Data Governance Framework

phn
MURRUMBIDGEE
An Australian Government Initiative

TABLE OF CONTENTS

DATA GOVERNANCE FRAMEWORK

DATA VISION STATEMENT:

MPHN COLLECTS, MAINTAINS AND ANALYSES POPULATION HEALTH DATA AND DATA FROM ITS COMMISSIONED SERVICES AND PROGRAMS TO INFORM ASSESSMENT OF HEALTH NEEDS AND TO PLAN FOR PRIMARY HEALTH SERVICES TO ENSURE “WELL PEOPLE, RESILIENT COMMUNITIES ACROSS THE MURRUMBIDGEE”.

The MPHN data governance framework is a set of principles that apply to all data collected and used throughout the organisation, broadly it articulates the roles and responsibilities of staff including the data custodian who is involved in the collection, use, access, analysis, privacy and security of all data sets.

Within MPHN, data is valued and managed as a strategic asset to support commissioning of health services. The underlying principles applied to data management in MPHN include:

1. **Privacy – Protection of the privacy of individuals is maximised.**
2. **Security – Confidentiality, integrity, and availability is maintained.**
3. **Trustworthy – Data is accurate, valid, reliable, timely, and relevant.**
4. **Accessible – Data is accessible.**
5. **Data management - definition, collection, manipulation, analysis, and dissemination.**

Murrumbidgee PHN is committed to ensure high levels of data security and governance across all of its functions.

The approach outlined in this framework is underpinned by the Privacy Act (Privacy Act 1988; Act No. 119 of 1988 as amended). Data governance is supported by MPHN’s information technology and system security functions.

Leadership and accountability regarding data management is defined, communicated and compliance is monitored, measured and reported through governance.

PRINCIPLE 1: PRIVACY

PROTECTION OF THE PRIVACY OF INDIVIDUALS IS MAXIMISED

CONTEXT

Collection, use and access of all MPHN data sets must comply with all relevant overarching legal requirements to ensure the privacy of individual people.

RATIONALE

Australians expect strong safeguards to ensure their health information is safe and secure, that the privacy of their health information is respected, and their rights protected. All healthcare providers in Australia have professional and legal obligations to protect their patients' health information.

DETAILS

Personal information is protected by law. All current privacy notices and privacy policies in MPHN are consistent with the Privacy Act 1988 (Act No. 119 of 1988 as amended), and relevant state or territory legislation. MPHN have a Privacy Policy available to all staff on the intranet.

CLASSIFICATION AND IMPACT ON PRIVACY

To ensure that data is de-identified, MPHN will undertake Privacy Impact Assessments on its data assets. In addition MPHN will classify its data using a robust system detailed below. Privacy Impact Assessments will be undertaken by the MPHN Data Custodian and the relevant Data Steward.

PRIVACY TRAINING

MPHN will ensure that all staff undertake privacy training on commencement and regularly throughout their employment.

RESOURCES

Privacy Act 1988 and Australian Privacy Principles for APP entities: specifically APP 10, 11, 12 and 13

State and Territory privacy laws

Guidelines approved under Section 95A of the Privacy Act 1988 – National Health and Medical Research Council, 2014

Health Records and Information Privacy Act 2002 No 71

The Office of the Australian Information Commissioner (OAIC) and Commonwealth Scientific and Industrial Research Organisation (CSIRO Data61 released in 2017 the De-identification Decision-Making Framework (DDF)

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES

AUSTRALIAN PRIVACY PRINCIPLES - A SUMMARY FOR APP ENTITIES (12 MARCH 2014)

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy.

APP 2 – Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 –Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

PRIVACY IMPACT ASSESSMENT

MPHN will undertake Privacy Impact Assessment (PIA) using the following guidelines:

- Threshold assessment
- Plan the PIA
- Describe the project
- Identify and consult with stakeholders
- Map information flows
- Privacy impact analysis and compliance check
- Privacy management – addressing risks
- Recommendations
- Report
- Respond and review

The PIA will ensure that a De-Identification Decision-Making Framework is used as detailed below.

The De-Identification Decision-Making Framework is based on five key principles:

1. It is impossible to decide whether data is safe to share/release by looking at the data alone.
2. But it is still essential to look at the data.
3. De-identification produces safe data, but it only makes sense if safe useful data is produced.
4. Zero risk is not a realistic possibility in producing useful data.
5. The measures put in place to manage risk should be proportional to the risk and its likely impact.

