Māori data governance guidelines

20/12/2024

nicholson CONSULTING

Table of Contents

Introduction

Māori data governance ensures that data practices respect and uphold Māori rights, aspirations, and values, fostering transparent, equitable, and culturally safe data management. By embedding this framework into its practices, the Royal Australasian College of Physicians (RACP) can build trust with Māori communities, improve Māori health outcomes, and fulfil its obligations to cultural safety and Te Tiriti o Waitangi. This approach enables RACP to align its data collection and use with the core values of *tika* (correctness) and *pono* (integrity), paving the way for equity-driven innovation and reinforcing partnerships with Māori.

This document offers culturally appropriate guidance to support RACP in managing data from a te ao Māori perspective. It was structured around the eight Māori data governance pou (pillars), which highlights key priorities for establishing effective governance. The guiding principles underpin these pou, ensuring that the practices align with Māori values and principles.

The report concludes with a section on **key definitions**, providing clarity on important terms and enhancing the understanding of the principles and framework. A list of the **reviewed documents** is included, highlighting key sources and references that informed the development of the Māori data governance guidelines, while offering additional context and insights into the research and discussions that shaped them. Additionally, a **document history** section outlines the report's development and revisions, ensuring transparency in its evolution.

Background

Nicholson Consulting was engaged by the Royal Australasian College of Physicians (RACP) to create a Māori data governance guidelines document, providing clear and culturally appropriate guidance for managing Māori data. The goal was to ensure that RACP's handling of Māori data was structured and accountable at every stage of its lifecycle, upholding Māori rights and values in data governance practices.
These guidelines were developed with a focus on Māori data governance, aligning with the eight Māori data governance pou to address key priorities for effective governance. This work aimed to support RACP in meeting its obligations, fostering cultural safety, and ensuring its data practices reflect Māori values.

Scope

This work focused specifically on Māori data governance, rather than a broader Indigenous data governance framework. This approach acknowledges the distinct governance needs of

Aboriginal and Torres Strait Islander communities in Australia, and recognising that they, too, require data practices to be rooted in their unique cultural contexts.

Nicholson Consulting's core role was to centre Māori data sovereignty while acknowledging that defining and implementing Indigenous data governance for Australian Indigenous peoples is the responsibility best held within their communities. Nicholson Consulting was to incorporate this understanding throughout the project, ensuring that the guidelines are specific to Māori data needs without undermining the autonomy and data sovereignty of Australia's Indigenous peoples. In a similar vein, the Pacific Data Sovereignty Network and any in-house Pasifika team are best placed to provide guidance around Pasifika data.

Approach

The term Māori data governance often generates a question about where information governance sits. This report focuses directly on guidelines relating to Māori data but many of the recommendations may also be relevant to managing Māori information as well.

In Phase 1, Nicholson Consulting conducted a high-level review of RACP's existing data policies to assess alignment with Māori data governance. Phase 2 involved consulting with RACP staff to gather insights on their data governance needs, followed by drafting and refining the guidance document in Phases 3 and 4. The final deliverable, produced in Phase 4, was a resource to support RACP in upholding culturally respectful Māori data management practices.

What Is Māori Data Governance

Te Mana Raraunga define Māori data governance as the principles, structures, accountability mechanisms, legal instruments and policies through which Māori exercise control over Māori data. Implementing Māori data governance practices upholds the rights and interests of Māori, which are represented by the Māori data sovereignty principles from Te Mana Raraunga. Though Māori data governance primarily relates to the management of Māori data, it also provides best data practices that are universally beneficial to all types of data and many groups of people.

In May 2023, Te Kāhui Raraunga released the Māori data governance model, which is intended to help guide the Aotearoa public service on implementing system-wide governance. which is grounded in te ao Māori, delivers on Māori aspirations and needs, and is in alignment with your principles of justice and equity and the Indigenous Object outlined in Section 1.1.9 of the RACP Constitution both of which cover Te Tiriti o Waitangi.

Māori Data Governance Pou

The Māori data governance pou provide the framework for the structure of this report, as outlined in the table below:

Table 1: Summary of the eight pou of the Māori data governance model

Ngā Pou	Description
Pou 1: Data Capabilities and Workforce Development	Focuses on enhancing Māori data skills both within the organisation and among communities. These skills should be grounded in Māori values and cultural practices (tikanga). Further there should be consideration of aspects such as cultural tax and cultural safety.
Pou 2: Data Infrastructure	Addresses decisions related to infrastructure, which encompasses hardware, software, networking, services, policies, and other related components. Māori data governance focuses on aspects of data infrastructure designed to benefit Māori, distributed and decentralised infrastructure, and places a strong emphasis on sustainable and forward-looking infrastructure.
Pou 3: Data Collection	Relates to a Te Tiriti based approach to the collection of data. Here there is a strong focus on Māori aspirations determining what data is collected, the reasons for collecting the data and how Māori will benefit
Pou 4: Data Protection	Relates to protecting data through privacy, security, and jurisdiction. It also relates to the concept of collective privacy and Māori tikanga relating to privacy
Pou 5: Data Sharing, Access and Repatriation	Relates to the ability of Māori to have access to data, receive data, and ensure data is returned when it is no longer needed. Accessibility of data is a key principle highlighted in the iwi data needs paper.
Pou 6: Data Use and Reuse	Relates to how data is used and reused, covering elements of consent, the formulation of appropriate research questions, and the development and application of algorithms.
Pou 7: Data Quality and System Integrity	Relates to the setting of standards, monitoring of data quality, and ensuring accountability to Māori. This Pou emphasises the importance of establishing clear and culturally appropriate standards for data governance. It includes rigorous monitoring processes to maintain high data quality and ensure that data practices are transparent and accountable to Māori communities. The focus is on upholding the integrity and reliability of data, ensuring that it meets the needs and expectations of Māori stakeholders.

