NSW GOVERNMENT

6 August 2021

Patient Reported Measures Data Governance and Management Framework

The Agency for Clinical Innovation (ACI) is the lead agency for innovation in clinical care.

We bring consumers, clinicians and healthcare managers together to support the design, assessment and implementation of clinical innovations across the NSW public health system to change the way that care is delivered.

The ACI's clinical networks, institutes and taskforces are chaired by senior clinicians and consumers who have a keen interest and track record in innovative clinical care.

We also work closely with the Ministry of Health and the four other pillars of NSW Health to pilot, scale and spread solutions to healthcare system-wide challenges. We seek to improve the care and outcomes for patients by re-designing and transforming the NSW public health system.

Our innovations are:

- person-centred
- clinically-led
- evidence-based
- value-driven.

www.aci.health.nsw.gov.au

AGENCY FOR CLINICAL INNOVATION

1 Reserve Road St Leonards NSW 2065

Locked Bag 2030, St Leonards NSW 1590
T +61 2 9464 4666
E aci-info@nsw.gov.au | aci.health.nsw.gov.au

SHPN (ACI) 210784, ISBN 978-1-76081-911-8

Further copies of this publication can be obtained from
the Agency for Clinical Innovation website at www.aci.health.nsw.gov.au

Version: 1 **Trim:** ACI/D21/1929

Contents

1. Document control

1.1 Change record

Date	Author	Version	Change reference
14/08/2019	Brett Avery	0.1	Endorsed version by PRM Steering Committee
6/8/2021	Melissa Tinsley	0.2	Final review and design for publishing

1.2 Reviewers

Name	Position
Melissa Tinsley	Manager, Clinical Information and Decision Support, Agency for Clinical Innovation
John Marshall	Information Management & Analysis Officer, Clinical Monitoring, Economics and Evaluation, Agency for Clinical Innovation
George Leipnik	Director, Health System Support Group, Ministry of Health
Briony Jack	Principal Project and Policy Officer, Health System Support Group, Ministry of Health
Sharon Smith	Executive Director, System Information & Analytics Branch, Ministry of Health
Liz Hay	Director, Economics and Analysis, Strategic Reform & Planning Branch, Ministry of Health
Natalie Cook	NSW/ACT Primary Health Network Coordinator
Louise Fischer	Director, Systems Integration Monitoring & Evaluation, Ministry of Health

1.3 Approvers list

Key stakeholder (individual / group)	Version	Date
PRM Steering Committee	0.2	29/06/2021

2. Introduction

2.1 Background

The Patient Reported Measures (PRM) program endeavours to support patients and clinicians and add value to their interactions. The program is divided into two sections:

- **Patient Reported Outcome Measures (PROMs)** are used to help assess and follow up a patient's clinical progress;
- **Patient Reported Experience Measures (PREMs)** help to assess the patient's experience of health care.

Establishing the Data Governance and Management Framework (the Framework) for the PRM data held by the Health Outcomes and Patient Experience (HOPE) information system is required to:

- enable decision making though clarity on roles, responsibilities and accountabilities;
- establish consistent policies and standard operating procedures;
- establish the foundation on which additional data-driven value-added services can be supported and delivered (for primary and secondary uses);
- provide ongoing alignment with current privacy and related policies and legislation;
- provide clarity and understanding of the various stakeholders and their role in ensuring overall quality and integrity of PRM data held within the NSW health system data;
- enable and support the goals to improve responsiveness in meeting the demands of a changing health system and to ensure ongoing benefits to patients and the NSW health system.

2.2 Objective

The focus of the Framework for the PRM data held by the HOPE information system is to establish the effective governance and management of PRM data as an important strategic asset for the NSW health system. The Framework aims to answer the following key questions:

1. What is the intended use of PRM data?
2. How will PRM data be governed?
3. What are the primary roles and who is accountable?
4. What policies and procedures are required?

2.3 Expected benefits

Implemented effectively, the Framework for PRM data held within the HOPE system will:

- **ensure decision making** through the clear articulation of data governance processes and structures for communicating complex activities and decisions;
- **reduce operational friction** due to a clear alignment between data governance and technology governance;
- **minimise the risk** of poor data integrity through well-coordinated and efficient assurance processes that provide confidence that the HOPE system is a trusted source for PRM data;
- **well-orchestrated processes and procedures** for the management of the HOPE system;
- **reduce waste and administrative costs** by defining clear roles and responsibilities for data management;
- **ensure transparency** over roles, responsibilities and accountabilities at all times;
- **identify known roles**, their responsibilities, and the escalation route to reduce time and effort for resolving data issues; and
- **provide the ability to verify** PRM data is fit for its intended use.

3. Purpose and scope

3.1 Purpose

The purpose of the Framework is to outline the principles and arrangements for the NSW health system to ensure effective management and governance of the PRM data held by the HOPE system. The Framework provides the stakeholders of PRM data with an instrument to govern PRM data assets effectively through the exercise of authority and control (planning, guiding and monitoring) over the management of these assets.

Additionally, the Framework defines the processes that acquire, control, protect, deliver and enhance the value of PRM data as an important strategic asset for the NSW health system.

3.2 Scope

The Framework:

- applies to all PRM data held within the HOPE system, and specifically the PROMs and PREMs collected by patients and used by clinicians;
- establishes the guidelines in relation to data-related activities and functions in the governance and management of PRM data, including the decisions on creating, modifying, retiring and business-as-usual management of PRM data health in the HOPE system;
- focuses on the roles and responsibilities of NSW Health entities in the management and governance of PRM data, with recognition of the proposed role and responsibilities of General Practices and Primary Heath Networks (PHNs).

This Framework does not apply to PRM data assets held within the Enterprise Data Warehouse for Analysis, Reporting and Decision Support (EDWARD) or included in clinical or public health registries such as Register of Outcomes, Value and Experience (ROVE). These assets are subject to their own data governance and management frameworks. PREM data collected through other surveys such as the Bureau of Health Information (BHI) survey are also exempt.

3.3 Audience

This document contains key information for all parties involved in the governance and management of PRM data; particularly those who have delegated authority to make data-related decisions. It is also an important source of information for NSW Health, including LHDs, SHNs, Pillars, Ministry of Health (Ministry) and agencies or General Practices that provide PRM data to, or receive PRM data from, the HOPE system. This also includes stakeholders, end users, and application support services of the HOPE system.

3.4 Review of the Framework

The Framework will be subject to regular review. The first review will occur during the pilot phase before the broad engagement and adoption of PRMs by General Practices. This review will consider:

- the capacity and capability of NSW Health entities and General Practices to meet the responsibilities of the data governance roles;
- the role of PHNs in supporting General Practices; and
- any changes to the governance structure for PRMs within NSW Health.

3.5 Definitions, acronyms, and abbreviations

A glossary of terms and acronyms used within this document are contained in the following tables.

Table 1: Glossary

Term	Meaning
Clinical Quality Registry (CQR)	CQR systematically monitors the quality (appropriateness and effectiveness) of health care, within specific clinical domains, by routinely collecting, analysing and reporting health-related information. Data collected is used to identify benchmarks and variation in clinical outcomes and is provided back to clinicians, patients and health system managements to inform clinical practice and decision making. ***Note:*** *It is the strategic intent of NSW Health to support 'virtual' registries that use linked data to provide clinicians, patients and health system managers with timely feedback on clinical practice against agreed indicators of quality that are benchmarked, risk-adjusted and based on reliable data.*
Data asset	Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a website that returns data in response to specific queries (e.g., www.weather.com) would be a data asset. ***Source:*** CNSSI 4009-2015
Data governance	Is "…a system of decision rights and accountabilities for information related processes, executed according to agreed-upon models which describe who can take what actions, with what information, and when, under what circumstances, using what methods." ***Source:*** Data Management Book of Knowledge (DMBOK)

Term	Meaning
Data linkage	Is "…the bringing together of two or more datasets to create a new, richer dataset". When patients use different health services, information about them is captured in different datasets. Data linkage brings together multiple sets of data about patients to provide a more complete picture of their journey in the health system, including the outcomes of their healthcare By bringing together sets of data that were previously isolated, researchers, clinicians and governments can deepen their understandings of the ways people use the health care system. ***Source:*** National Statistics Service, *Data linking: What is data linking? (Information Sheet)*
Data management	Is "…the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets." ***Source:*** Data Management Book of Knowledge (DMBOK)
Data re-identification	Any process by which data is matched to its true owner after it has been released in de-identified form.
Disclosure	Refers to the communication or transfer of information outside an organisation
Encounter	An encounter is a patient's contiguous contact with an organisation health service provider. In the admitted patient setting, an encounter represents a stay in hospital, which may include one or more service event. In community health settings it may represent a course of treatment or care by one health service team for a particular problem or set of problems. In emergency department settings, the service encounter and service event represent the same occasion of assistance received by a client from the health service provider. ***Note:*** A patient questionnaire is linked to a patient's medical record through the encounter.
Human Research Ethics Committee (HREC)	HREC is a committee constituted in accordance with National Health and Medical Research Council (NHMRC) Ethics Committee guidelines, which protects the subjects of research and ensures that ethical standards are maintained by reviewing and advising on the ethical acceptability of research proposals.

Term	Meaning
State-wide data asset	A data collection, data stream, or dataset, held by a NSW Health entity including the Ministry of Health, Local Health Districts, Specialty Health Networks, Shared Services, Agencies and Pillars.
Secondary use of health data	When personal health information is used outside of direct care delivery. It includes such activities as analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing, and other business applications.
Service event	An instance or occasion of assistance received by a client from a health service provider. Generally, a service event is described by a cluster of data elements that provide information about when it happened, where it happened, what assistance was received, how much and from whom. A service event is a more granular concept than an encounter. There may be multiple service events during an encounter.
Use	Refers to the communication or handling of health information within an organisation
Value added copies	Value added copies of the PRM data are considered ‘downstream’ and separate data assets subject to their own data governance and management framework.

