Data governance framework

Fostering a responsible, safe and compliant data culture.

March 2024

phn NORTH WESTERN MELBOURNE

An Australian Government Initiative

North Western Melbourne
Primary Health Network

nwmphn.org.au

ABN 93 153 323 436

Telephone: (03) 9347 1188
Fax: (03) 9347 7433

Street address: Level 6, 737 Bourke Street
Docklands, Victoria 3008

Email enquiries: nwmphn@nwmphn.org.au

Disclaimer

While the Australian Government Department of Health and Aged Care has contributed to the funding of this material, the information contained in it does not necessarily reflect the views of the Australian Government and is not advice that is provided, or information that is endorsed, by the Australian Government. The Australian Government is not responsible in negligence or otherwise for any injury, loss or damage however arising from the use of or reliance on the information provided herein.

Acknowledgements

We acknowledge the people of the Kulin nations as the Traditional Custodians of the land on which our work in the community takes place. We pay our respects to their Elders past and present.

We also recognise, respect and affirm the central role played in our work by people with lived experience, their families and/or carers.

Shutterstock images, cover and page 5.

RECONCILIATION ACTION PLAN
INNOVATE

REGISTERED CHARITY
acnc.gov.au/charityregister

Certified System
Quality
ISO 9001
SAI GLOBAL

Contents

Introduction 4

Legal and regulatory environment 5

Guiding principles 6

Data governance structures 7

Data roles and responsibilities 8

Data management 11

Policies and procedures 14

Monitoring and compliance 15

Introduction

Melbourne Primary Care Network (MPCN) trading as North Western Melbourne Primary Health Network (NWMPHN) recognises that data is a strategic asset that has value to the entire organisation. Data is the foundation of our planning, decision making and operational functions.

NWMPHN is the custodian of a vast number of data assets. We rely on strong data governance to perform our functions effectively and maintain the trust of our data providers, data recipients and stakeholders in acquiring, handling and releasing data.

Definitions

TERM	DEFINITION
MPCN	Melbourne Primary Care Network, trading as North Western Melbourne Primary Health Network (NWMPHN)
NWMPHN	North Western Melbourne Primary Health Network operated by Melbourne Primary Care Network (MPCN)
RDG	Research and Data Governance Committee

Purpose

The purpose of the framework is to outline how NWMPHN effectively governs data. It provides information on:

- the legal and regulatory environment that mandates how the organisation handles personal and sensitive information
- its guiding principles for governing data
- its data governance structure, including roles and responsibilities
- systems and tools used to manage data throughout its lifecycle
- supporting policies, procedures and processes to ensure compliance.

The framework applies to all data and information assets listed in NWMPHN systems inventory and data asset registry. This includes data collected or processed by NWMPHN, collected on behalf of NWMPHN, or obtained from external sources.

Audience

The intended audience of this document is all NWMPHN staff and stakeholders, including commissioned service providers that provide, receive or use data from NWMPHN.

Legal and regulatory environment

NWMPHN must comply with federal and state legislation, and health industry standards, concerning how data is collected, managed, secured, shared and protected.

These key documents are relevant to this framework:

- The Australian Government Privacy Act 1988
- The Office of the Australian Information Commissioner’s Privacy Principles
- The Australian Government Department of Health and Aged Care’s Practice Incentives Program Quality Improvement Incentive guidance
- The Australian Government Department of Health and Aged Care’s framework to guide the secondary use of My Health Record system data
- The Australian Government Department of Health and Aged Care’s Primary Mental Health Minimum Data Set resources guide
- The Australian Institute of Health and Welfare’s data governance framework 2022
- The Primary Health Network national data governance policy

Guiding principles

The governance of data at NWMPHN is supported by the following principles:

Data is a strategic asset

Data is the foundation of the organisation's planning, decision-making and operational functions. Given the sensitive nature of primary health data, care must be taken to appropriately manage and govern it through its lifecycle.

Data must have clear stewardship

Data is managed in a way that is transparent to stakeholders. Clear roles and responsibilities are defined to ensure accountability.