Ngā Pou	Description
Pou 8: Data Classification	Relates to the ability to define Māori data and ensure the use of appropriate metadata.

Guiding Principles

The Māori data sovereignty principles are used to inform these Māori data governance guidelines. These principles are integral to the decision-making processes surrounding Māori data. They guide the framework for decision-making and ensure cultural integrity is maintained throughout the data management lifecycle. The guiding questions below should be considered by RACP when collecting, using, sharing, or storing Māori data.

For an explanation of what these terms mean, please see the definitions table.

Rangatiratanga
Guiding questions

- Who holds decision-making power over Māori data?
- How does this decision support Māori members to self-determine?
- Are we involving appropriate Māori members and staff in the governance process?
- How do our data collection practices enable Māori to exercise self-determination?

Whakapapa
Guiding questions

- What contextual metadata does this data have, and how does it inform its current use?
- What level of disaggregation is most appropriate for our membership body to both inform decision making whilst not personally identify members because of small count sizes?
- What safeguards are in place to ensure that future use of the data remains connected to its original purpose and relationships?
- Are our data collection methods aligned with the importance of whakapapa, ensuring that the origins and context of the data are accurately recorded?

Whanaungatanga
Guiding questions

- What obligations do we have to Māori members and external medical groups regarding this data?
- How are we balancing the rights of Māori members with organisational accountability and responsibility?

- In what ways can we enhance relationship-building with our Māori members through transparent data governance practices?
- How can our data collection methods foster trust and maintain strong relationships with Māori members?

Kotahitanga
Guiding questions

- How does this data decision serve the collective benefit of our Māori members?
- What steps are we taking to build internal Māori data capacity?
- Are there ways to connect this data governance decision with broader Māori goals and community outcomes outlined in our Indigenous Strategic Framework?

Manaakitanga
Guiding questions

- How are we obtaining consent from Māori members regarding data use?
- In what ways are we showing respect for Māori values and protocols in our data governance practices?
- How will this data decision enhance or harm relationships with our Māori members?
- Will our members be offended that we have asked for specific data to be collected?

Kaitiakitanga
Guiding questions

- What ethical considerations are required to safeguard Māori data during and after its transfer or storage?
- How are we ensuring that our data platforms and technologies align with kaitiakitanga principles, especially regarding data storage?

Are there access restrictions necessary to protect this data in alignment with Māori guardianship principles?

Findings and Recommendations

Pou 1: Data Capabilities and Workforce Development

Pou 1 covers enhancing Māori data skills both within the organisation and among communities. These skills should be grounded in Māori values and cultural practices (tikanga) and also consider cultural safety and cultural tax.

Building Cultural Safety

The Māori Health Committee brief states that it is important that all staff members working directly with Māori data receive appropriate cultural safety training on Māori data. Currently training covers cultural safety more generally but lacks enough dedicated content relating to Māori data.

Understanding cultural safety in a general sense can be a stepping stone to better understand the safe use of Māori data. RACP has initiated this journey with a one-day cultural safety training programme for staff. By encouraging self-reflection and bias awareness, staff should find it easier to give effect to the Māori data sovereignty principles and in particular the guiding principles in this document.

In the longer term, RACP aims to expand structured data-sharing practices more broadly to include the board, committees and potentially adding a module to the curriculum for members. RACP is also exploring physician cultural safety initiatives, although it recognises that achieving widespread support will require gradually building understanding and buy-in. For instance, some physicians question the relevance of cultural safety training, as they may not currently see indigenous patients, including Māori. A staged approach to implementing these practices will likely be most effective, enabling gradual adaptation and fostering a deeper appreciation for cultural safety across the organisation.

It is recommended that RACP:

- Develop tailored training modules on Māori data sovereignty principles to complement cultural safety training, ensuring alignment with the ethical and equitable use of Māori data.
- Pilot cultural safety training with a group of Māori staff and data staff first to seek feedback before rolling out across the organisation
- Cultural safety training focused on Māori data sovereignty and the guiding principles within this document should be completed yearly by staff
- Longer term add this training to the curriculum so that members are also familiar with culturally appropriate use of Māori data

- Between training, members and staff can draw upon self-reflection tools such as the Āta model or Taikitoru framework

Māori Data Practices

Current in-house practices relating to Māori data currently involve asking Māori staff for advice. This can cause cultural tax for Māori staff who do not work in the data space as well as risks of knowledge retention when Māori staff leave. In some scenarios there is a general lack of awareness that such questions should be asked, which can cause issues for members and RACP when Māori data is not handled appropriately.

It is recommended that RACP develop their own in-house resources to support staff with the safe use of Māori data. These resources include:

- Practical, hands-on training sessions that incorporate real-world scenarios that have been encountered by Māori staff within RACP,
- Example case studies that illustrate best practices for handling Māori data and navigating complex ethical considerations.

By embedding these initiatives into its operations, RACP can ensure its workforce is both culturally competent and equipped to uphold the principles of Māori data sovereignty.