Table 2: Acronyms

Acronym	Description
ACI	NSW Agency for Clinical Innovation
BHI	Bureau of Health Information
CQRs	Clinical Quality Registries
CUA	Conditions of Use Agreement
EDWARD	Enterprise Data Warehouse for Analysis, Reporting and Decision support
HOPE	Health Outcomes and Patient Experience
IDWG	Implementation and Design Working Group
IT	Information Technology
HREC	Human Research Ethics Committee
LHD	Local Health District
PHN	Primary Health Network
PREM	Patient Reported Experience Measure
PRM	Patient Reported Measures
PROM	Patient Reported Outcome Measure
ROVE	Register of Outcomes, Value and Experience
SHN	Specialty Health Network

4. Data governance context

4.1 Data governance concepts

There is a distinction between the related concepts of data governance, data management and information technology (IT) governance. Alignment of each of these concepts supports NSW Health in achieving its strategic objectives and effectively developing and utilising data resources.

- **Data governance** designates the source of authority for making decisions about data; the roles/structures authorised to make decisions; and the basis upon which decisions are made.
- **Data management** is the planning, execution and oversight of policies and processes that acquire, store, protect, and deliver data and information assets.
- **IT governance** describes processes that ensure the effective and efficient use of IT in enabling an organisation to achieve its goals.

Alignment of each of these concepts supports NSW health system in achieving its strategic objectives and effectively developing and utilising data resources.

4.2 Policy context

This Framework is compliant with relevant statutes, regulations and policies. It stipulates how the management and governance of PRM data is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations.

Obligations regarding data governance arise from State and Commonwealth statutes including:

- *Government Information (Public Access) Act 2009* (NSW) [https://www.legislation.nsw.gov.au/#/view/act/2009/52]
- *Health Records and Information Privacy Act 2002* (NSW) [https://www.legislation.nsw.gov.au/#/view/act/2002/71]
- *Health Administration Act 1982* (NSW) [https://www.legislation.nsw.gov.au/#/view/act/1982/135]
- *Mental Health Act 2007* (NSW) [https://www.legislation.nsw.gov.au/#/view/act/2007/8/whole]
- *Privacy Act 1988* (Cth) [https://www.legislation.gov.au/Details/C2019C00025]
- *Privacy and Personal Information Protection Act 1998* (NSW) [http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/]
- *Public Health Act 2010* (NSW) [https://www.legislation.nsw.gov.au/#/view/act/2010/127]
- *State Records Act 1998* (NSW) [http://www.records.nsw.gov.au/about-us/state-records-act-1998].

NSW Health also has common law obligations in relation to information obtained as part of the treating relationship.

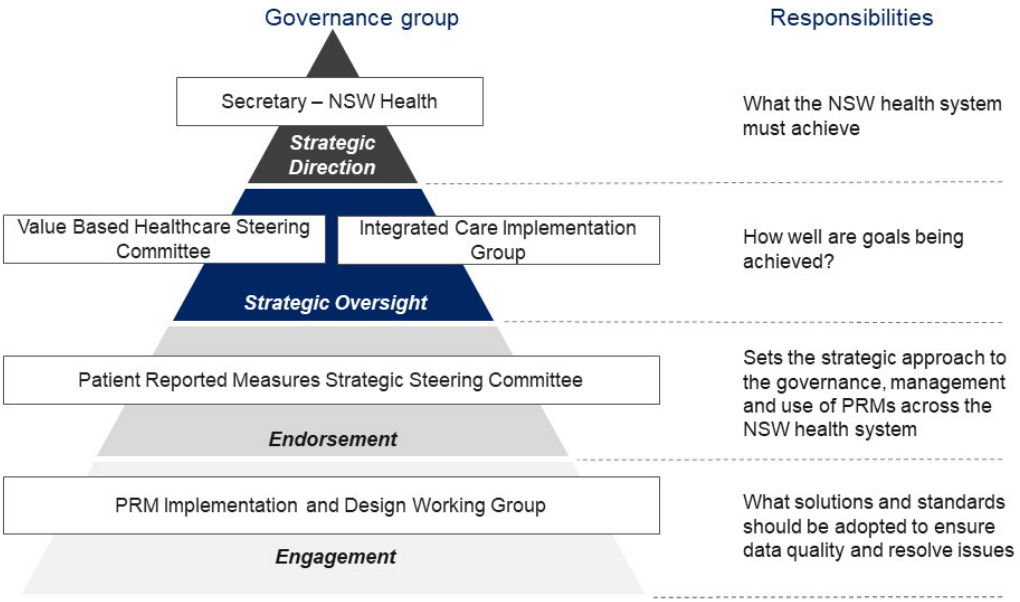
Data governance roles specified in this document are also subject to the:

- *Privacy Manual for Health Information (setting out operational aspects of the Health Records and Information Privacy Act)* https://www.health.nsw.gov.au/policies/manuals/Pages/privacy-manual-for-health-information.aspx
- NSW Health Combined Administrative Financial Staff Delegations Manual
- Health System Support Group Delegations Manual
- HealthShare NSW Delegations Manual
- Health Infrastructure Delegations Manual
- District, Network or Pillar Delegations Manual.

4.3 PRM strategic governance

The strategic governance structure, with clearly defined roles and responsibilities, identifies the governance and working group that are accountable for achieving the strategic goals for PRMs within the NSW health system.

Figure 1: PRM data governance strategic model



PRM data held by the HOPE system is governed by the strategic approach to build a PRM capability across the NSW health system. Building the capability requires maturity across people, process, technology in order to improve the management of PRM data from a strategic and operational perspective.

The space inside each level of the pyramid represents the rough percentage of instances each of the governance groups are expected to make decisions on the approach to continually build and mature the PRM capability.

The governance groups are accountable for the following areas of responsibilities:

- **Engagement** - LHDs, ACI, BHI, Cancer Institute, Ministry, eHealth NSW, and PHNs representing General Practice are engaged through the PRM Implementation and Design Working Group (IDWG) in order to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.

  From a PRM data perspective, the PRM IDWG makes decisions on data concepts (i.e. the taxonomy and data dictionary) for PRM data; the PRM Technical Design Working Group makes decisions on the data architecture and data sharing standards.

- **Endorsement** - The Patient Reported Measures Strategic Steering Committee sets the strategic approach to the governance, management and use of PRMs across the NSW health system.

  From a PRM data perspective, the Patient Reported Measures Strategic Steering Committee decides on the appropriate primary use and secondary re-use of PRM data.

- **Strategic oversight** - The Value Based Healthcare Steering Committee and the Integrated Care Implementation Group oversee how well strategic goals for PRMs are being achieved.

- **Strategic direction** - The Secretary of NSW Health defines the role of PRMs in achieving a value-based health system in NSW.

5. Guiding principles of the Framework

The Framework outlines a series of guiding principles used to manage the collection, use, sharing and release of PRM data for primary and secondary purposes. The table below contains a summary of the principles applied and are discussed in more detail throughout the Framework.

Guiding principles

5.1	**Primary and secondary uses of PRM data**
5.1.1	**Primary purpose and use** The HOPE system will support the primary purpose and use of PRM data and directly related secondary purposes, such as using PRM data for quality assurance activities.
5.1.2	**Secondary purpose and use** Secondary uses of PRM data for the management of health services and research will be facilitated through value added copies of the PRM data held within the HOPE system. These copies are considered separate data assets subject to their own data governance and management framework.
5.2	**Data governance model for PRM data held in the HOPE system**
5.2.1	**Data Sponsor** The Deputy Secretary, Health System Strategy and Planning at the Ministry is the *Data Sponsor* for the purposes of the Framework.
5.2.2	**Data Custodian** Chief Executives of NSW Health entities and General Practices will implement the Framework in the role of *Data Custodian* for PRM data held within the HOPE system.
5.2.3	**Centralised Data Steward** The Agency for Clinical Innovation (ACI), acting in the role of *Centralised Data Steward*, will be responsible for ensuring that the collection, use, sharing (and release) of PRM data is performed according to policies and practices as established by the Framework.
5.2.4	**Local Data Stewards** Local administrators of NSW Health entities and General Practices, acting in the role of *Local Data Stewards*, will be responsible for the day to day operation and implementation of the PRM data management plan within their healthcare provider organisation.

5.2.5	**Governance Group** The PRM Strategic Steering Committee, acting in the role of a *Governance Group*, will oversee the development and operation of the HOPE system.
5.2.6	**Working Groups** The PRM IDWG, acting in the role of a *Working* Group, will engage with key business and technology stakeholders in order to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.
5.2.7	**Privacy Officer** The NSW Health entity's or General Practice's privacy officer, ensuring privacy compliance on the collection, use and sharing of PRM data, will be responsible for providing assurance and advice on privacy issues.
5.2.8	**Security Officer** The NSW Health entity's or General Practice's security officer, ensuring security compliance on the collection, use and sharing of PRM data, will be responsible for providing assurance and advice on security issues.
5.2.9	**Data Specialists** The ACI data and information managers, acting in the role of *Data Specialist*, will provide for providing ongoing support to the PRM data held by the HOPE system through analysis and problem solving of PRM data related topics.
5.2.10	**Data Users** Patients, clinicians, managers or administrators who access, input, amend, delete, extract, and analyse PRM data held by the HOPE system, is responsible for the safety (privacy and security) and integrity of the PRM data.
5.2.11	**Third Parties** Organisations / individuals requesting access to PRM data for secondary use purposes are responsible for preparing an access request and committing to participating in the monitoring and assurance arrangements as stipulated by a conditions of use agreement.
5.2.12	**System Administrators** eHealth NSW, acting in the role of *System Administrator*, will be responsible for the analysis, design, implementation and maintenance of new, and changes on existing HOPE system data structures, and the storage and operations of PRM data held within the HOPE system.