Data security and privacy must be protected

NWMPHN is aware of the high standards that the community and the organisations stakeholders expect. Sensitive and personally identifiable data must be protected by best practice security standards. Personally identifiable information must be managed in accordance with legal, regulatory, and other relevant governance frameworks.

Data is accessible

Data is easy to locate and use when required and is stored in a manner ensuring there is a single source of truth. Data is available and accessible to authorised individuals to help deliver insights on health trends and deliver population health improvements.

Data quality and integrity improvement is essential

Data accuracy, consistency and reliability is maintained over its entire lifecycle to ensure it is dependable for the purposes of planning, decision-making and operational functions.

Indigenous data sovereignty

Indigenous data sovereignty is recognised and incorporated in data governance and management practices.

Data governance structures

NWMPHNs Research and Data Governance Committee (the RDG Committee) provides cross-organisational leadership and oversight to data governance activities. It brings together representatives from all business areas to ensure effective, efficient, and approved acquisition, use and management of data assets.

The role of the committee is to ensure organisational compliance with the NWMPHN Research and Evaluation Strategic Action Plan, data governance frameworks, and associated policies and procedures.

Specifically, the committee:

- makes approval decisions on requests for research partnerships, reviewing against set criteria to ensure alignment with NWMPHN's strategic objectives and research strategy focus areas
- provides advice and recommendations for data-related matters, such as breaches, that must be escalated
- must be informed about data privacy and security issues
- provides advice on ethical considerations of internal research-related activities, beyond established and approved procedures
- identifies and addresses emerging research and data-related organisational needs that are not otherwise covered under research and data strategic action plans, such as staff training, resources, and internal research requests.

Members of the RDG Committee are:

TERM	DEFINITION
Chair	Executive Director, Insight, Performance and Digital Services
Secretariat	Research Coordinator
Members	Chief Executive Officer Executive Director, Health Systems Integration Executive Director, Service Development and Reform Executive Director, Systems Director, Evaluation and Research Director, Technical Development Information Security and Governance Specialist

The committee periodically reports to the Finance Audit and Systems (FAS) Board sub-committee. When needed, it also provides updates to the Commissioning Quality and Performance (CQP) committee.

The RDG Chair is also a member of the National Data Governance Committee convened by the PHN Cooperative.

Data roles and responsibilities

Data governance is everyone's responsibility. All NWMPHN staff and stakeholders have parts to play. The main roles are the chief data officer, privacy officer, data sponsor, business and technical data stewards, and data users.

NWMPHN maintains a systems inventory and data asset register where the details of each assigned role are recorded. It also contains information about each data asset such as its description, information security classification, purpose, and storage location.

1. Chief data officer

The chief data officer is the executive director of the Insights Performance and Digital Services business unit. As a delegate of the chief executive officer, they exercise overall responsibility for NWMPHN data collections, in accordance with the policies, guidelines and any specific conditions that must be applied. They also represent NWMPHN data governance matters within Victoria and nationally.

The chief data officer is responsible for:

- managing risks related to data governance within NWMPHN
- the enforcement of data security policies and management of security breach incidents
- prioritising and building on data assets
- establishing and maintaining engagement with external and internal business data stewards
- maintaining data and information management audit processes to ensure NWMPHN's compliance with all legislative, regulatory and policy requirements
- reviewing and authorising completion of privacy impact assessments
- authorising external data and information-sharing requests and agreements.

2. Privacy officer

The privacy officer is the executive director of the Systems business unit, and the first point of contact for advice to staff relating to privacy matters. They are also responsible for dealing with breaches under national and Victorian legislation, policies, and guidelines and have responsibility for procedures for managing unsolicited identifiable data received by NWMPHN.