Pou 2: Data Infrastructure

Pou 2 addresses decisions related to infrastructure, which encompasses hardware, software, networking, services, policies, and other related components. Māori data governance focuses on aspects of data infrastructure designed to benefit Māori, distributed and decentralised infrastructure, and places a strong emphasis on sustainable and forward-looking infrastructure. Given the size of RACP and ability to influence the tech sector the focus of this section will only be on data infrastructure that works for Māori.

Data infrastructure that works for Māori

RACP's infrastructure comprises a range of systems and applications, including but not limited to WhichDoctor CAS, Aptify, MyCPD, and an e-learning platform. However, these systems were not designed with intentional consideration of Māori needs and values, highlighting an opportunity for RACP to review and adapt its infrastructure to better support culturally appropriate practices and align with Māori data governance principles.

In the future, when existing platforms are replaced, or new platforms are procured:

- Māori Data Guardians and membership body should be consulted before the procurement process for data infrastructure starts.
- The guiding principles within this document should be used to inform technology decisions

- The procurement process should incorporate some questions relating to Māori data governance to ensure that this forms part of the decision-making process when selecting a vendor.

Pou 3: Data Collection

Pou 3 relates to a Te Tiriti based approach to the collection of data. Here there is a strong focus on Māori aspirations determining what data is collected, the reasons for collecting the data and how Māori will benefit.

Prioritising Māori needs

RACP already collaborates with the Māori Health Committee to inform aspects of data collection relevant to Māori members. This includes gathering insights on Māori members educational pathways, career trajectories, and workforce involvement. These efforts provide an overview of Māori participation within RACP.

RACP also has a diversity questionnaire in development aimed at gathering a broader range of data on members backgrounds. See 'Pou 7: Setting standards' for more information on the content within the questionnaire itself and proposed changes for improvement.

In the future, Māori needs could be prioritised by:

- Increasing direct consultation with Māori members and committees to co-design data collection.
- Assessing how the data will benefit Māori and considering potential risks or unintended consequences prior to data collection. This could be achieved by consulting with the Māori Data Guardian on ethical guidelines and impact assessments.

Collect only what is needed

RACP collects member data through multiple means, including initial onboarding, applications for scholarships, and internal surveys.

Collecting only what is needed not only respects members privacy but also demonstrates a commitment to data minimisation, ensuring that any data gathered is directly linked to the organisational priorities and avoids unnecessary intrusiveness. This approach supports the RACP Indigenous Strategic Framework, launched in 2018, which underscores the importance of culturally aligned data practices within a Māori Data Governance framework.

To guide RACP's data collection efforts, it is recommended a thorough stocktake is conducted to:

- Understand all available data and information,

- Identify any data collection gaps based on feedback from the Māori Data Guardian and Māori members,
- Ensuring that future data collection aligns with strategic goals, particularly increasing the Māori physician workforce and enhancing cultural safety.
- and reducing the duplication of data collection described in *Brief To The DGG – Standardising Collection of Member Indigenous Identity Data*

Distinctions between personal and organisational data are crucial here, as each requires specific handling to respect Māori concepts of health and wellbeing. For instance, personal data gathered on health or wellbeing (hauora) should reflect holistic Māori perspectives, such as wairua (spiritual health), whānau (family), and whenua (land), especially where members indicate an interest in such areas. By conducting a comprehensive audit, RACP can streamline data collection, ensure that each data point serves a clear purpose, and provide meaningful insights without overextending resources or risking data oversaturation.

How data is collected matters

The MHC Brief has raised issued relating to current Māori data practices including how Māori data is collected, recorded and stored. Currently, the Power BI dashboard only captures data from one primary system, while additional data sources exist separately, often gathered through hard copy forms. This lack of integration and standardisation creates challenges in collating information and achieving a comprehensive understanding of the Māori members' journeys and the diversity within RACP.

Standardising questions and approaches to data collection, particularly with ethnicity data, is not just beneficial but crucial. Such data is key for workforce planning, allowing RACP to assess current representation and forecast future needs in alignment with the strategic priority of increasing the Māori physician workforce. A consistent collection method not only improves the quality of data but also enhances accuracy, reliability and fairness. Addressing these gaps is critical for developing effective workforce planning, fostering inclusivity, and strengthening trust among all members.

It is recommended that:

- A standardised set of Māori data questions are asked. See 'Pou 7: Setting standards' for a set of standardised questions relating to Māori data.
- Ensure there is a consistent process for collecting and updating data that minimises duplication of data collection
- Ensure that all source systems are connected so it is easier to share a wider range of insights to your members and it is easier for RACP to identify the Māori data it holds

Pou 4: Data Protection

Pou 4 relates to protecting data through privacy, security, and jurisdiction. It also relates to the concept of collective privacy and Māori tikanga relating to privacy.

Privacy

The RACP privacy policy and the data governance policy provide specific guidance around privacy considerations.

In addition, the following changes should be made to these documents:

- Review the data retention policy to determine whether retaining members records 10 years after death or 120 years after birth is reasonable. This assessment should include an analysis of regulatory requirements, operational needs, and privacy best practices. Engage with stakeholders to define a feasible retention period that reflects both compliance and member expectations.
- As RACP tools and systems are upgraded, explore if more sophisticated data protection such as data masking and other anonymisation techniques are required to further safeguard member data.

Collective privacy is often an area that is not covered in legislation. The Māori Data Sovereignty and Privacy paper from the Tikanga in Technology project may be useful if RACP wishes to learn more about collective privacy and implications for their organisation.