5.3	**Data governance model for value added copies of PRM data**
5.3.1	**Accountability roles** Value added copies of the PRM data are considered separate data assets subject to their own data governance and management framework.
5.4	**Patient control of PRM data in the HOPE system**
5.4.1	**Conditions of consent** Patients providing consent to participate in the PRM program will need to agree to the conditions of consent, stating the intended primary and secondary use of their data.
5.4.2	**Withdrawal of consent** Patients can withdraw their consent to participate in the PRM program and their data being used for the primary purpose it was collected. Patients' PRM data may continue to be used for secondary purposes where data analysis projects request access to data collected during a period of time when consent had been provided.
5.5	**Collection and use PRM data for its primary purpose**
5.5.1	**Conditions of use** NSW Health entities and General Practices will need to enter into a NSW Health [conditions of use] agreement, stating the intended primary and secondary use of PRM data collected, and their roles and responsibilities in the collection, use, sharing, security and maintenance of PRM data.
5.6	**Use and disclosure of PRM data for a secondary purpose**
5.6.1	**Secondary use of PRM data** For applications requesting access to local PRM data (i.e. PRM data owned by one NSW Health entity or General Practice), the application should be directed to the Data Custodian for the requested PRM data held within the HOPE system. The Data Custodian will perform a data risk assessment and assurance process to assess the request for the secondary use of PRM data, approve / deny the request, and specify [in an agreement] what PRM data is available and the conditions of use.

5.6.2	**Secondary use of value added copies of PRM data** For applications requesting access to area-wide PRM data (i.e. PRM data owned by more than one NSW Health entity or General Practice), the application should be directed to the Data Custodian for the PRM data held within EDWARD. The Data Custodian will perform a data risk assessment and assurance process to assess the request for the secondary use of PRM data, approve / deny the request, and specify [in an agreement] what PRM data is available and the conditions of use.
5.7	**Protecting the privacy of individuals**
5.7.1	**Data safety** The Data Custodians of PRM data assets will regularly reconsider the privacy protection processes around primary and secondary use of PRM data, to maintain an acceptable level of protection to ensure privacy, security and confidentiality of PRM data.
5.8	**Fit for purpose**
5.8.1	**Data quality** The Centralised Data Steward will establish a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the PRM data, for primary and secondary use.
5.9	**Risk mitigation strategies**
5.9.1	**Risk of breach** The Data Custodians of PRM data assets will ensure that the risk of a breach of privacy for an individual is reduced to an acceptable level by minimising the risks associated with the collection, use, sharing (and release) of PRM data for primary and secondary purposes.
5.10	**Effective governance**
5.10.1	**Framework review** As part of the ongoing better practice of effectively managing and governing PRM data, the Framework will be reviewed every year or when there are material changes either to either the strategic governance of PRMs or to policies and legislation that impact on data governance.

5.1 Primary and secondary uses of PRM data

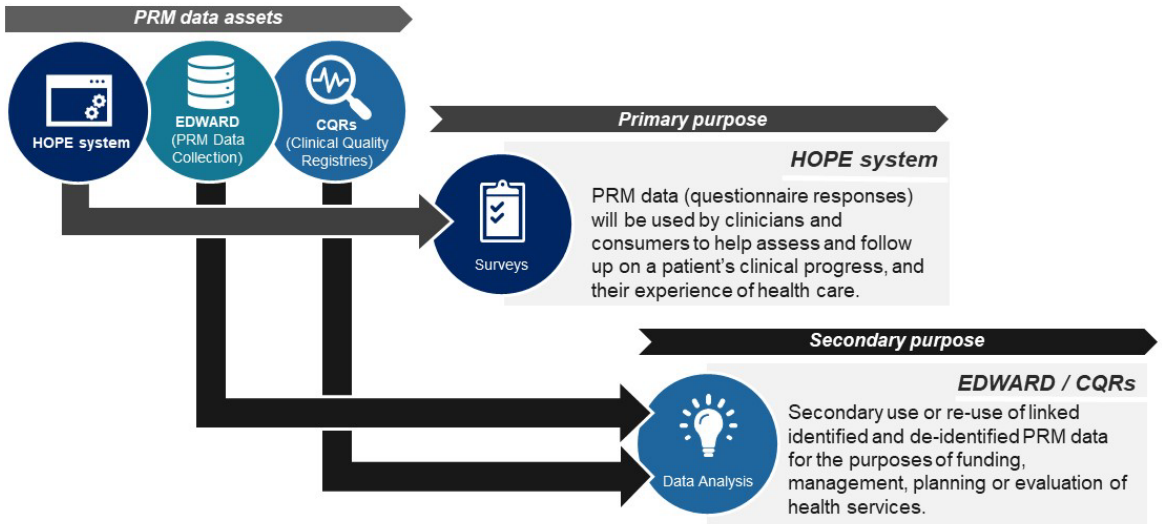
Guiding principles

5.1	Primary and secondary purpose and use of PRM data
5.1.1	**Primary purpose and use** The HOPE system will support the primary purpose and use of PRM data and directly related secondary purposes, such as using PRM data for quality assurance activities.
5.1.2	**Secondary purpose and use** Secondary uses of PRM data for the management of health services and research will be facilitated through value added copies of the PRM data held within the HOPE system. These copies are considered separate data assets subject to their own data governance and management framework.

PRM data holdings and intended use

PRM data will be held by a number of information systems, including the HOPE system where PRM data is collected for primary use and directly related secondary use; and in support of secondary use, value added copies of the PRM data held within the HOPE system (including a state-wide data collection held within EDWARD, and clinical quality registries (CQRs)).

Figure 2: PRM data assets and their intended purpose



Registries

There are a number of different registry formats including those virtual registries established under the *Public Health Act 2010* (NSW). Other registries follow a more traditional format of directly collecting data using Clinical Quality Registries. In the future, NSW Health will focus on ensuring that registries produce a desired outcome in that registries are a mechanism to provide clinicians, patients and health system managers with timely feedback on clinical practice against agreed indicators of quality that are benchmarked, risk-adjusted and based on reliable data. The strategy should allow for a multi-dimensional approach whereby different means of achieving the desired outcome can co-exist and complement each other.

Future efforts will focus on enhancing existing electronic medical record systems to reliably and accurately capture relevant data elements that can be extracted and used to create 'virtual registries'. This may include linkage to other health and non-health datasets to capture relevant patient outcomes. This approach has the potential to provide a holistic person-centred perspective rather than a disease specific focus and provide data back to stakeholders in a timelier manner.

NSW Health will continue to focus on enabling the establishment of virtual registries and will prioritise virtual registry development based on NSW Health system priorities. Within this context PRMs data may form an important part of this registry strategy.

An example that proposes to use PRM data is a Register of Outcomes, Value and Experience (ROVE). ROVE intends to use PRM data, linked to other administrative and clinical outcomes / process data in order to conduct a number of analyses associated with the patient journey across care settings, sustainability, evaluation and monitoring. ROVE also intends to evaluate the effectiveness of interventions; evaluate and monitor models of care; and provide risk-adjusted, benchmarked feedback on clinical practice and patient outcomes.

5.1.1 Primary purpose and use

PRM data (questionnaire responses) will be collected by patients and used by clinicians to contribute directly to the care and treatment of patients. PRMs will be used by patients and caregivers to help decide their choice of treatment, and to improve their ability to manage the quality of care received as relevant to their health care needs.

The primary use for PRM data relates to the two main categories of PRMs. Generally, NSW Health entities and general practices may use and disclose PRM data only for the primary purpose for which PRMs were collected.

a) Patient-Reported Outcome Measures (PROMs)

PROMs are directly reported by the patient without interpretation by a clinician or anyone else associated with healthcare or treatment. They measure patients' perceptions of their health status, clinical outcomes, mobility and quality of life.

PROMs are used to report outcomes for certain patients as a method for collecting information of the effectiveness / impact of patient care within the NSW health system from the patient perspective.

b) Patient-Reported Experience Measures (PREMs)

PREMs ask patients to describe, rather than simply evaluate, what happened during their encounters with health services. They measure a patient's perception of their experience of care.

PREMs are used to report experience for certain patients as a method for collecting information of the effectiveness / impact of patient care with the NSW Health system from the patient perspective. These indicators may include respect for patient-centered values, preferences, and expressed needs; coordination and integration of care; information, communication, and education; physical comfort; emotional support; welcoming and involvement of family and friends; transition and continuity; and access to care.

5.1.2 Secondary purpose and use

Opportunities exist for secondary use or re-use of linked identified or de-identified PRM data for the purposes of funding, management, planning or evaluation of health services (dependent on the legal basis for linkage), including:

- the measurement and monitoring of the impact of treatments for diseases and conditions;
- the measurement and monitoring of the impact of health services;
- the planning of health programs, or treatments or services;
- the evaluation of health programs, or treatments or services.

For PRM data to be used for a secondary purpose (other than the primary purpose it was collected), there must be a legal basis for the use and disclosure of the data. Health Privacy Principle 10 and 11 of the *Health Records and Information Privacy Act 2002* state the legal basis for the use or disclosure of PRM data.

This includes (but not limited to):

1. **Consent** – the need for consent from an individual whom the PRM data relates to for the use or disclosure of PRM data for a secondary purpose;
2. **Direct relation** – the secondary purpose being directly related to the primary purpose of PRM data and the individual would reasonably expect PRM data to be used for the secondary purpose;
3. **Management of health services** – the use or disclosure of PRM data for the secondary purpose is reasonably necessary for the funding, management, planning, quality improvement or evaluation of health services;
4. **Training** – the use or disclosure of PRM data for the secondary purpose is research necessary for the training or employees of the NSW Health entity or general practice;
5. **Research** – the use or disclosure of PRM data for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest consistent with existing processes for the use of any health data for research purposes.