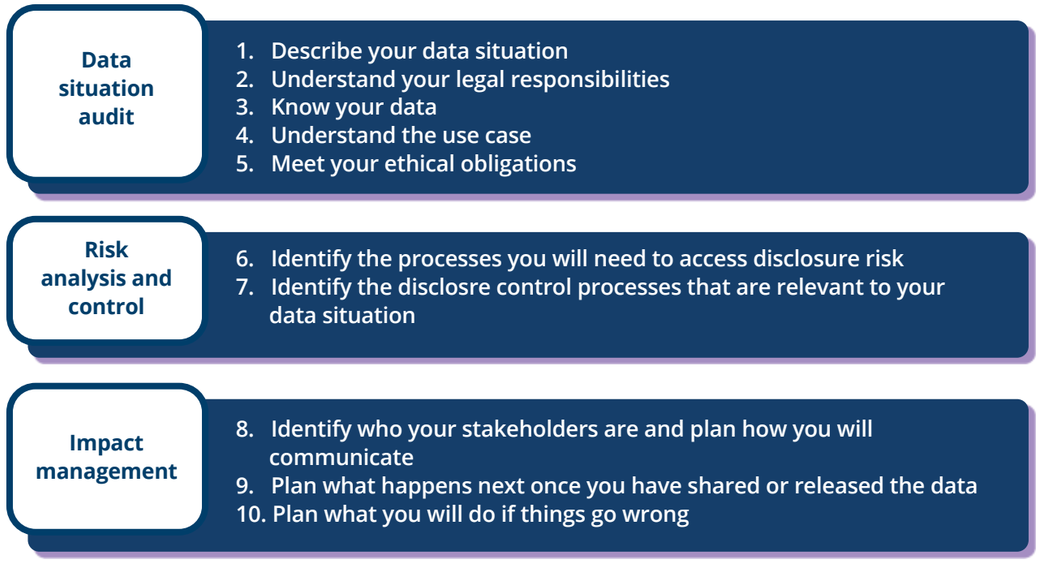


Figure 1 Privacy Management Framework's use of De-identification Decision-Making Framework

DATA CLASSIFICATION

MPHN will classify its data by assigning one of the following classifications. Collections of diverse information will be classified as to the most secure classification level of an individual information component with the aggregated information.

Most information does not need increased security and may be marked 'Public' or left unmarked. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality of the information.

People are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank, or level of authorised access.

Sensitive and Highly Sensitive classified information have special handling requirements, especially during electronic transmission or physical transfer. It is only to be used and stored in physical environments that provide a fitting level of protective security. All documents of this nature will be marked "sensitive" or "confidential".

Data Classification	Description	Example Data Types
Highly Sensitive	Data that if breached owing to accidental or malicious activity would have a **high** impact on MPHN activities and objectives.	Data subject to regulatory control, prohibiting reporting or sharing Medical Children and young persons Credit card
Sensitive	Data that if breached owing to accidental or malicious activity would have a **medium** impact on MPHN activities and objectives.	Organisational financial data Research data (containing personal data)
Private	Data that if breached owing to accidental or malicious activity would have a **low** impact on MPHN activities and objectives	Business unit process and procedures Unpublished intellectual property ITC system design and configuration information
Public (unclassified)	Data that if breached owing to accidental or malicious activity would have an **insignificant** impact on MPHN activities and objectives	Public directory information Published data

PRINCIPLE 2: SECURITY

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY IS MAINTAINED

CONTEXT

Collection, transfer, access and storage of all MPHN data is undertaken in a secure manner to maintain the three pillars of security: confidentiality, integrity, and availability.

RATIONALE

Strong security and risk management frameworks that protect sensitive information while also enabling the safe and efficient sharing of information are vital.

DETAILS

Storage of all MPHN data sets meets the requirements for health data. The data custodian monitors changes in technology and data science to anticipate new confidentiality and integrity threats. They use this knowledge to inform their security and risk approach. Data management is underpinned by the fit for purpose information and technology security systems in place at MPHN.

CONFIDENTIALITY IS MAINTAINED WITH APPROPRIATE CONTROLS

- Data custodian implements role based access controls based on specified business needs
- Data custodian identify, mitigate and accept risks
- Data custodian encrypt sensitive data at rest and in transit
- Dissemination of data by PHN reporting or provision to an external organisation will only involve the use of de-identified and aggregated data
- No raw or identifiable data will be disseminated by MPHN

INTEGRITY IS MAINTAINED DURING DATA EXTRACTION, TRANSFER AND STORAGE

- Data custodian controls access to the data at all times and is responsible for approval, data extraction, data transfer and storage
- Data custodian maintains logs of all access, change, and transit of data
- Should highly sensitive data need to be transmitted it will be encrypted or distributed through another suitable secure method
- Data that is classified as Sensitive or private will be by transmitted with appropriate security controls such as password protection.