Security

RACP information security policy provides specific guidance around security considerations. Strengthening these security measures requires an understanding of current risks and the implementation of best practices in line with emerging standards.

Security could be further improved by:

- Reviewing whether date of birth is required by the college. Date of birth can often be used as a verification question so if that data was leaked it could present security risks. Year of birth may be sufficient for the type of analysis that RACP does.

Jurisdiction

RACP data systems store and process data in a variety of jurisdictions including but not limited to: Australia, New Zealand and the United States.

It is recommended that:

- RACP provides members an annual report and update of where data is stored and processed.

- Whilst there is a preference for data to be stored and processed in Australia or New Zealand, the guiding principles should be used to determine that the benefits of storing within Australia or New Zealand outweigh the costs.

Pou 5: Data Access, Sharing and Repatriation

Pou 5 covers the ability of Māori to have access to data, receive data, and ensure data is returned when it is no longer needed.

Access

RACP uses a Member Data Report and Insights Request Form, which must be approved by the Māori Data Guardian before any Māori data is accessed. This process ensures that access to data is carefully controlled, reviewed, and only granted when it is culturally appropriate and aligned with organisational needs. This existing practice is strong, as it fosters accountability and allows only authorised personnel to access sensitive data.

In the future, RACP will need to further enhance access management by considering the balance between accessibility and privacy in new ways, particularly as data needs evolve. While enabling access for members and relevant stakeholders is essential to fostering knowledge-sharing and informed decision-making, RACP must also determine whether access should be restricted or denied. This approach will protect culturally sensitive information and help to maintain the trust of Māori members and communities.

It is recommended that:

- Where data contains personal or culturally significant information, access restrictions should be based on well-defined criteria, such as the user's role, the purpose of access, and alignment with Māori Data Sovereignty principles.
- Data access granted through the Māori Data Guardian's approval is accessed solely by the requestor(s) and strictly used for the purpose it was requested. Access to data or information should be granted via secure links with a defined expiration period, ensuring data cannot be accessed by others or accessed beyond the approved timeframe.

Developing role-based access control and regular audits can further support this by ensuring that data access decisions are transparent, fair, and sensitive to the specific needs and expectations of Māori members.

Sharing

Sharing data effectively within RACP is essential because it ensures that the right information reaches those who need to make informed, impactful decisions, all while respecting Māori data governance practices. RACP exercises caution in sharing Māori data externally, currently managing most data requests through ad hoc email chains. Generally, the organisation closely scrutinises any external sharing of information, ensuring that data handling aligns with RACP's ethical standards and safeguards members privacy.

While this approach minimises unnecessary data sharing, it lacks the consistency and transparency that a more structured system could provide. Evidence from other settings shows that structured agreements, like Memoranda of Understanding (MOUs), can offer a more systematic approach to data sharing. For example, RACP has an MOU with the Ministry of Health (MOH) analytics team, enabling specific data exchanges when justified. This MOU allows for the sharing of de-identified data to support long-term planning, such as workforce projections in the health sector.

This highlights that while ad hoc approaches have their benefits, there are structured methods RACP could consider adopting more widely to enhance clarity and governance in data sharing.

It is suggested that RACP could benefit from establishing a centralised process for all data-sharing requests, where each request is evaluated on key criteria:

- **Purpose and alignment with RACP values:** Assessing how shared data will be used and its benefit to Māori communities.
- **Narrative consistency:** Ensuring that data use aligns with the narrative RACP seeks to uphold regarding Māori health and wellbeing.
- **Data security and retention:** Defining how shared data will be securely stored, how long it will be retained, and the responsibilities for its eventual deletion or return.

Through these measures, RACP can promote a balanced approach that enables effective knowledge-sharing while respecting the privacy and cultural sensitivities of Māori data, reinforcing trust with Māori members and communities.

Repatriation

Currently, RACP does not have formal procedures in place for repatriating Māori data, though data retention is managed, with some records removed based on age or legal requirements. Reviewing existing retention timeframes would be a positive step in refining these processes; the current guideline of retaining data up to 120 years after birth, or 10 years after death, may extend longer than necessary for some records. A reassessment of

these timeframes, informed by consultation with Māori Data Guardians, could ensure data is retained only as long as it remains relevant to both RACP and Māori communities.

While the existing approach demonstrates an awareness of data longevity, it lacks a specific focus on facilitating Māori members' ongoing access to their own data or transferring it to a custodian they trust if RACP no longer requires it. Formalising repatriation procedures would strengthen RACP's Māori data governance by ensuring that Māori data is ultimately accessible to its original custodians and that Māori members retain control over their own data.

Repatriation, or the return of data to its original community or owner, is a crucial component of Māori data governance. For RACP, the concept of repatriation reflects a commitment to respecting Māori ownership and control over their data, recognising that Māori data is not simply an asset of the organisation but a cultural taonga (treasure) that belongs to the community it represents.

In the future, a repatriation framework could be developed which covers:

- Consulting with Māori members and Data Guardians to develop repatriation practices that uphold the principles of kaitiakitanga (guardianship) and rangatiratanga (self-determination). This would honour the cultural, spiritual, and genealogical significance of data to the Māori community.
- Allowing Māori members to specify their preferences for data handling upon retirement, departure, or death. This could include options for secure deletion, return to family or iwi, or transfer to a trusted Māori data custodian.
- Developing secure systems for archiving and repatriating data over time, especially for data of historical or cultural relevance. This would ensure data transfer is carried out securely and with integrity, maintaining the accessibility of data to Māori communities.