The following clauses of Principle 5.1.2 *Secondary purpose and use* are provided as guidance only. Any decision to use of PRM data for a secondary purpose must be in accordance with the *Privacy Manual for Health Information*, *Health Records and Information Privacy Act 2002* and its Statutory Guidelines, and the

NSW Combined Delegations Manual. If there is uncertainty as to the legal basis for the use and disclosure of data, the Ministry's Legal and Regulatory Service branch should be consulted.

a) Secondary uses that are permitted

Permitted secondary uses of PRM data include some that are considered 'directly related' to the primary purpose (i.e. quality assurance) and others which are more remote (i.e. management of health services and research).

NSW Health entities and General Practices may use and disclose PRM data for any secondary purpose if patient consent has been given. PRM data can be used or disclosed without consent of the patient when there is a directly related secondary purpose that is within the reasonable expectations of that patient.

Permitted secondary uses that fall within a 'directly related purpose' to the primary purpose include but may not be limited to:

- disclosing PRM information to the patient's nominated GP, other treating health services or medical specialists involved in the care and treatment of a patient
- providing relevant health information (revealed by PRMs) to carers to assist with care for the patient
- sending reminders to a patient for a patient to complete a patient outcome questionnaire before presenting to a health service for follow up care and treatment
- contacting a patient for further information on the feedback on the service received based on the patient experience questionnaire for the purpose of evaluation and improvement of the service
- improvement of existing health service (e.g. evaluate the health care in terms of clinical effectiveness and impact of intervention and care over time)
- using information for quality assurance or clinical audit activities carried out by the health service such as monitoring, evaluating, auditing the provision of the particular service the health service has or is providing the person (in considering the operation of the clinical service from the perspectives of funding, planning, safety and quality improvement activities)
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating, auditing the provision of a particular clinical service the health service has provided or is providing to the person (as long as the individual reviewing the health records is bound by privacy legislation or a professional code of ethics).

Secondary uses that fall outside a 'directly related purpose' and are related to the management of health services, training, and research that are permitted include but may not be limited to:

- provision of data for linkage for agreed purposes (e.g. those purposes specified in the *Public Health Act*, research)
- development of clinical decision support systems (e.g. link data on individual's health with PRM data to influence treatment choices at point of care)
- evaluation of health interventions and/or health programs (e.g. determine if an intervention or service is generating outcomes/benefits consistent with investment decisions)

- quality improvement in health care service delivery (e.g. using PRMs to better enable benchmarking between services and interventions for continuous quality improvement)
- health services research relevant to public health (e.g. aggregated PRM data used for evaluation and research to understand patient needs, preferences and adherence or impact of treatment and care)
- construction of registries (e.g. create or supplement data in registries, such as those established under the provisions of the *Public Health Act* e.g. ROVE, other clinical quality registries or other existing registries).
- develop/enable technology innovations (e.g. develop software applications that support patient's making informed choices of health services and interventions that are appropriate for their health status and life situation)
- development of health policy (e.g. establish and evaluate policies to benefit whole populations)
- preparation of publications (e.g. on the appropriateness and value of established health care services).

b) Secondary uses that are not permitted

Secondary uses that are not permitted include but may not be limited to:

- remuneration of individual clinicians (e.g. to make/modify payments)
- individual clinician audit (note: this does not exclude examining practice variations for the purposes of quality improvement or adherence to best-practice guidelines at a health service level)

5.2 Data governance model for PRM data held in the HOPE system

Guiding principles

The Data Governance roles are consistent with the NSW Health Data Governance Framework and ownership follows the delegation manuals for data ownership.

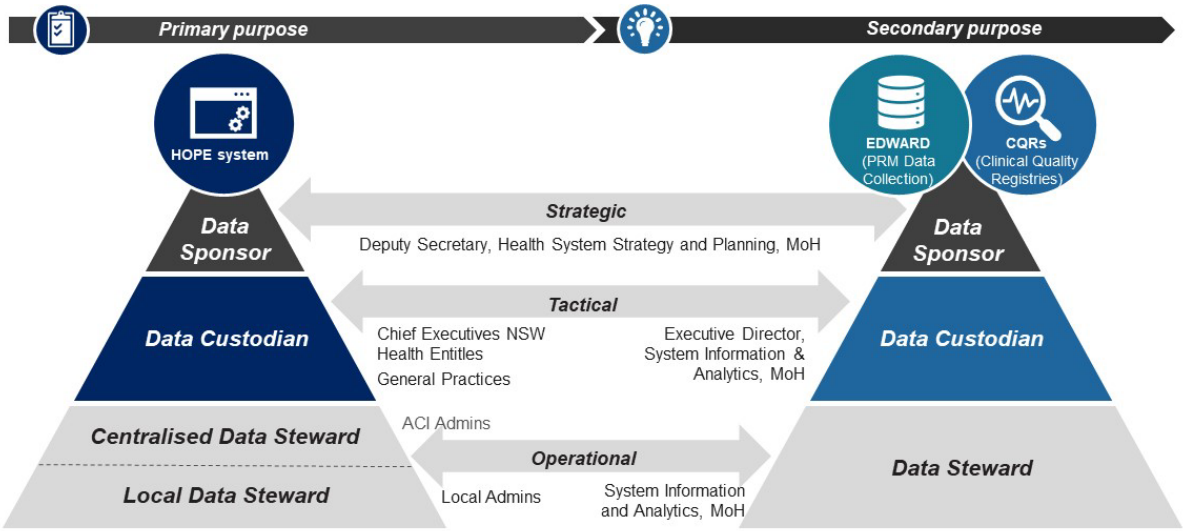
5.2	Data governance model for PRM data held in the HOPE system
5.2.1	**Data Sponsor** The Deputy Secretary, Health System Strategy and Planning at the Ministry is the *Data Sponsor* for the purposes of the Framework.
5.2.2	**Data Custodian** Chief Executives of NSW Health entities and General Practices will implement the Framework in the role of *Data Custodian* for PRM data held within the HOPE system.
5.2.3	**Centralised Data Steward** The Agency for Clinical Innovation (ACI), acting in the role of *Centralised Data Steward*, will be responsible for ensuring that the collection, use, sharing (and release) of PRM data is performed according to policies and practices as established by the Framework.
5.2.4	**Local Data Stewards** Local administrators of NSW Health entities and General Practices, acting in the role of *Local Data Stewards*, will be responsible for the day to day operation and implementation of the PRM data management plan within their healthcare provider organisation.
5.2.5	**Governance Group** The PRM Strategic Steering Committee, acting in the role of a *Governance Group*, will oversee the development and operation of the HOPE system.
5.2.6	**Working Groups** The PRM IDWG, acting in the role of a *Working* Group, will engage with key business and technology stakeholders in order to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.

5.2.7	**Privacy Officer** The NSW Health entity's or General Practice's privacy officer, ensuring privacy compliance on the collection, use and sharing of PRM data, will be responsible for providing assurance and advice on privacy issues.
5.2.8	**Security Officer** The NSW Health entity's or General Practice's security officer, ensuring security compliance on the collection, use and sharing of PRM data, will be responsible for providing assurance and advice on security issues.
5.2.9	**Data Specialists** The ACI data and information managers, acting in the role of *Data Specialist*, will provide for providing ongoing support to the PRM data held by the HOPE system through analysis and problem solving of PRM data related topics.
5.2.10	**Data Users** Patients, clinicians, managers or administrators who access, input, amend, delete, extract, and analyse PRM data held by the HOPE system, is responsible for the safety (privacy and security) and integrity of the PRM data.
5.2.11	**Third Parties** Organisations / individuals requesting access to PRM data for secondary use purposes are responsible for preparing an access request and committing to participating in the monitoring and assurance arrangements as stipulated by a conditions of use agreement.
5.2.12	**System Administrators** eHealth NSW, acting in the role of *System Administrator*, will be responsible for the analysis, design, implementation and maintenance of new, and changes on existing HOPE system data structures, and the storage and operations of PRM data held within the HOPE system.

PRM data governance models

Each PRM data asset is subject to its own data governance and management framework.

Figure 3: PRM data governance models

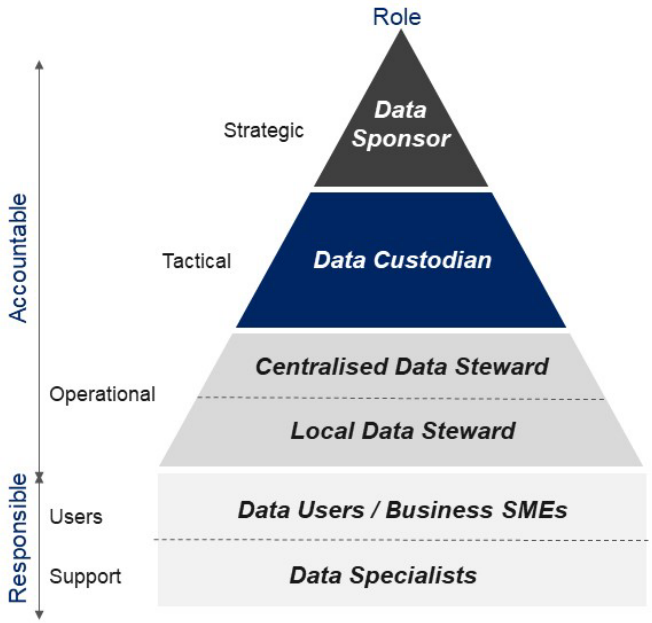


Secondary uses of PRM data will be facilitated through value added copies of the PRM data. These copies are considered separate data assets subject to their own data governance and management framework.

Accountability roles

Roles and responsibilities in the creation, ownership, management and operation of PRM data held by the HOPE system are outlined in the governance structure below. It provides an escalation and approval path for each governance group where issues / decisions at the operational level may need to be deferred to tactical or strategic level.