3. Data sponsor

Data sponsors are likely to be directors or executive directors and they are responsible for:

- advocating for the strategic management, governance and operations of data assets
- establishing the rationale for NWMPHN holding data assets in the data sponsor's work domain
- providing direction and guidance and authorising appropriate resources for management of data assets
- ensuring adherence with all relevant legislation, policies, standards and procedures
- appointing business data stewards and ensuring their duties are fulfilled
- ensuring users with access to the NWMPHN data assets have necessary approvals and reviews the ongoing need and appropriateness of access for individual NWMPHN personnel.

4. Business data steward

A business data steward is a person designated by the data sponsor for each of the data assets. They are appointed to be responsible for data held within that asset which may be a single system, or part of a larger system, application or database.

Business data stewards are responsible for:

- the day-to-day management of data and information from a business perspective
- maintaining the integrity and accuracy of data within their work domain and implementing processes for rectification of integrity and accuracy issues
- ensuring users with access to data within their work domain have necessary approvals
- reviewing the ongoing need and appropriateness of access for individual NWMPHN personnel
- providing evidence, in combination with the data sponsor, that data is being managed according to compliance requirements
- classifying the information held with the data asset.

Business data stewards are likely to be managers or directors. Ideally there will be one assigned steward for each data set. However, in some instances stewardship may be shared, for instance, when a data set is used for very different functions. For example, the primary care data set may be used for quality improvement, but also be accessed for a needs assessment or other approved research.

5. Technical data steward

Technical data stewards are members of the Insights, Performance and Digital Services business unit and they are responsible for:

- working with the chief data officer, data sponsor and business data steward to ensure users with access to the data within NWMPHN have necessary approvals and reviews the ongoing need and appropriateness of access for individual NWMPHN personnel
- maintaining integrity and accuracy of data and implementing required processes for rectification of integrity and accuracy issues
- working with business data stewards and stakeholders to develop and maintain metadata, including a data dictionary, business rules and user guide
- escalating material risks and issues to the chief data officer
- reviewing the business data steward's reports before release to ensure they are compliant with policies, legislation, and guidance documents.

The technical data steward may be delegated some or all responsibilities of the chief data officer, where necessary.

6. Data user

A data user is any person who is authorised to use a data asset. They are responsible for:

- ensuring that their access is carried out in a way which does not jeopardise data security and privacy
- not allowing their usernames or passwords to be used by any other person
- not accessing data on behalf of any other person
- understanding their obligations with regard to consent, data sharing, data management.

Data management

Data management includes the administrative processes through the lifecycle of data. A plan documenting these processes must be developed for each data asset.

1. Data acquisition

NWMPHN collects data to better understand and improve the health system. Data is only collected and held if it is necessary for, or directly related to, one or more of its functions or activities. Data should be stored alongside metadata and data dictionaries to accurately define and describe it.

All new or significantly changed data assets are recorded in NWMPHNs systems inventory and data asset register. This identifies the data sponsor and stewards for each asset, its storage location, and whether it contains identifiable material. Privacy impact assessments are completed for each asset to assess risks and appropriate controls.

2. Data storage and security

NWMPHN stores data onsite and in secure cloud-based storage solutions.

The organisation's information security management system, ICT policy and IT disaster recovery plan provide detailed descriptions of:

- security requirements for internally and externally hosted systems
- hosting requirements for cloud-based solution data centres
- data centre back-up and restoration requirements
- access level controls to services and proper use of IT systems.

NWMPHN's cloud services policy stipulates the requirements of cloud-hosted services and describes the shared services model.

Security is an important component of maintaining data integrity, whereby the appropriate security measures protect data from unauthorised access, alteration or corruption. NWMPHN ensures data security by:

- authorising access to data according to permissions determined by the data sponsor
- regularly updating security protection on all devices
- providing online safety awareness training to staff.

All data handled by NWMPHN systems are subject to this framework, and internal policies such as the information security policy, cyber security framework, and data and record retention procedure. This is to ensure that clear and robust documentation supports the data governance principles that eventually lead to protecting the attributes of confidentiality, integrity and availability.

3. Data quality

Data quality management encompasses activities and processes to optimise and enhance the quality of data held by NWMPHN.