Pou 6: Data Use and Reuse

Relates to how data is used and reused, covering elements of consent, the formulation of appropriate research questions, and the development and application of algorithms. RACP does little work with algorithms so instead there has been a focus on appropriate purpose.

Consent

The use and sharing of data with external parties, such as Te Ohu Rata o Aotearoa and Māori Medical Practitioners should be consent-driven. There is an explicit preference amongst RACP for data not to be shared automatically; instead, the consensus is that

external parties should only receive data when there has been explicit consent to share that data.

Nicholson Consulting suggests the following considerations:

- Data sharing with other entities will rely on explicit consent rather than default inclusion, ensuring that Māori data sovereignty and stakeholder preferences are respected.
- Consent processes should be clearly communicated and documented, with Māori Data Guardians and Māori Health Committee members overseeing consent-related decisions for high-stakes data sharing.
- Consent agreements should outline data-sharing boundaries, specify who can access the data, and clarify data governance protocols to protect Māori data rights.

Appropriate purpose

Determining the appropriate purpose for data collection and use requires transparency and accountability, particularly around sensitive information such as iwi affiliations. RACP aims to better manage and centralise Māori data requests to streamline approvals and avoid ad-hoc data sharing, particularly when iwi-specific or other demographic information is involved.

It is recommended that:

- Data requests should clearly outline the intended purpose, ensuring alignment with Māori health and workforce planning needs.
- Where feasible, RACP should formalise agreements like MOUs with various health bodies to provide structure around data sharing, clarifying what data will be shared and for what purpose.
- Using data for a secondary purpose will require explicit reapproval.
- Consider future iwi workforce needs and weigh the value of collecting iwi-specific data against the privacy risks associated with small cohorts. Decisions about data use, especially regarding sensitive Māori demographic information.
- Given the small number of Māori professionals, breaking down data by iwi could easily lead to identifiable information. To mitigate this, RACP can explore broader categorisations, such as rohe or waka, as an alternative for workforce planning purposes.

Asking the right questions

It's important to consider what information is necessary and how it will be used, especially for data points that RACP currently collects or wishes to collect that intersect with cultural identity or personal attributes (e.g., iwi affiliation, first language, sexual orientation). Some existing questions may have limited applicability or relevance to the intended outcomes of Māori health and cultural safety goals.

It is recommended that:

- Each data field collected should serve a clear purpose that aligns with RACP goals. For example, understanding why Māori data points such as iwi affiliation or first language are collected is crucial. Any irrelevant fields should be reviewed to ensure data collection aligns with best practices and cultural respect.
- Engage with Māori Health Committee members and Māori Data Guardians to explore how specific data, like iwi affiliations, might be beneficial for future initiatives without compromising privacy. Consider if information on iwi or rohe could support iwi-led workforce planning, cultural safety, or regional service delivery.
- Assess the relevance of collecting sexual orientation data if it doesn't directly contribute to RACP's mission or cultural safety.
- The Indigenous Data Governance policy provides a framework to ensure all data collected aligns with Indigenous priorities. A checklist could help evaluate whether current data practices align with objectives such as trainee experience, equity in specialities, or Indigenous mentoring and support networks.
- Decisions about data use, especially regarding sensitive Māori demographic information, should be guided by ethical frameworks. This could include Te Ara Tika Research Guidelines if you want to be consistent with the Health Research Council, or Ngā Tikanga Paihere if you would like data-specific ethical framework grounded in tikanga Māori.

Pou 7: Data Quality and System Integrity

Pou 7 Relates to the setting of standards, monitoring of data quality, and ensuring accountability to Māori. This Pou emphasises the importance of establishing clear and culturally appropriate standards for data governance. It includes rigorous monitoring processes to maintain high data quality and ensure that data practices are transparent and accountable to Māori communities. The focus is on upholding the integrity and reliability of data, ensuring that it meets the needs and expectations of Māori stakeholders.

Setting Standards

Diversity and indigenous status data

Diversity data are demographics that enable RACP to understand the variety of people within their membership body including whether they are indigenous members. This information can provide a baseline for monitoring whether the membership body is reflective of the general population. RACP has drafted guidance which contains standardised survey questions, developed and owned by the Project Manager, Member Wellbeing & Support, to ensure consistent data quality across the organisation.

Having standardised questionnaires and guidance relating to diversity data and specifically indigenous status will:

- Improve the member experience by having data that will allow RACP to better track and check-in with Indigenous members at critical points across the training pathway.
- Enable Māori Health committee to exercise good governance over their respective member data sets in ways that are culturally appropriate.
- Fulfil the priorities of the RACP's Indigenous Strategic Framework

The guidelines can be found in the following documents:

- *Guideline for Collecting Diversity Data of College members*, and
- *Guideline for Collecting Indigenous Status Data of College members*.

In addition, there is limited understanding within RACP of the difference between total response and prioritised ethnicity, as well as the distinction between ethnicity and descent data, and the circumstances in which each should be used. These gaps in understanding can lead to inconsistent data use and undermine efforts to reflect the diversity of the membership accurately.

Nicholson Consulting note that the following changes should be made to these documents:

1. Clarify the use of ethnicity data for reporting: The *Guidelines for Collecting Diversity Data of College members* should be updated to be explicit about whether RACP will use total response or prioritised ethnicity for reporting.