Figure 4: PRM data governance operating model of roles and responsibilities



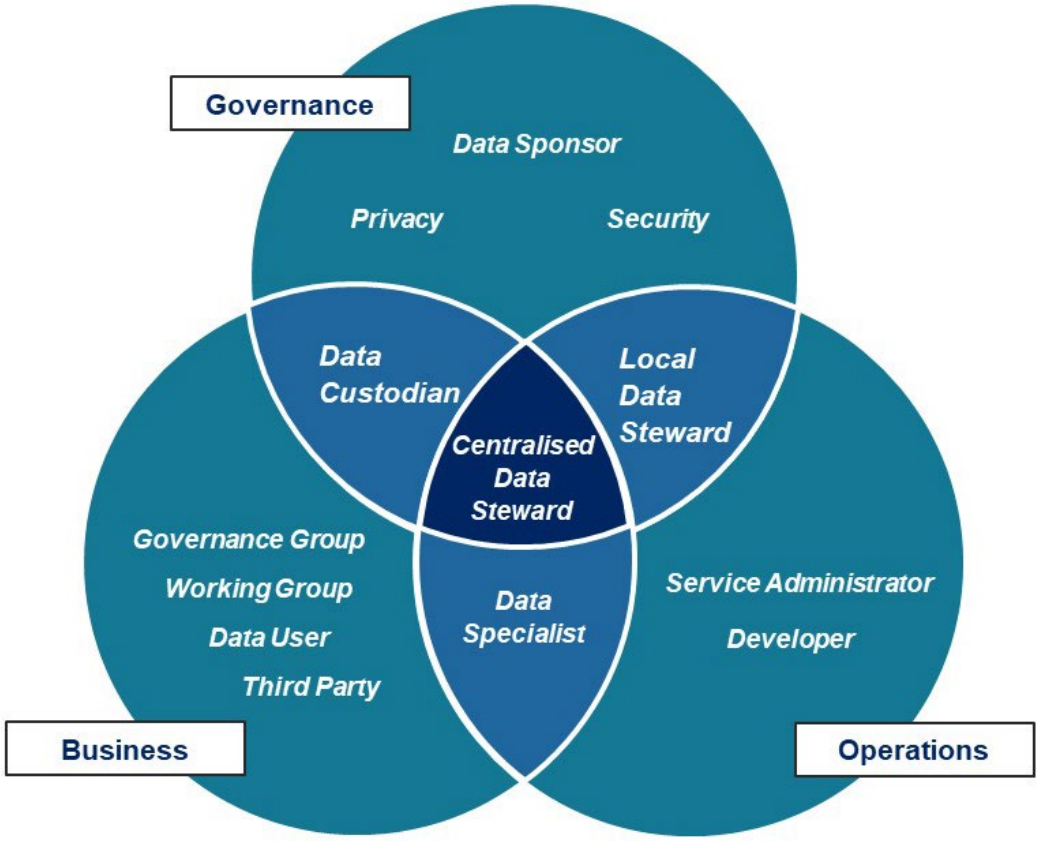
Responsible party	Key responsibilities
Deputy Secretary, Health System Strategy and Resources	Controls the strategic direction of PRMs and has full accountability on behalf of the NSW health system.
Chief Executives of *LHD / SHNs* (with data delegations*) General Practices	Day to day oversight of unit-level PRM data; approval of access to PRM data.
ACI Administrators	Ensure PRM data-related work is performed according to policies and practices as established by the Framework.
Local Administrators	Day to day operation and implementation of PRM data management within their healthcare provider organisation.
Administrators, Clinicians, Clerks, Patients, Carers	Any User that has access to the HOPE system is entrusted with the protection of PRM data.
Administrators, Application Support Services	Creating PRM survey templates; identifying data quality issues and implementing application fixes.

The space inside each level of the pyramid represents the rough percentage of instances each role is expected to make decisions about PRM data. The data governance roles and key responsibilities aligns with the NSW Health Data Governance Framework to ensure decision making through the clear articulation of data for communicating data-related issues and decisions.

Accountability responsibilities

The key roles and responsibilities for governing the collection, use, sharing, security and maintenance of PRM data held within the HOPE system are summarised in Figure 5.

Figure 5: PRM accountability responsibilities



5.2.1 Data Sponsor

The Data Sponsor controls the strategic direction of PRMs and has full accountability on behalf of the NSW health system The Data Sponsor champions the importance of the PRM program and associated information management and is responsible for overseeing the continuous improvement of PRM data governance and management.

a) Key accountabilities

- Establish the basis for the PRM data asset held by the HOPE system;
- Enable strategic management, governance and operation of the PRM data;

- Provide direction and guidance, and authorise appropriate resources for management of PRM data;
- Implement the PRM Data Governance and Management Framework for the PRM data;
- Authorise any public release of information, except where this authority is delegated by the Combined NSW Health Delegations Manual;
- Ensure compliance with all relevant legislation, policies and standards;
- Appoint Data Custodians and ensure the Data Custodians' duties are fulfilled.

b) Responsible party

- Deputy Secretary, Strategy and Resources, Ministry of Health.

c) Contact when

- Lines of business are established or changed that require information and records management roles;
- New / changes policy or legislation is proposed;
- Compliance issues arise;
- Need resourcing for information management responsibilities.

5.2.2 Data Custodians

The Data Custodian has operational responsibilities of day to day oversight of unit-level PRM data; approval of access to PRM data; approval of access to data and the overall quality and security of the data. The data custodian is the delegated "owner" of the PRM data.

a) Key accountabilities

- Ensure that: any use of the PRM data aligns with the purpose for which it was collected; there are up-to-date technical documents for the supply and storage of PRM data; PRM data remains relevant to system and business needs;
- Ensures the value of PRM data is maximised through sharing;
- Control access to data in compliance with all relevant legislation, policies and standards, and any conditions specified by the Data Sponsor;
- Considers requests for the secondary use of PRM data, approves / denies these requests and specifies what data is available for secondary use;
- Regularly review users with access to PRM data and the ongoing need and appropriateness of access;
- Establish and maintain an acceptable level of protection to ensure privacy, security and confidentiality of PRM data;
- Ensure there is a documented process for responding to breaches and potential breaches of data security, or the data asset's policies and procedures.

b) Responsible party

- Chief Executives of LHDs, SHN (with data delegations);
- General Practices.

c) Contact when

- A major business need for data is identified;
- Issues arise concerning data policy, business value, scope, security.

5.2.3 Centralised Data Stewards

The Centralised Data Steward is an inclusive role that accepts one or more negotiated stewardship activities on behalf of the Custodian. Stewards have the operational or technical ability to collect, deliver or maintain PRM data. Note, a Data Custodian cannot transfer accountability to the Centralised Data Steward, although the Steward may be responsible for specific activities.

a) Key accountabilities

- Manage the PRM data in compliance with relevant legislation, policies and standards, and any conditions specified by the Data Sponsor;
- Classify and approve the use of PRM data to Data Users (including Local Administrators) based upon the appropriateness of the user's role and the intended use (refer to Principle 5.5.1 for HOPE system roles);
- Ensures that all Data Users are appropriately trained and are aware of their obligations in the protection of PRM data;
- Provide advice to Data Custodian(s) and the Data Sponsor on the management of PRM data as required;
- Establish a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the PRM data held within the HOPE system;
- Ensure processes are in place to provide feedback to Local Data Stewards about data quality including issues requiring rectification;
- Provide feedback to Local Data Stewards in relation to data quality issues.

b) Responsible party

- ACI employees assigned the role of *ACI Administrator* (refer to Principle 5.5.1 for specific conditions of use).

c) Contact when

- When operational needs arise.

5.2.4 Local Data Stewards

The Local Data Stewards undertake day to day operation and implementation of PRM data management plan within their healthcare provider organisation. They have detailed knowledge of data structure, content, and appropriate use of the information for their areas, develops and sets data management standards approved by the Data Custodian.

a) Key accountabilities

- Management and oversight of the PRM data held in the HOPE system to help provide Data Users with high-quality PRM data that is easily accessible in a consistent manner;
- Approve the use of PRM data (under delegation from a Data Custodian) to Data Users, based upon the appropriateness of the user's role and the intended use (refer to Principle 5.5.1 for HOPE system roles);
- Ensures that all Data Users are appropriately trained and are aware of their obligations in the protection of PRM data;
- Provide advice to Data Custodian and Central Data Steward on the management of PRM data held within the HOPE system as required;
- Provide feedback to Data Users in relation to data quality issues;
- Ensure processes are in place to provide feedback to Data Users about data quality including issues requiring rectification;
- Escalate material risks and issues to their Data Custodian.

b) Responsible party

- NSW Health entity and General Practice employees assigned the role of *Local Administrators* (refer to Principle 5.5.1 for specific conditions of use).

c) Contact when

- Data access is required, within the scope of their organisation;
- Operational, business, or data definition issues arise or cannot be resolved, or data errors are perceived;
- Further detailed information about their organisation's PRM data is required;
- Further data services are required to meet new business needs for PRMs;
- Data management planning is required, or additional data may be encompassed within their business scope.

5.2.5 Governance group

Collectively define the strategic scope of PRMs and overall business services.

a) Key accountabilities

- Defines the role of PRMs in achieving a value-based health system in NSW;
- Oversees how well strategic goals for PRMs are being achieved;
- Sets the strategic approach to the governance, management and use of PRMs across the NSW health system;
- Decides on the appropriate primary use and secondary re-use of PRM data;
- Ensures Data Custodians liaise between their organisations and others;
- Establishes and resources the areas of data responsibility;
- Approves organisation policies related to PRMs;
- Oversees compliance with legislation, policies and standards;
- Formally recognises and communicates the importance of information to the business.

b) Responsible parties

- Value Based Healthcare Steering Committee;
- Integrated Care Implementation;
- Patient Reported Measures Strategic Steering Committee.

c) Contact when

- New/changed policy or legislation is proposed;
- Compliance issues arise;
- Need resourcing for data responsibilities.

