does the data sharing agreement allow the creation of additional Māori-specific/iwi-specific data sets?
3. Does the agreement recognise Treaty relationships?
    a. Are Māori/Iwi involved in the governance?
    b. Are Māori/Iwi involved in the data sharing approval process?
    c. Are Māori/Iwi involved in decision-making for issues that have been escalated?
4. Does the agreement recognise Māori rights to data and interests in data?
5. What mechanisms are in place to protect Māori data?
6. Is the agreement specific about the purpose and use of data?
7. To what extent are the Te Mana Raraunga principles given effect to?

Pasifika Futures
Dignity, respect and 'data'

Pasifika Futures was invited to put to work a draft version of the Guidelines for Trusted Data Use in Aotearoa New Zealand to see how they performed in practice. "For Pasifika Futures, data and evidence is essential to enabling over 14,000 Pacific families to achieve their aspirations," explains Seini Jensen, Director of Performance and Evaluation. "It enables Pacific families to achieve their goals and aspirations and improve their wellbeing and prosperity outcomes." Pasifika Futures invited researchers from Toi Āria: Design for Public Good at Massey University to participate in a series of Talanoa with a cross-section of staff from Pacific Whānau Ora providers, to explore how the guidelines might work in practice.

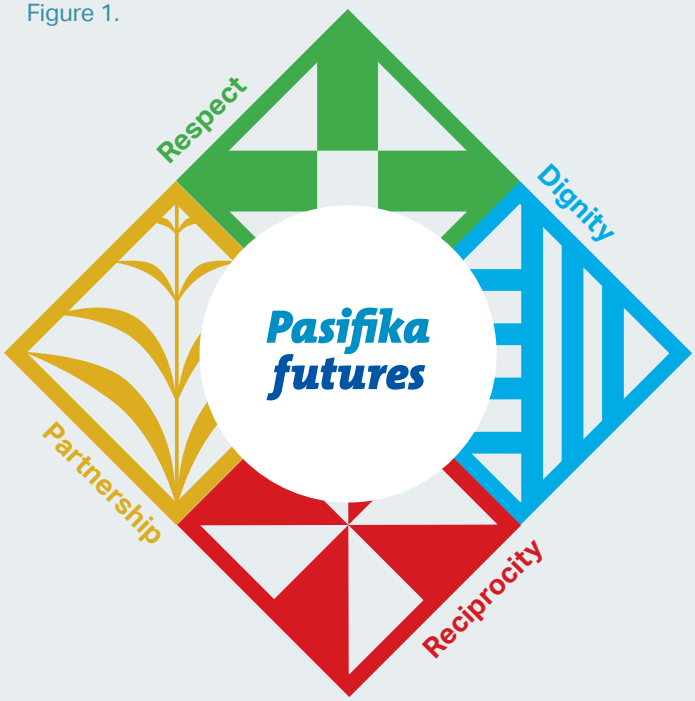
The key finding was that without specific consideration of Pacific cultural contexts, the eight questions in the guidelines provoked more questions than answers. "Many of the conversations didn't get past the word 'data' itself. The term obscures the real nature of the information that is collected and used — which is Pacific families' stories. The people who work with families build incredibly close and trusting relationships with them, and they emphasise that this intimate dialogue — Talanoa — brings with it a raft of cultural expectations, conditions and obligations concerning how those stories may be used and shared".

For Jensen, to address the eight questions posed by the guidelines it is important to know more about how data gathered from Pacific families would be interpreted and used for decision-making by government and other organisations outside of the Pacific community. There is a cultural obligation to honour the expectations of the families contributing the data. "The absolute foundation of being able to use Pacific families' data is a trusting relationship founded on common Pacific cultural values." Based in part on the findings of the Talanoa series, Pasifika Futures articulated these cultural values as they apply in practice to Pacific people's data (see figure 1).

What is Talanoa?

"Talanoa is a traditional word used... across the Pacific to reflect a process of inclusive, participatory and transparent dialogue. The purpose of Talanoa is to share stories, build empathy and to make wise decisions for the collective good. The process of Talanoa involves the sharing of ideas, skills and experience through storytelling... Talanoa fosters stability and inclusiveness in dialogue, by creating a safe space that embraces mutual respect for a platform for decision making for a greater good."
United Nations Climate Change: 2018 Talanoa Dialogue Platform

Figure 1.



About Pasifika Futures

Pasifika Futures Limited (PFL) is a Pacific owned, governed and led charitable company, founded by the Pasifika Medical Association. Its vision is to see prosperous Pacific families living longer and better lives, succeeding in education through lifelong learning, having financial freedom and leading and caring for families, communities and country. In 2014 PFL was appointed as the Whānau Ora Commissioning Agency for Pacific families in Aotearoa.

Respect

Respect in using and making sense of data requires understanding the data and the cultural and relational context in which it is situated. It is about: placing families at the centre of decision making and acknowledging their cultural context; acknowledgling the owners of the data are Pacific families and people who share it; understanding and responding to cultural protocols, hierarchies and context; and ensuring families understand how and why the data is being collected and how it will be used and shared.