   To provide clarity the following explanations could be used:
   - Total response: This approach counts all ethnic groups a person identifies with, meaning percentages may exceed 100% as individuals can belong to more than one group.
   - Prioritised ethnicity: This method allocates individuals to a single ethnic group, following a pre-determined priority order, which simplifies analysis but can underrepresent people who identify with multiple groups.

- Descent information relates to whakapapa or ancestry it should be used when analysing populations demographics or scenarios when policy and resource allocation is dependent on whakapapa regardless of ethnic identification (e.g. scholarships for Māori)
- Ethnicity is self-reported cultural affiliation which is often used when comparing health outcomes across groups or social involving those who actively identify with Māori culture.

For further information, see the Ministry of Health HISO on ethnicity data protocols

2. Create standardised Māori data questions. Several documents already articulate proposed Māori data questions. We suggest the following standardised Māori data questions
    a. Change the descent question to be more consistent with the Stats NZ Census i.e. the wording should be 'from Māori' rather than 'from *a* Māori'. The full question should read: "Are you descended from Māori? (that is, did you have a Māori birth parent, grandparent or great-grandparent, etc)? He tūpuna Māori ōu?"
    b. Remove the iwi affiliation question from the standardised questionnaire (see the next section for more details)
    c. Change the first language question to the Stats NZ Census question: "In which language(s) could you have a conversation about a lot of everyday things?"

The guidelines (and subsequent iterations) must be signed off by the Māori Data Guardians. Once the guidelines have been signed off, the BI Hub will implement the approved questions and statement across all existing collection points in RACP.

Iwi affiliation data

Iwi affiliation data should not be collected unless there is a clear purpose and benefit. Furthermore, it is good practice to consult with iwi organisations to understand what data points would be useful for the iwi.

With more than 100 iwi and approximately 100 Māori RACP members, Nicholson Consulting believes the Māori membership population size within RACP is too small to warrant iwi affiliation capture across the entire membership population. However, in a situation where a member applies to be a part of the Māori Health Committee then iwi information can be collected so that RACP can work towards diverse representation across iwi on the committee. As there are currently no use cases that would justify collection of iwi information across all members, the Stats NZ iwi classification and the Ministry of Health iwi affiliation data protocols have not been formally adopted by RACP.

Monitoring

Whilst there is monitoring of the number of Māori members, there is no regular monitoring of Māori data related requests. Monitoring processes should focus on regular checks for data integrity, with particular attention to the quality of data related to Māori members. In addition, monitoring of relevant data can also help with priorities set out in the RACP Indigenous Strategic Framework and determine whether additional Māori Data Guardian roles are required to manage these responsibilities effectively.

A robust monitoring framework might include:

- Assessing data quality issues relating to Māori data
- Tracking the number of data access requests relating to Māori data
- Data support requests made to the Māori Data Guardian, especially those requiring access to Māori data, to ensure adherence to data governance principles and to support equitable health outcomes.

Accountability

Roles and responsibilities of the (Indigenous) Data Guardian are articulated in the data governance policy from a data and information management perspective. From a Māori data governance perspective, the Māori Data Guardian is responsible for the following:

The Māori Data Guardian is responsible for:

- Pou 1: Implementing culturally safe data practices and building up Māori data capability.
- Pou 1: Promote any webinars on Māori Data Sovereignty to staff involved with Indigenous member data collection when webinars when applicable.
- Pou 3: Ensuring that data collected on Māori members reflects Māori priorities, values, cultures, worldviews, and diversity
- Pou 3: Approving all key stages in collection of Māori member data or advising the scope and duration of approval when the approval request is received.
- Pou 3: Maintaining the *Collecting diversity data guideline* alongside the Project Manager, Member Wellbeing & ensuring that questions asked to collect the diversity data are asked in respectful and safe way.
- Pou 6: Deciding what, how, and why Māori member data is used
- Pou 7: The Māori Data Guardian role is to review any quality issue(s) impacting **Māori** data and to approve any course of action recommended to resolve the identified data quality issue.
- Pou 8: Setting business rules and guidelines and data definitions as it relates to Māori data (see data governance policy).
- Pou 8: In conjunction with the Māori membership body, determine how Māori data is classified within RACP.

The Māori Data Guardian is accountable for:

- Pou 3: Deciding what, how, and why Māori member data is collected
- Pou 5: deciding what, how, and why Māori member data is accessed
- Pou 6: approving all key stages in analysis, and reporting of Māori member data or advising the scope and duration of approval when the approval request is received.

The Māori Data Guardian is consulted on:

- Pou 2: Data infrastructure that works for Māori.
- Pou 3: Changes IT makes to mechanisms so that feedback from membership body can occur
- Pou 4: In addition, the Māori Data Guardian should be consulted to provide feedback on indigenous privacy.
- Pou 4: Opportunity to feed into technology decisions that will store Māori data (in particular) relating to jurisdiction.
- Pou 7: Data Governance Policies and Standards (see data governance policy). However, when standards relate to ethnicity, descent or iwi affiliation then the Māori Data Guardian is accountable.

Given the Māori Data Guardian is heavily involved in Māori data governance, there is nothing for the Informed section of the RACI matrix.

Risk classification matrix

Currently the mechanism for identifying Māori data risks relies on asking the Māori cultural advisor. This adds cultural tax to the role and creates a singe point of failure. It is important to bring up the competency of staff at RACP so that gradually they will have the confidence to deal with low risk issues.