5.2.6 Working Groups

Engage with key business and technology stakeholders in order to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.

a) Key accountabilities

- Makes decisions on data concepts (i.e. the taxonomy and data dictionary) for PRM data;
- Makes decisions on the data architecture and data sharing standards.

b) Responsible parties

- PRM Clinical Design & Measurement Working Group;
- PRM Technical Design Working Group.

c) Contact when

- A need for a new business function(s) or new application functions(s) is identified.

5.2.7 Privacy Officer

Responsible for enterprise wide approach to privacy and is responsible for providing leadership, assurance and advice on privacy issues.

a) Responsibilities

- Setting the vision for privacy across the organisation;
- Ensuring privacy compliance with the strategic direction of government;
- Engaging with the Office of the Privacy Commissioner, and clients;
- Ensuring strategic and operational plans for privacy are developed;
- Establishing and promoting the organisation's privacy policies, in alignment with National and State policies and standards.

b) Responsible parties

- NSW Health entity or General Practice privacy officer.

c) Contact when

- Privacy compliance issues arise;
- Strategic direction of PRMs changes;
- Information management policy amendments or new policy is required.

5.2.8 Security Officer

Responsible for enterprise wide approach to security and is responsible for providing leadership, assurance and advice on security issues.

a) Responsibilities

- Setting the vision for security across the organisation;
- Ensuring security compliance with the strategic direction of NSW government;
- Ensuring strategic and operational plans for security are developed;

- Establishing and promoting the organisation's security policies, in alignment with National and State policies; and standards.

b) Responsible parties

- NSW Health entity or General Practice chief security officer.

c) Contact when

- Security compliance issues arise;
- Strategic direction of PRMs changes;
- Information management policy amendments or new policy is required.

5.2.9 Data Specialists

The Data Specialists are the business and technical subject matter experts responsible for providing ongoing support through analysis, and problem solving PRM data related topics, including data design, data relationships, data quality, and data modelling. The Data Specialist has access to and makes sense of information contained, albeit hidden, in the organisation. It's a critical role for business decision-making.

a) Responsibilities

- Understand high-level requirements of the business and provide solutions related to business strategies;
- Translate business and technical jargon to understandable language for different audience;
- Creating PRM survey templates; identifying data quality issues and implementing application fixes;
- Assist Data Users in their requirements;
- Promote comprehensive PRM data use within the NSW Health system.

b) Responsible parties

- ACI data and information managers assigned the role of *ACI Administrator* (refer to Principle 5.5.1 for specific conditions of use).

c) Contact when

- Insight is needed for changed or new strategies to meet business outcomes for PRM.

5.2.10 Data Users

Data Users are patients, clinicians, managers or administrators who access, input, amend, extract, and analyse PRM data held by the HOPE system to carry out their day to day duties. Appropriate security and approval is required from Data Stewards to maintain the quality and integrity of PRM data.

Any Data User that has access to PRM data, is also entrusted with the protection of that data.

a) Responsibilities

- Ensure that PRM data is recorded or collected according to data standards;
- Report data errors and quality issues in a timely manner;
- Ensure data security and privacy are maintained whenever data is accessed;
- Ensure login details are kept confidential and are only used by the designated user;
- Report any breach or suspected breach of data security or privacy;
- Sign an acknowledgement of their obligations to protect data privacy;
- Obtain approval from Data Sponsor or delegated authority for public release of PRM data;
- Abide by all terms and conditions associated with approval for access to PRM data.

b) Responsible party

- NSW Health entity or General Practice healthcare professional and support staff acting in the role of *Clinician*, or *Clerk* (refer to Principle 5.1 for specific conditions of use);
- NSW consumers acting in the role of *Patient* or *Carer* (refer to Principle 5.5.1 for specific conditions of use);
- NSW Health entity or General Practice data analysts.

c) Contact when

- Business-related queries are required;
- Business decision support is required through analysis and problem solving PRM data related topics.

5.2.11 Third Parties

A Third Party is an organisation / individual requesting access to PRM data for secondary use purposes. The Third Party is responsible for preparing an access request and committing to participating in the monitoring and assurance arrangements as stipulated by the conditions of use agreement.

a) Responsibilities

- Obtain approval from Data Custodian for access to PRM data by preparing an application requesting access to PRM data and supporting the risk assessment of the request for the secondary use of PRM data;
- Sign an acknowledgement of their obligations to protect data privacy [where access to PRM data for secondary use as been approved] as part of the conditions of use agreement;
- Abide by all conditions of use associated with approval for access to PRM data;
- Ensure data security and privacy are maintained whenever PRM data is accessed and analysed;
- Report any breach or suspected breach of data security or privacy.

b) Responsible party

- Researches, etc.

c) Contact when

- Data analysis is required for clinical research.

5.2.12 System Administrator

The System Administrator is responsible for the analysis, design, and implementation of new and changes on existing data and information structures and applications, and for administration and backup. They plan, co-ordinate, and implements security measures and manages the performance and efficiency of data storage underpinning the HOPE system.

a) Responsibilities

- Ensures alignment of data and IT governance;
- Manage IT architecture, data architecture, infrastructure and security;
- Accountable for access control and derive the best possible business benefit from the use of underlying technology of the HOPE system;
- Identifying data quality issues and implementing application fixes;
- Conducting impact analysis and coordinating changes to the HOPE system to avoid adverse impacts on PRM data assets;
- Ensuring that efficient data structure design and disaster recovery/backup procedures are effectively tested and implemented;
- Ensuring the transition from test environment to production environment;
- Reviewing physical data structures in consultation with the Data / Information Architect and Database Developers;
- Ensuring security administration through monitoring and administering DBMS security constraints, such as removing users, administering quotas, auditing, and checking for security problems;
- Analysing data stored in the database and making recommendations relating to performance and efficiency of that data storage.

b) Responsible party

- eHealth NSW application support services.

c) Contact when

- Physical data models are ready for implementation;

- A need for a new business function(s) or new application functions(s) is identified;
- Expertise is required to resolve issues related to data management anomalies occurring in the operation, physical data security, disaster recovery or back-up, system migration or platform standards, performance degradation.

5.3 Data governance model for value added copies of PRM data

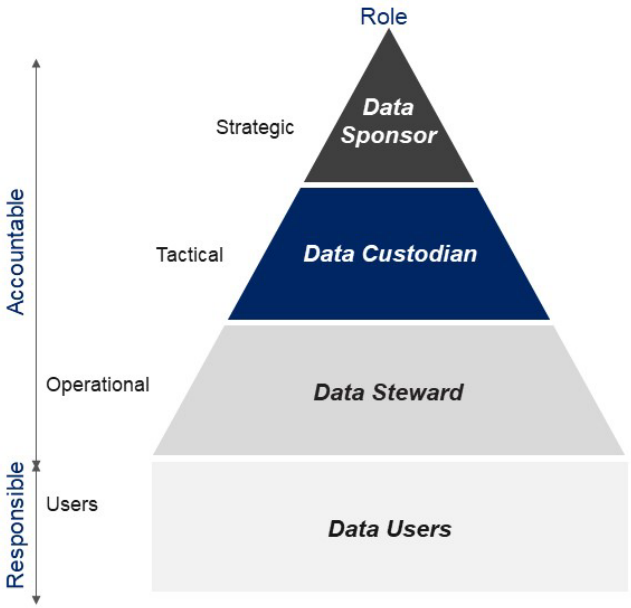
Guiding principles

5.3	Data governance model for value added copies of PRM data
5.3.1	**Accountability roles** Value added copies of the PRM data are considered separate data assets subject to their own data governance and management framework.

5.3.1 Accountability roles

Value added copies of the PRM data held within the HOPE system are considered separate data assets subject to their own data governance and management framework. Figure 6 models the data governance roles and responsibilities for value added copies of PRM data.

Figure 6: PRM data governance operating model of roles and responsibilities for value added copies of PRM data



Responsible party	Key responsibilities
Deputy Secretary, Strategy and Resources, Ministry	Controls the strategic direction of PRMs and has full accountability on behalf of the NSW health system. Responsible for overseeing the continuous improvement of PRM data governance and management.
Executive Director, System Information & Analytics, Ministry	Day to day oversight of value-added copy of PRM data asset; approval of access to the PRM data asset, and the overall quality and security of the asset.
EDWARD Administrators, System Information & Analytics, Ministry CQRs Administrators	Day to day management and operation of the PRM data asset, its completeness and quality.
System Managers, Primary Health Networks (PHNs), Researchers, Health Professionals	Any User that has access to the value-added copy of PRM data have a responsibility to maintain and protect the privacy, quality and efficacy of the PRM data.

The data governance roles and key responsibilities aligns with the *NSW Health Data Governance Framework* to ensure decision making through the clear articulation of data for communicating data-related issues and decisions.

a) Responsible parties

The Framework recognises that the Executive Director, System Information and Performance has data delegations as the Data Custodian for value added copies of PRM data and is responsible for day to day oversight and approval of access to PRM data. The accountabilities for value added copies PRM data identifies the individual responsibilities of:

- EDWARD Administrators (System Information and Analytics, Ministry) providing a Data Steward role for value added copy of PRM data held within EDWARD, ensuring data to day management of the PRM data asset.
- CQRs Administrators providing a Data Steward role for value added copy of PRM data held within a CQR, ensuring data to day management of the PRM data asset.
- System Managers, Primary Health Networks (PHNs), researchers, and health professionals, as users of value added copies of PRM data, have a responsibility to maintain and protect the privacy, quality and efficacy of the PRM data.

5.4 Patient control of PRM data in the HOPE system

Guiding principles

5.4	Patient control of PRM data in the HOPE system
5.4.1	**Conditions of consent** Patients providing consent to participate in the PRM program will need to agree to the conditions of consent, stating the intended primary and secondary use of their data.
5.4.2	**Withdrawal of consent** Patients can withdraw their consent to participate in the PRM program and their data being used for the primary purpose it was collected. Patients' PRM data may continue to be used for secondary purposes where data analysis projects request access to data collected during a period of time when consent had been provided.