AVAILABILITY IS MAINTAINED THROUGH APPROPRIATE GOVERNANCE AND CONTINGENCY PLANNING

- All data will be stored in the organisations data warehouse or designated data server
- Data custodian will maintain version control of all data stored in the data warehouse
- Data warehouse has appropriate back-ups and disaster recovery plans
- It is against the organisations policy to store data in emails, personal drives or removable devices.
- MPHN has a data governance committee, framework and policy for all aspects of data management

CYBER RESILIENCE

MPHN will implement two processes for cyber security; vulnerability management and penetration testing

Vulnerability management includes:

- conducting vulnerability assessments and penetration tests for systems throughout their life cycle to identify security vulnerabilities,
- analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls,
- sing a risk-based approach to prioritise the implementation of identified mitigations.

Governance of cybersecurity is achieved through reports provided to the Finance Audit and Cybersecurity Committee on a quarterly basis regarding organisational management and risks relating to cyber resilience and data breaches.

DATA BREACH

MPHN have a notifiable Data Breach policy and procedure that complies with the Privacy Amendment (Notifiable Data Breaches) Act 2017. All data breaches are reportable to the MPHN Executive and Finance Audit and Cybersecurity Committee. All data breaches will be investigated in line with the policy. The Policy is available to all staff and has been presented to staff during regular staff meetings.

IDENTITY MANAGEMENT FOR INFORMATION SYSTEMS

MPHN employ a two factor authentication process for access to the data warehouse.

RESOURCES

Information Security Guide for small healthcare businesses – ADHA

Guide to securing personal information – Office Australian Information Commissioner

Essential Eight Explained – Australian Cyber Security Centre

Stay Smart Online Small business guide – Australian Cyber Security Centre

Computer Information Security Standards – 2nd edition RACGP

PRINCIPLE 3: TRUSTWORTHY

DATA IS ACCURATE, VALID, RELIABLE, TIMELY, AND RELEVANT

CONTEXT

Trustworthiness of the data, both internal and external will be of the highest standard to ensure that interpretation is based on accuracy, validity, reliability, timeliness and relevance.

RATIONALE

Decision making for implementation or continuation of primary health care services should be based on collection and interpretation of the most trustworthy data and information.

DETAILS

ACCURATE

MPHN will endeavour to use data collected from gold standard sources or sources with sufficient information to verify the integrity of the data. This includes timeframes of data collected, sample sizes and other pertinent details. From time to time MPHN will receive data that does not comply with this level of integrity, data may or may not be utilised. If data is used it will be accompanied by a caveat that states that data should be interpreted with caution.

VALID

It is important to ensure that MPHN data has logical integrity, this includes data cleansing to ensure that data meet requirements for logical integrity and is not negatively impacted by the design of the data collection employed or in human error in recording of information.

RELIABLE

The process of data cleansing, integration and data version control will be overseen by the Senior Data Analyst. The process will be conducted using best practice principles. This process will be an ongoing process through the life of the stored data.

TIMELY

Data sets will be sourced from gold standard sources using the most up to date releases. Data updates will be monitored by the Senior Data Analyst and will be updated locally annually.

RELEVANT

Data will be considered relevant when it meets the criteria for improving the health of the community in the primary health setting and informing the delivery of health care services.

PRINCIPLE 4: ACCESSIBLE

DATA IS ACCESSIBLE

CONTEXT

Data provides the basis for evidence and as such should be accessible where possible for staff to use.

RATIONALE

Defining access is important to ensure that the previous principles are not compromised whilst maintaining an open and transparent use of data. external organisations. Where a data request is approved de-identified aggregated data will be provided.

DETAILS

INTERNAL STAFF ACCESS

Internal staff will be given access to data relevant to their work activities through data visualisation reports in SharePoint utilising Power BI as the interface. Internal staff will also be given access to Organisational reports which may include data through access to the intranet publications.

SERVICE PROVIDER ACCESS

Service providers will be given a monthly or quarterly report in PDF format from the data they provide. This report will be generated from the SharePoint Power BI data analysed by MPHN data management team. Data requests from providers will be considered on merit and should be submitted using the external data request form. Raw data will not be provided to service providers.

PUBLIC ACCESS

Public access through MPHN internet will include access to reports and data summaries. Where a data request is made to MPHN through the public, each application must be in writing and accompanied by a completed 'External Data Request Form' that will be assessed on its merit prior to the release of any data. Raw data will not be provided to the public. Where a data request is approved de-identified aggregated data will be provided.

EXTERNAL ORGANISATIONS ACCESS

External organisations will have the same access to public documents above. Where a data request is made to MPHN through an external organisation, each application must be in writing and accompanied by a completed 'External Data Request Form' that will be assessed on its merit prior to the release of any data. Raw data will not be provided to external organisations. Where a data request is approved de-identified aggregated data will be provided.

DATA REGISTRY OF DATA SETS

MPHN maintains a Data Registry of data sets that are being shared/released.