Dignity

Enhancing dignity of Pacific peoples in all aspects of data collection, use and sharing requires that it is used to empower Pacific people and families to achieve their goals and aspirations. Dignity requires acknowledgement of the strengths and aspirations of Pacific families, while deficit framing and analysis diminishes the dignity of the owners of the data — Pacific people.

Reciprocity

Reciprocity is understanding and communicating clearly that data collected from Pacific peoples and families must benefit Pacific families and communities. When Pacific families share data and knowledge through Talanoa, a reciprocal relationship is created, with an expectation that the data is used to benefit Pacific families and will support them to achieve their aspirations and improve their outcomes.

Partnership

Partnerships between Pacific people and organisations are essential if data about Pacific people is to be used to enable and support Pacific people and families to achieve their aspirations. For respect, dignity and reciprocity to be maintained, there must be a trusted relationship with the organisation to whom data is shared. Partnership is created when stories are shared, questions are answered, assessments and registration forms are completed.

Debbie Sorensen, CEO of Pasifika Futures, says that while these values firmly guide her organisation's approaches to data collection, use and sharing, the practices of many organisations fall short. "Our experience is that Pacific people's information is gathered and used to serve decision-making that is far removed from the lived experiences of our communities", she says. "Because of this, Pacific people's data can be used to inform or legitimise decisions that don't actually benefit the people and families from whom that data came. A common outcome of that decision-making is deficit-based services that actually harm our people."

Sorensen sees an ongoing process of involving Pacific people in development of culturally-informed guidelines for their data as being crucial. "Guidelines have to start to engage and talk about culture and values, otherwise they are not realistic or useful. Guidelines that reflect cultural values will provide validation for our people and their practice — and at the same time, help non-Pacific organisations and entities to collect, use or share Pacific peoples' data in ways that affirm our people and the values they live by. Pacific people will need to lead this process. Their leadership is critical. Otherwise guidelines won't be effective or impactful."

She adds: "There has to be true partnership with the organisations using the data. We need to influence government agencies in particular, at a whole number of different levels, to ensure that data about Pacific people is used to improve outcomes for Pacific families".

HealthOne
Trusted data use

What is HealthOne?

HealthOne is a secure record that stores patient health information including general practice records, hospital records, dispensed medications and test results. It is available across all of the South Island but was originally set up as a matter of urgency after the Christchurch earthquake. HealthOne is operated in partnership by Pegasus Health, Orion Health and Canterbury DHB and subject to clinical and consumer governance.

HealthOne recognises the importance for doctors, nurses, pharmacists and other clinicians, of having a holistic understanding of other clinicians' treatment when providing safe care. For regular users of the health system, shared care plans are available to ensure consistent treatment that is aligned with the person's wishes and goals.

HealthOne aims to change patient journeys by providing quality information at the point of care to inform safe and effective care plans by healthcare providers, e.g. during an emergency or when a patient is being treated across multiple providers. Having patient information stored in HealthOne means medical professionals don't need to rely on patients to remember their medical history and prescribed medicines and patients don't need to repeat the same information to different providers. Additionally, everyone saves time, effort and money by not having to wait for paper records to be transferred physically or repeat tests which frees up more time for clinicians to spend treating patients.

Data Use

Currently, HealthOne responds to the guidelines for data use in the following ways:

1. What will data about me be used for?

Clinicians including GPs, hospital doctors, nurses, pharmacists and emergency services use patient data stored in HealthOne to determine the best and safest course of care at the point of treatment.

2. What are the benefits and who will benefit?

HealthOne benefits clinicians by enabling them, regardless of their location, to access patient information leading to informed and safer care plans. The reduction in the duplication of services and a general increase in efficiency frees up valuable clinical time to spend with patients and their whānau.

Patients will benefit by not having to repeat tests or answer the same questions over and over, rely on memory or recall clinical details e.g. medicines and dosage, or wait while clinicians wait for data to be sent or shared with them.

3. Who will be using data about me?

HealthOne is used by GPs, hospital doctors, nurses, pharmacists and emergency services. Patient data cannot be accessed by anyone except the authorised clinicians who are providing treatment.

HealthOne is designed to provide access where there is a clinical relationship. If a clinician accessed a patient's information without consent it would be identified in audit and the clinician would be asked to explain why they accessed the information.

HealthOne
Shared knowledge - better, safer care

4. Is data about me secure?

Access to HealthOne is only possible through a highly secure health care information network (not the internet). Access to information is audited by HealthOne and procedures are in place to identify and act upon any inappropriate activity. Patient information cannot be accessed by anyone other than authorised users — and only when the patient is under their care.

Health professionals are subject to strict controls in their employment contract regarding access to HealthOne. Training is also provided outlining their obligations to patients. They are made aware that breaches to privacy and security policies are treated seriously and may result in dismissal from employment.

5. Will data about me be anonymous?

The information is securely stored with strong controls for accessing it, but the purpose is to allow health professionals to understand the person's details for safer care.

6. Can I see, correct or have data about me deleted?

There is no public access to HealthOne which means patients can only access their information when they are with a health professional. The information in HealthOne is entered by the clinician administering patient care. A patient portal would create the need for individual passwords as well as the ability for patients to understand and interpret their clinical information.