This risk assessment is structured to provide a clear framework for identifying, classifying, and managing risks related to Māori data within RACP. All identified risks must be recorded in a risk register upon identification and categorised using a risk classification matrix (see Figure 1). A risk classification matrix is a self-assessment tool designed to evaluate both the severity of the impact should the risk occur and the likelihood of the risk occurring.

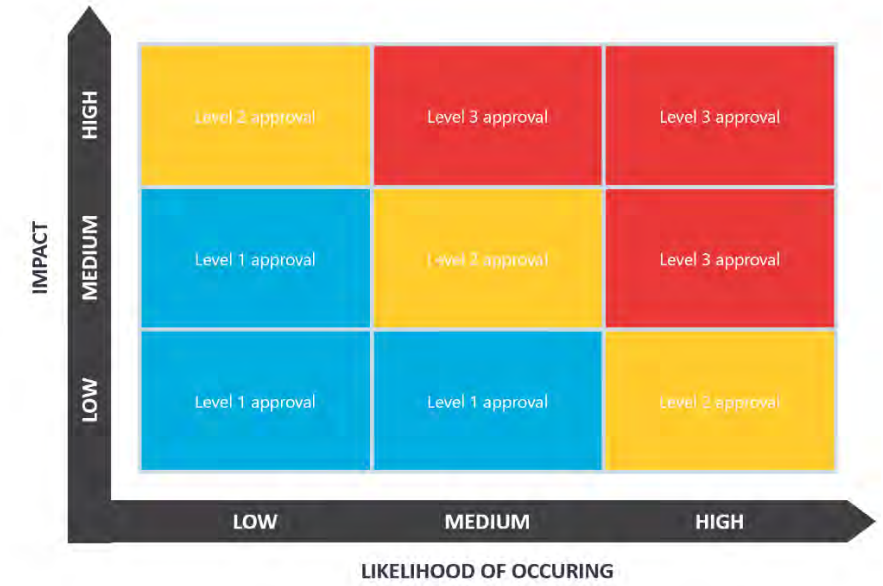

Figure 1: likelihood of occurring risk register

The structure classifies risks as low, medium, or high, based on their potential impact and the probability of occurrence. Low-risk items (level 1), such as identifying data quality issues or securing Māori data, can be approved by the Māori Data Guardian whilst staff capability is being developed. Medium-risk items (level 2), like defining Māori data or collecting new data points, require additional sign-off by the Māori Health Committee (MHC). High-risk items (level 3), such as gathering iwi affiliation data or sharing information with external entities, call for an external independent review to ensure they are managed with the utmost sensitivity and compliance.

This structured approach aims to support decision-makers by streamlining approvals based on risk level, clarifying responsibilities, and providing an escalation point for higher-risk scenarios. This section outlines practical examples for each risk level, ensuring a consistent and culturally informed method of assessing and managing risks associated with Māori data.

Examples of low risks situations could include:

- **Identifying data quality issues relating to Māori data:** This involves recognising and rectifying inaccuracies or inconsistencies, which is essential for maintaining data integrity. It presents minimal risk as it focuses on internal improvements.
- **Ensuring that the team has completed training with a provider on the culturally appropriate use of data:** This proactive step helps the team handle Māori data respectfully, enhancing internal competency without impacting the data directly.
- **Controlling access to Māori data:** limiting access based on roles and responsibilities helps prevent unauthorised use, safeguarding data without needing external review.

Examples of medium risks situations could include:

- **Determining and updating the definition of Māori data:** this influences how Māori data is understood and categorised, which can have broader implications for data governance, privacy, and cultural safety. It requires oversight to maintain cultural accuracy and respect.
- **Collection of new data points from Māori:** Gathering additional information from Māori individuals introduces new data, which can raise privacy and cultural considerations. This step needs validation to ensure it is handled with cultural sensitivity.
- **Determining how Māori data is used**: Deciding on the application or purpose of Māori data can impact Māori communities, and oversight ensures it aligns with RACP's values and Māori interests.

Examples of high risks situations could include:

- **Collection of new data points that are of particular interest to Māori e.g. iwi affiliation:** Iwi affiliation is a sensitive and important cultural identifier. Collecting such data requires careful consideration, as misuse or mishandling could affect trust and relationships with Māori communities.
- **Sharing data with new external collectives that RACP is not legally obliged to share information with:** When RACP shares data with external entities, especially those without existing legal agreements, it introduces risks to privacy, security, and cultural propriety. An external review ensures these actions are justified, transparent, and aligned with Māori data governance principles.

Pou 8: Data Classification

Relates to the ability to define Māori data and ensure the use of appropriate metadata.

Defining Māori data

The working definition used by RACP to define Māori data is: "Digital or digitisable information or knowledge that is about or from Māori Peoples, their language, culture, resources, or environments." Currently, there are no formal business rules in place at RACP which may lead to inconsistencies in identifying Māori data across systems. Therefore, establishing clear business rules for identifying Māori data is critical.

Metadata

Metadata tagging could enhance data organisation, making it easier for authorised users to locate Māori data and respond to common information requests, such as those related to member contact details, numbers of Fellows and trainees, specialities, and locations of work. While RACP does not currently utilise tagging, exploring this feature could strengthen its Māori data management practices. A minimum metadata standard could help identify key metadata to be captured.

A searchable data catalogue or a data asset register are good starting points to make data easier to discover. Currently, Power BI reports act as the main point of reference for Indigenous staff and select IT specialists, but data is also captured across various systems, including CRM, training portals, and other adhoc systems. A stocktake to identify all points of Māori data capture would help RACP catalogue this data, ensuring that all Māori data sources are accounted for and accessible in alignment with data governance priorities.