Users should have access to data that is accurate, complete, consistent and up to date. Information about the quality of a data asset should be accessible to users to ensure appropriate caveats are considered.

Data quality activities include verifying business processes, identifying and resolving quality issues and continuous monitoring and improvement.

The data stewards are responsible for documenting quality metrics. These must include measures of accuracy, completeness, consistency, timeliness, availability and fitness for use.

4. Data access, use and analysis

The data sponsor is responsible for approving internal access and use of datasets. In considering approval, they must seek to balance ease of access with minimising risks. The latter include accidental loss or damage, unauthorised access, malicious misuse, and inadvertent alteration or disclosure.

The core principles of data access and use include:

- Ethics: the data sponsor must meet ethical obligations to consider risks and burdens to individuals to whom the data relates, informed consent, privacy and whether review is required.
- Need to know: the data sponsor must grant users the minimum requirements to undertake their business role or for approved purposes.
- Specific and authorised: the data must not be used by people other than those authorised to do so.
- Approved disclosure: authorised people must not disclose data to anyone without approval from the data sponsor.
- Specified use: the data must only be used for the purpose specified.
- Secure and controlled use: the data must always be protected by the appropriate security and controls.
- Duration of access: the data must not be kept for longer than approved.

5. Data sharing and release

Sharing and release of data to third parties must comply with state and federal privacy legislation. An appropriate assessment must be undertaken to determine the purpose of releasing data and any privacy and security risks must be considered. This includes ensuring that consent provided when the data was collected supports the purpose of the data being shared.

6. Data retention and disposal

NWMPHN is an ISO-9001 accredited organisation. As such it is required to ensure documented information is available and suitable where and when it is needed. It must also be adequately protected from loss of confidentiality, improper use, or loss of integrity. NWMPHN extends these standards to all records and data.

The data and record retention and disposal policy supports the proper and efficient data record management practices at NWMPHN.

Policies and proceedures

NWMPHNs internal data-related policies, guidelines and procedures are designed to ensure compliance with the legal and regulatory environment in which we operate. They provide staff, especially those with delegated authority such as data sponsors and stewards, with clear sources of information to perform their roles effectively and appropriately.

It is the responsibility of all staff to observe and comply with this framework and associated NWMPHN policies and procedures. These include:

- **Data governance:** data roles and responsibilities manual, systems inventory and data asset register, external data report sharing guidelines, data and record retention and disposal policies, data retention and disposal procedures.
- **Data privacy:** privacy policy, privacy and confidentiality procedure.
- **Information and cyber security:** ICT policy, cyber security management policy.
- **Data breach:** data breach response plan.

Induction procedures for NWMPHN staff include an overview of their information and data security responsibilities.

Please be aware that these policies and procedures may be updated from time to time.

The data and record retention and disposal policy supports the proper and efficient data record management practices at NWMPHN.

Internal resources

NWMPHN staff can access the following resources on Prompt.

- Information security policy
- Terms of reference research and data governance committee
- Head to Health data governance framework
- Risk management framework
- Data and records disposal procedure
- Data and record retention procedure

Monitoring and compliance

Through a proactive and responsive approach, NWMPHN regularly monitors compliance with its data management and security requirements.

- Data stewards continuously monitor assets and undertake reviews and analyses of identified problems. Actions and outcomes are documented as part of the Research and Data Governance Committee's risk, issues, and decisions register.
- The RDG Committee undertakes regular reviews and audits of related policies, the systems inventory and data asset register, privacy impact assessments and data sharing agreements.
- Regular reporting against the RDG Committee's workplan and the organisation's compliance with data governance arrangements will be provided to the MPCN Board.

Data breaches

In the event of a data breach, NWMPHN has a procedure to ensure it can act swiftly to mitigate risk and prevent recurrence. This includes the notification of the breach if it is likely to result in serious harm to an individual, as required under the Office of the Australian Information Commissioner's notifiable data breaches scheme.

phn
NORTH WESTERN
MELBOURNE

An Australian Government Initiative

nwmphn.org.au