5.4.1 Conditions of consent

Individual patients are invited to participate in the PRM program. Participation in the program is subject to agreeing to the conditions of consent, which states the intended primary and secondary use of their PRM data.

5.4.2 Withdrawal of consent

Patients who have PRMs will be able to withdraw from the PRM program and the use of their PRM data for primary and secondary purposes. Where a patient has recorded PRMs (questionnaire responses) but has subsequently withdrawn, the PRM data with the HOPE system will no longer be available for primary or secondary use purposes.

a) Impact on access to PRM data

The result of patients removing consent to participate in the PRM program and their PRM data being used for the primary purpose it was collected includes:

- Clinicians and health services that scheduled the patient's questionnaires no longer be able to access the questionnaire responses to provide ongoing treatment and care. They will still have access to the PRM data to respond to access notices / court orders;
- Patient's PRM data will no longer be able to be accessed within value added copies for secondary use purposes;
- Patient's PRM data may continue to be used for secondary purposes where data analysis projects requested access to the patient's PRM data that was collected during a period of time when consent had been provided.

5.5 Collection and use of PRM data for a primary purpose

Guiding principles

5.5	Collection and use PRM data for its primary purpose
5.5.1	**Conditions of use** NSW Health entities and General Practices will need to enter into a NSW Health [conditions of use] agreement, stating the intended primary and secondary use of PRM data collected, and their roles and responsibilities in the collection, use, sharing, security and maintenance of PRM data.

5.5.1 Conditions of use

NSW Health entities and General Practices are required to enter into a Conditions of Use Agreement (CUA) which will identity the person who will be the Data Custodian and accountable for the PRM data held within the HOPE system. The Data Custodian may (and it is anticipated that NSW Health entities will) delegate specific data and information governance roles and responsibilities to individual positions within their organisation related to the provision of PRMs using the HOPE system. This includes assigning employees, healthcare professions and healthcare support staff in the roles of System Administrator, Centralised Data Steward, Local Data Stewards, and Data Users.

a) Protection of individual's privacy

The Centralised and Local Data Stewards will ensure that individual's privacy is protected in the processes of approving the primary use of PRM data to Data Users, based on the appropriateness of the user's role and the intended use.

b) User roles of the HOPE system

The roles and responsibilities of HOPE system user roles are listed in Table 3 below. It is the responsibility of the Centralised and Local Data Stewards to assign Data Users to a user role in the HOPE system that provides the right level of access to PRM data and responsibilities over the management of that data.

Table 3: Data governance roles and responsibilities related to the HOPE system

User role name	Has a role in	Data governance equivalent role	Roles / responsibilities
System Administrator	All operational procedures related to IT governance and management of IT architecture, data architecture, infrastructure and security	System Administrator	(i) Upon receipt of approval from the Data Sponsor, establishes the ACI Administrators (ii) Provides ongoing technical support of the HOPE system
ACI Administrator	All PRM data-related work to ensure that it is performed according to policies and practices as established by the Framework.	Centralised Data Specialist	(i) Assigns, maintains and re-assigns Local Administrator identity, roles and permissions (ii) Control the authoring and approval of PRM survey templates into the HOPE system (iii) Ensures that all HOPE system users are appropriately trained and are aware of their obligations in the protection of PRM data (iv) Establishes a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the PRM data held in the HOPE system (v) Provides feedback to Local Data Stewards in relation to data quality issues
Local Administrator	All day to day operations and PRM data management within their healthcare provider organisation	Local Data Stewards Data User	(i) Assigns, maintains and re-assigns health service roles and permissions (ii) Ensures that all HOPE system users are appropriately trained and are aware of their obligations in the protection of PRM data (iii) Is expected to have high level knowledge and expertise in the PRM data content of the HOPE system (iv) Provides advice to Data Custodian and Central Data Steward on the management of the PRM data held in the HOPE system

User role name	Has a role in	Data governance equivalent role	Roles / responsibilities
			(v) Provides feedback to HOPE system users in relation to data quality issues
Internal Clinician	All PRM data (questionnaire responses) related to their NSW Health entity	Data User	(i) Abide by all terms and conditions associated with the conditions of use agreement for access to PRM data (vi) Must have completed HOPE system training, including training in privacy and information security (vii) Report any breach or suspected breach of PRM data security or privacy
External Clinician	All PRM data (questionnaire responses) related to their General Practice	Data User	(i) Abide by all terms and conditions associated with the conditions of use agreement for access to PRM data (ii) Must have completed HOPE system training, including training in privacy and information security (iii) Report any breach or suspected breach of PRM data security or privacy
Internal Clerk	All PRM data (questionnaire responses) related to their NSW Health entity	Data User	(i) Abide by all terms and conditions associated with the conditions of use agreement for access to PRM data (ii) Must have completed HOPE system training, including training in privacy and information security (iii) Report any breach or suspected breach of PRM data security or privacy
External Clerk	All PRM data (questionnaire responses) related to their General Practice	Data User	(i) Abide by all terms and conditions associated with the conditions of use agreement for access to PRM data

User role name	Has a role in	Data governance equivalent role	Roles / responsibilities
			(ii) Must have completed HOPE system training, including training in privacy and information security (iii) Report any breach or suspected breach of PRM data security or privacy
Patient	PRM data (questionnaire responses) they input	Data User	(i) Agree to all terms and conditions associated with the consent to collect PRM data (ii) Report any breach or suspected breach of PRM data security or privacy
Carer	PRM data (questionnaire responses) related to the patient(s) they are recognised as their carer	Data User	(i) Agree to all terms and conditions associated with the consent to collect PRM data (ii) Report any breach or suspected breach of PRM data security or privacy

5.6 Use and disclosure of PRM data for a secondary purpose

Guiding principles

5.6	Use and disclosure of PRM data for a secondary purpose
5.6.1	**Secondary use of PRM data** For applications requesting access to local PRM data (i.e. PRM data owned by one NSW Health entity or General Practice), the application should be directed to the Data Custodian for the requested PRM data held within the HOPE system. The Data Custodian will perform a data risk assessment and assurance process to assess the request for the secondary use of PRM data, approve / deny the request, and specify [in an agreement] what PRM data is available and the conditions of use.
5.6.2	**Secondary use of value added copies of PRM data** For applications requesting access to area-wide PRM data (i.e. PRM data owned by more than one NSW Health entity or General Practice), the application should be directed to the Data Custodian for the PRM data held within EDWARD. The Data Custodian will perform a data risk assessment and assurance process to assess the request for the secondary use of PRM data, approve / deny the request, and specify [in an agreement] what PRM data is available and the conditions of use.

Secondary use of PRM data

A number of processes are needed to consider, determine, monitor and report on a request to use PRM data held within the HOPE system for secondary purposes. Data Custodians assessing applications requesting access to PRM data are responsible for:

1. assessing the request based on the intended use of the data;
2. perform a data risk assessment and assurance process to assess applications to access PRM data for secondary use;
3. ensuring that PRM data has that been made accessible for secondary use must not leave NSW (i.e. is to be stored in a facility within NSW, however there is scope for data analyses, data algorithms and reports to be share more broadly);
4. ensuring that PRM data that is accessed or released for secondary use has the appropriate security controls in place commensurate with the conditions of use identified from the data risk assessment and assurance process; and
5. putting a set of processes in place to provide assurance to stakeholders and clients that the use of PRM data is only for the approved primary and secondary purposes.

Any decisions made on the secondary use and disclosure of PRM data must be in accordance with the Privacy Manual for Health Information, Health Records and Information Privacy Act 2002 and its Statutory Guidelines, the NSW Combined Delegations Manual, and Policy Directive PD2018_001, Disclosure of unit record data by Local Health Districts for research or contractor services. The Appendix provides guidance of the processes, and the roles and responsibilities of the parties involved in requesting and access PRM data for secondary use.

5.6.1 Secondary use of value added copies of PRM data

For applications requesting access to area-wide PRM data (i.e. PRM data owned by more than one NSW Health entity or General Practice), the application should be directed to the Data Custodian for the PRM data held within EDWARD.

5.7 Protecting the privacy of individuals

Guiding principles

5.7	Protecting the privacy of individuals
5.7.1	**Data safety** The Data Custodians of PRM data assets will regularly reconsider the privacy protection processes around primary and secondary use of PRM data, to maintain an acceptable level of protection to ensure privacy, security and confidentiality of PRM data.

5.7.1 Data Safety

NSW Health entities and General Practices are required to meet the Australian Privacy Principles (APPs) in Schedule 1 of the *Privacy Act 1988* with respect to the collection, storage, security, access, use and disclosure of personal information. The Data Custodians of PRM data assets will regularly reconsider the privacy protection processes around primary and secondary use of PRM data, to maintain an acceptable level of protection to ensure privacy, security and confidentiality of PRM data. Proven methods should be used to reduce the risk of breaching an individual's privacy to very low levels.

a) Data storage

PRM data that is disclosed must be stored by the recipient Third Party or other systems in a secure fashion at all times. Acceptable secure storage includes storage on physically secure file servers that are configured in such a way that password protection is universally enforced, or in files that are encrypted by "strong" encryption software. Storage on portable media, laptops and desktop computer hard drives is not acceptable.

5.8 Fit for purpose

Guiding principles

5.8	Fit for purpose
5.8.1	**Data quality** The Centralised Data Steward will establish a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the PRM data, for primary and secondary use.

5.8.1 Data quality

Data quality has a direct impact on the Data User. Incomplete or inaccurate data may result in adverse or invalid decisions or findings that have an unexpected or even detrimental impact.

PRM data must be fit for the primary and secondary uses it is intended. Data custodians are responsible for ensuring each PRM data asset has defined data quality standards. Data quality strategies must address the accuracy, completeness, timeliness, relevance, consistency and reliability of data.