Summary

The Māori data governance framework has been used to review existing RACP processes and provide recommendations for how RACP can enhance their approach to Māori data.

The recommendations include:

- Pou 1: Focusing on Māori data specific training that draws upon RACP real-world scenarios that will be available to all staff and eventually members to demonstrate best practices for handling Māori data
- Pou 2: Involving the Māori Data Guardian in procurement decisions and ensuring the Māori perspectives are incorporated into the procurement process.
- Pou 3: Conducting a data stock take, using a standardised set of questions related to Māori data and ensuring that the data collected aligns with Māori member and RACP aspirations.
- Pou 4: Reviewing the retention policy, reviewing whether date of birth is necessary to collect and opting for Australia or New Zealand storage solutions where benefits outweigh the costs. Data storage and processing locations should be reported.
- Pou 5: Access to data is done through secure links for specific people that will expire when access is no longer required and a centralised process for data sharing based on Māori perspectives including repatriation of data.
- Pou 6: Having explicit consent before sharing data externally and a documented consent process that ensures that is used for an appropriate purpose. Specifically, collecting iwi information for all members should not occur until there is a clear purpose for use that aligns with Māori member and RACP aspirations.
- Pou 7: Formal Māori data standards should be adopted, monitoring of Māori data should be carried out and the specific roles and responsibilities of the Māori Data Guardian noted in alignment with the Māori data governance model.
- Pou 8: A minimum metadata standard that speaks to Māori data could be useful alongside a data asset register or a searchable data catalogue that identifies Māori data.

The Māori Data Guardian will review these recommendations and consider an implementation plan once the review is complete.

Key Definitions

Check out the data governance policy definitions

Term	Means
Aotearoa	traditional name now commonly used as a Māori name for New Zealand
Application Data (OLTP)	Information, data and files that are entered into and stored in a source system. In the RACP this would include data in CAS, WD, Aptify, MyCPD, Sharepoint etc.
Cultural Safety	"Cultural safety is based on the experience of the recipient of care, rather than from the perspective of the medical practitioner. It involves the effective care of a person or family from another culture by a medical practitioner who has undertaken a process of reflection on their own cultural identity and recognises the impact their culture has on their own medical practice" (RACP, n.d)
Cultural Tax	The additional work that Māori in corporate positions are requested to do over and above their job description (Auckland University, 2020)
Data Custodian	Is responsible for managing a data asset from a technical perspective. This includes providing the data infrastructure to enable data analysis & quality assurance, ensuring data security and providing technical expertise on data asset management.
Ethnicity Data Protocols	A HISO from Ministry of Health that speaks to collecting, classifying, recording and story ethnicity data.
Indigenous Data Guardian	Is a key decision maker in the development and application of the College's data governance framework as it impacts the indigenous peoples in Australia and New Zealand. The Indigenous Data Guardian ensures the collection, managing, storing and sharing of indigenous data is conducted based on the principles agreed with the College's Indigenous Committees. Separate roles exist for Australia and New Zealand. A Māori Data Guardian is the New Zealand (indigenous) data guardian.
Kaitiakitanga	guardianship – considerations about guardianship, ethics and restrictions

Kotahitanga	collective benefit – considerations about benefit, building capacity and connecting
Manaakitanga	reciprocity – considerations about respect and consent
Māori	the Indigenous People of Aotearoa
Māori Data	Māori data refers to digital or digitizable information or knowledge that is about or from Māori people, our language, culture, resources or environments.
Māori Data Governance	Māori Data Governance refers to the principles, structures, accountability mechanisms, legal instruments and policies through which Māori exercise control over Māori data.
Māori Data Sovereignty	Māori Data Sovereignty refers to the inherent rights and interests that Māori have in relation to the collection, ownership, and application of Māori data.
Rangatiratanga	authority – considerations about jurisdiction, control and self determination
Whakapapa	relationships – considerations about context, disaggregating data and future use
Whanaungatanga	obligations – considerations about balancing rights and accountabilities

Reviewed Documents

The documents listed below were reviewed as part of developing the Māori data governance guidelines for RACP

Document	Version	Date
AIDA Data Collection Letter	NA	21 May 2021
Brief to DGG - Standardising Collection of Member Indigenous Identity Data	NA	22 February 2022
Brief to SLT - Half year report	NA	30 June 2024
Combined Australian and Aotearoa Classification of Ethnicities	NA	Unknown
Data Governance Policy - Final	2.0	4 March 2024
Guideline for Collecting Diversity Data of College members	NA	September 2024
Indigenous Data Governance Policy	NA	1 January 2024
Member Data Request Form_External Data Request_2020	NA	2020
MHC Brief on Māori data governance draft	NA	29 August 2024
MHC By-law_Board Approved_16.02.24	3.0	6 March 2024
RACP Constitution	NA	May 2023
RACP-member-statistics-and-insights-report-2023	NA	June 2023
Record Management Policy	1.0	3 January 2023
Statement of Principles for Justice and Equity_4	NA	Unknown

Document History

Summary of changes	Version	Date
First iteration of the Māori data governance guidelines	0.1	8th Nov 2024
Version 1 following feedback: Dr Samantha Jackson (Māori Health Registrar) and Nicky McCurdy, (Kaitohutohu Ahurea), and Dr Tawera Wharetohunga (Māori Health Registrar). Additional detail added relating to implementation in particular building up capability, guidance on data collection	1.0	20th Dec 2024