Patients are automatically opted in for HealthOne but they can opt out at anytime by calling a dedicated 0508 number or emailing the HealthOne Privacy Office. Posters and pamphlets are visible at each facility informing patients they can opt out. This can mean that those treating the patient may not have the most accurate, or updated information when they are treating a patient. This can be important when prescribing or dispensing medications that may have contra-indications or if the patient has any serious allergies. Alternatively patients may choose to remain opted in but may mark some information as confidential.

7. Will I be asked for consent?

Patients are asked for consent before their HealthOne record is accessed by the clinician treating them (individuals under the age of 16 who present without a parent or guardian are subject to the same process). If the patient is unable to provide consent (e.g. if they are unconscious) the clinician has to add a note to explain the access.

8. Could data about me be sold?

Commercial organisations do not have access to HealthOne. Also, HealthOne cannot be used for 'research'. However patient clinical information may be used if that patient is part of a trial/research project in which the clinician accessing the HealthOne information is delivering the care e.g. taking vitals, bloods or prescribing medication.

Section 4: Existing frameworks and useful links

The links included here contain further information, primarily from Aotearoa New Zealand that may be be useful, depending on the nature of your organisation's work. In each case, the references include guidance and advice on how to think about, and adopt, relevant practices that relate to the respectful use of people's information.

Data Guidelines and Policies

Trustworthy AI in Aotearoa
https://data.govt.nz/assets/data-ethics/algorithm/Trustworthy-AI-in-Aotearoa-March-2020.pdf

Data Protection and Use Policy
https://dpup.swa.govt.nz

Data strategy and roadmap for New Zealand
https://www.data.govt.nz/about/data-strategy-and-roadmap-setting-the-direction-for-new-zealands-data/data-strategy-and-roadmap/

Guidance on sharing information across the child welfare and protection sector
https://www.orangatamariki.govt.nz/assets/Uploads/Working-with-children/Information-sharing/Information-sharing-Guidance-OT-Act-1989.pdf

Privacy, Human Rights & Ethics Framework (PHRaE)
https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/phrae-on-a-page.pdf

Algorithm Charter for Aotearoa New Zealand
https://data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/

Ng Tikanga Paihere
https://data.govt.nz/use-data/data-ethics/nga-tikanga-paihere/

Principles for the safe and effective use of data and analytics
https://privacy.org.nz/assets/Uploads/Principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance3.pdf

Data information from Government and other relevant agencies

StatsNZ
https://www.stats.govt.nz/about-us/data-leadership/

ACC
https://www.acc.co.nz/privacy/privacy-notice-your-personal-and-health-information/?smooth-scroll=content-after-navs

Department of Internal Affairs
https://www.dia.govt.nz/Legal-Privacy-Index

Ministry of Justice
https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

Office of the Privacy Commissioner
https://privacy.org.nz/privacy-for-agencies/your-obligations

Ministry of Social Development
https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html

Te Mana Raraunga Principles of M ori Data Sovereignty
https://www.temanararaunga.maori.nz/

Work and Income
https://workandincome.govt.nz/about-work-and-income/privacy-notice/

Social Wellbeing Agency
https://dpup.swa.govt.nz/about/references-and-useful-links/

New Zealand Government
Open Government Partnership Action Plan 2018-2020.
https://ogp.org.nz/assets/Publications/OGP-National-Action-Plan-2018-2020.pdf

Privacy Maturity Assessment Framework
https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/core-expectations-and-self-assessments/privacy-maturity-assessment-framework-pmaf/

Acts and Legislation

Human Rights
http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html

New Zealand Bill of Rights
http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html

Official Information
http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html

Privacy Act 1993
http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

Public Records Act
http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html

Community Engagement

Policy Methods Toolbox: Community Engagement
https://dpmc.govt.nz/our-programmes/policy-project/policy-methods-toolbox/community-engagement

Industry Standards

New Zealand Data and Information Management Principles
https://www.data.govt.nz/manage-data/policies/new-zealand-data-and-information-management-principles/

Health Information Standards
https://www.health.govt.nz/our-work/digital-health/digital-health-sector-architecture-standards-and-governance/health-information-standards-0

The New Zealand Farm Data Code of Practice
https://www.farmdatacode.org.nz/

NZ Asset Metadata standards
https://www.linz.govt.nz/regulatory/regulatory-search?dt=103

Board leadership and strategy

The Four Pillars of Governance
https://www.iod.org.nz/resources-and-insights/4-pillars-landing-page/#

5 Essential Components of a Data Strategy (SAS)
https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/5-essential-components-of-data-strategy-108109.pdf

Developing Your Data Strategy: A Practical Guide (SAS)
https://support.sas.com/resources/papers/proceedings17/0830-2017.pdf

How To Create A Successful Data Strategy (MIT CISR Data Research Advisory Board)
https://cisr.mit.edu/reports/create-a-data-strategy/intro.php

Developing a Data Strategy: Australian Our Community Group
https://www.ourcommunity.com.au/financial/financial_article.jsp?articleId=6048