Data quality may be facilitated by:

- publication of metadata including a data dictionary, business rules and guide for use;
- regular communication with stakeholders regarding changes to the PRM data asset;
- regular assessment of data quality against each of the intended uses and communication of results to Data Users;
- timely advice to Data Stewards and Data Users in relation to data quality and rectification actions required.

a) Quality assurance

The Centralised Data Steward will put a set of processes in place to provide feedback to Local Data Stewards about data quality including issues requiring rectification.

The Local Data Stewards will ensure that PRM data collected is of sufficient quality to support the intended primary and secondary use of the data.

5.9 Risk mitigation strategies

Guiding principles

5.9	Risk mitigation strategies
5.9.1	**Risk of breach** The Data Custodians of PRM data assets will ensure that the risk of a breach of privacy for an individual is reduced to an acceptable level by minimising the risks associated with the collection, use, sharing (and release) of PRM data for primary and secondary purposes.

5.9.1 Risk of breach

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse;
- malicious actions, such as theft or ‘hacking';
- internal errors or failure to follow information handling policies that cause accidental loss or disclosure;
- not adhering to the laws of NSW or the Commonwealth of Australia.

The Data Custodians of PRM data assets will ensure that the risk of a breach of privacy for an individual is reduced to an acceptable level by minimising the risks associated with the collection, use, sharing (and release) of PRM data for primary and secondary purposes.

a) Data security and protection

The RPM data held within the HOPE System must have in place processes to protect the privacy and confidentiality of data through access management and security controls. It is the responsibility of the Data Custodian, in consultation with the System Administrator, to ensure that the necessary penetration testing and other security assessment is undertaken to guarantee that PRM data is appropriately secured, backed up and disposed of according to agreed and documented protocols. Alignment of data and IT governance must enforce regulatory, architectural and security compliance requirements.

b) Risk assessment and assurance process

The Data Custodian, in consultation with the System Administrator, must undertake an appropriate data risk assessment and assurance process to consider, determine, monitor and report on a request to use PRM data for secondary purposes. The requirement for the Data Custodian to undertake a data risk assessment and assurance process is to ensure that:

1. an assessment of the impact of privacy can be performed; privacy and security concerns are managed through application of this PRM Data Governance and Management Framework; and that the proposed technology security controls for the storage of PRM data have been verified using an information security assessment.
2. the monitoring and assurance process and conditions of use are defined and clearly understood by all parties.

5.10 Effective governance

Guiding principles

5.10	Effective governance
10.1	**Framework review** As part of the ongoing better practice of effectively managing and governing PRM data, the Framework will be reviewed every year or when there are material changes either to either the strategic governance of PRMs or to policies and legislation that impact on data governance.

5.10.1 Framework review

The Framework is an evolving and living document that will be reviewed, as part of the ongoing better practice of effectively managing and governing PRM data. As part of the ongoing review of the Framework the list of permitted and non-permitted uses will be considered and amended, along with the roles and responsibilities of NSW Health entities, General Practices, and Primary Health Networks.

6. Appendix

6.1 Requesting and accessing PRM data for secondary use

Table 4 and Figure 7 below describe the processes and the responsibilities of each data governance role.

Table 4: Roles and responsibilities in the process of requesting and accessing PRM data for secondary use

Role	Responsibility
Data Custodian	The Data Custodian will apply this Framework in making decisions around approving access to PRM data for secondary use.
Third Party	The Third Party is an organisation / individual requesting access to PRM data for secondary use purposes. The Applicant is responsible for preparing the application and committing to participating in the monitoring and assurance arrangements as stipulated by the Data Custodian.
Data User	Acting as the data integrator, is responsible for conducting the necessary data linkage as specified by the Data Custodian.
System Administrator	Its role includes 'to prepare and provide de-identified data for research and public health purposes'. Other authorisations provide the basis for the disclosure of identified information for secondary use with individual consent

Figure 7: Processes for requesting and accessing PRM data for secondary use

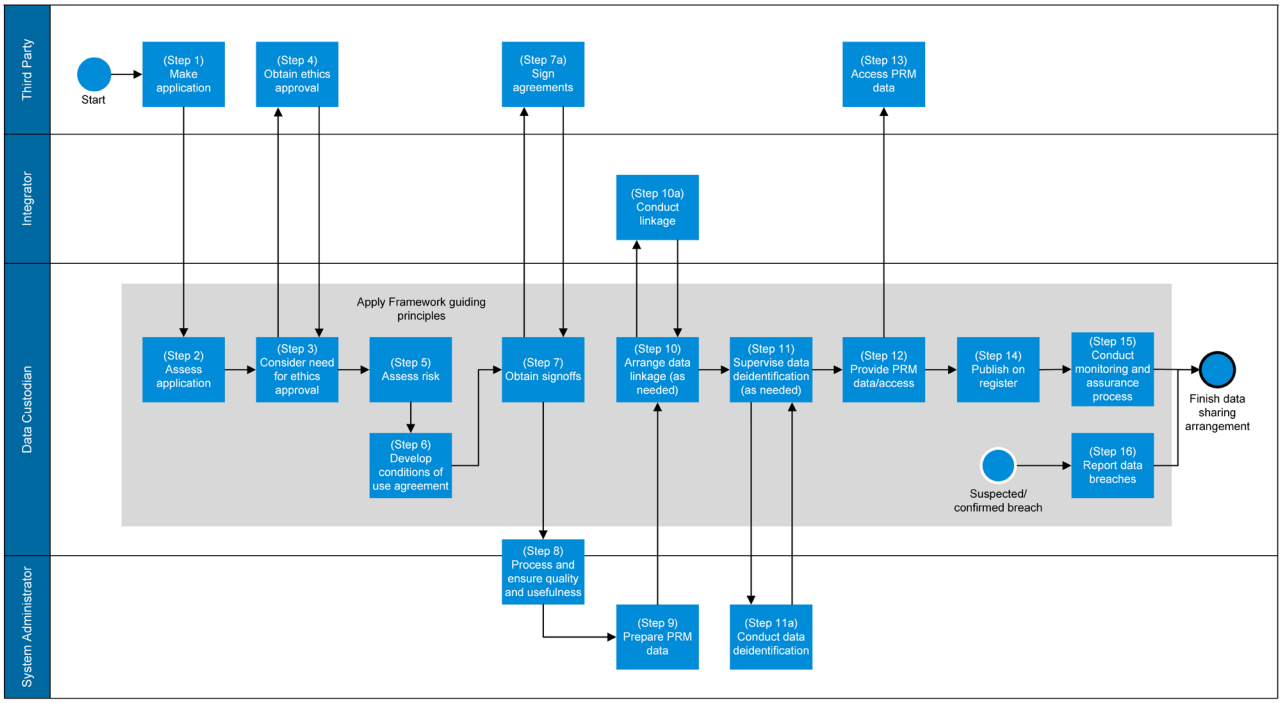


Table 5 provides further guidance of the processes, and the roles and responsibilities of the parties involved in requesting and access PRM data for secondary use.

Table 5: Processes in the use of PRM data for secondary use

Step	Description of process	Responsibility
Step 1	Make an application for secondary use of PRM data using predefined format / method. Submit a risk management plan with the application.	Third Party
Step 2	Assess application in terms of the intended use *Additional Information* On receiving a request for use or disclosure of PRM data, the Data Custodian should consider the following: (i) Whether aggregate PRM data (rather than unit-level PRM data) is sufficient to meet the needs of the Applicant (ii) Whether the activity could be undertaken using or disclosing de-identified unit level PRM data (iii) Whether the request should be refused.	Data Custodian

	Requests may be refused, but there should be reasonable grounds for this. Examples of reasonable ground may include: (a) based on the guidelines in this Framework on the appropriate and inappropriate use of PRM data (b) based on the 'Five safes' principles to assess applications	
Step 3	Identify if ethics approval is required and, if so, request the applicant to obtain it. *Additional Information* If the request is for a secondary purpose related to the management of health services or research, the request should be referred to the Human Research Ethics Committee (HREC). The *Health Records and Information Privacy Act 2002* requires proposals for funding, management, planning or evaluation of health services, and research proposals to be submitted and reviewed by a HREC. If the request is for Aboriginal health information, consideration should be given as to whether the project should be submitted to the AH&MRC Ethics Committee.	Data Custodian
Step 4	Obtain ethics approval (if requested) via institutional HREC. *Additional Information* Ethics committee approval / advice will help inform the decision to support disclosure of the information. Approval by the HREC of an application to use PRM data does not by itself constitute authority for disclosure of the data but is a prerequisite for an authorisation for disclosure to occur.	Third Party
Step 5	Conduct a risk assessment to determine monitoring and assurance processes, including consideration of the published minimum data security requirements.	Data Custodian
Step 6	Develop Conditions of Use Agreement (CUA) *Additional Information* The CUA should be based on the guidelines in this Framework and for NSW Health entities, PD2018_001: *Disclosure of Unit Record Data held by Local Health Districts for Research or Contractor Services*.	Data Custodian
Step 7	Ensure CUA has been signed by the Applicant.	Data Custodian

Step 7a	Sign CUA.	Third Party
Step 8	Process, clean and ensure quality and usefulness of data.	System Administrator and Data Custodian
Step 9	Prepare the required PRM data for release / access by Third Party	System Administrator
Step 10	Arrange data linkage as needed.	Data Custodian
Step 10a	Conduct data linkage as requested.	Data Integrator
Step 11	Assess the need to de-identify data and if required, supervise the method most appropriate to protect individual's privacy.	Data Custodian
Step 11a	De-identify the data using the method prescribed by the Data Custodian.	System Administrator
Step 12	Provide PRM data and / or access to PRM data as needed to allow approved requests to proceed.	System Administrator
Step 13	Receive / access PRM data through the approved means (including linked data as appropriate).	Third Party
Step 14	Publish applications and their outcomes on the Public Register.	Data Custodian
Step 15	Undertake monitoring and assurance processes consistent with the CUA.	Data Custodian
Step 16	Report any data breaches (as identified).	Data Custodian