DATA ETHICS

Data ethics includes the value judgements and approaches made when generating, analysing and disseminating data. The following principles are applied to ethical integrity review

- Legally right doesn't mean ethically right
- Needs to be clear user need and public benefit
- Needs to comply with relevant legislation and codes of practice
- Needs to use data that is proportionate to the user need
- Needs to have an understanding of the limitations of the data
- Needs to be transparent and be accountable
- Needs to ensure that data use occurs responsibly

FORMALISED DATA SHARING AGREEMENT (DSA)

All data sharing agreements entered into with external organisations must specify what data is contained, what the recipient is allowed to do with that data, how the recipient will maintain the security and privacy of that data, and how the data will be securely provided to the recipient.

SECONDARY USE OF DATA

MPHN acknowledge that much of their data is secondary data. The Australian Institute of Health and Welfare (AIHW) describe secondary use of data as "any application of data beyond the reason for which they were first collected (known as the primary use or purpose). An example of this is data collected by general practice recording patients care. Secondary use of this data occurs when using aggregated patient data to describe general practice use across the MPHN region. Secondary use of data presents an enormous opportunity to improve the treatment that Australians receive through quality improvement. A note of caution, the "use of an individual's health data to enable these improvements must be balanced against the risk to their privacy."

CONSENT

The Royal Australian College of General Practitioners (RACGP) have developed a guideline as to Patient Consent in the General Practice environment that, alongside the advice provided by other sources including the Privacy Act, guides MPHN in terms of what consent does and does not apply to data that they collect or analyse. Elements of consent related to patient data include;

- nformed consent
- Inferred or express consent
- A verbal or written consent may be:
  - express – when a patient signs or clearly articulates their agreement
  - inferred (or 'implied') – where the circumstances are such to reasonably infer the patient has consented.
- Withheld consent
- Competence, capacity and maturity to provide consent

MPHN accredited General Practices comply with the above core standard 6.

DATA GOVERNANCE FRAMEWORK
MURRUMBIDGEE PRIMARY HEALTH NETWORK

PRINCIPLE 5: DATA MANAGEMENT

DEFINITION, COLLECTION, MANIPULATION, ANALYSIS AND DISSEMINATION

CONTEXT

Management of data through all stages will be articulated and in line with best practice principles. Analysis and interpretation will be considered and used to inform identification of needs and planning of service delivery.

RATIONALE

Detailed management that follows robust documented processes will lead to confidence in the evidence that informs the work of MPHN.

DETAILS

DEFINITION

Data is typically comprised of numbers, words or images. Data includes representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing.

Definition of metadata

- Structural metadata – data about the containers of data (i.e. data element definitions)
- Descriptive metadata – individual instances of application data or the data content (may be excel files, access databases, online data extracts and commissioned service provider reports)

Definition of data elements

- Precise – The definition should use words that have a precise meaning. Try to avoid words that have multiple meanings or multiple word senses.
- Concise – The definition should use the shortest description possible that is still clear. Definitions should not contain acronyms that are not clearly defined.
- Non Circular – The definition should not use the term you are trying to define in the definition itself. This is known as a circular definition.
- Distinct – The definition should differentiate a data element from other data elements. This process is called disambiguation.
- Unencumbered – The definition should be free of embedded rationale, functional usage, domain information, or procedural information.

COLLECTION

External data

For external data, the process of data capture/collection, extraction, migration and conversion will be undertaken in the data warehouse by an automated process. The frequency of data capture will be determined in line with Commonwealth requirements for updating of needs assessment information. Data will be stored in the data warehouse.

Data provided to MPHN from Commonwealth sources where approval to share externally is denied will not be publically reported. The purpose for this data is to inform needs assessments and will be used in that capacity only.

Internal data

For Internal data, any reports and/or data sheets provided to MPHN by commissioned services or created by MPHN staff for the recording of data and information relevant to their work programs will be stored in the data warehouse. In the first instance management of data collection will remain with the Portfolio/ Project Manager. Tracking and uploading of data in compliance with contractual obligations remains the domain of the relevant Portfolio/Project Manager. Once data has been uploaded to MPHN data will be stored in the data warehouse.

Commissioned providers of MPHN are required to obtain informed consent from consumers of services to ensure that consumers are aware that data will be collected, stored and used by themselves and MPHN.

MANIPULATION

Any data set designed by MPHN will comply with best practice and any relevant legislation in relation to method of collection and capacity to include logic checking at the data collection stage. Data cleaning will be undertaken on all MPHN data sets regularly prior to analysis. Data cleaning will be undertaken once data has been uploaded to the data warehouse and will be overseen by the Senior Data Analyst.

ANALYSIS

Data analysis and/or modelling will be conducted primarily by the Senior Data Analyst for the health needs assessment however may be conducted alone or in concert with the Senior Data Analyst by other staff from time to time.

Data analysed will be reported in line with standard statistical analysis outputs and will ensure that where there are issues related to interpretation due to sample size constraints that data is suppressed in accordance with Australian Institute of Health and Welfare guidelines. Data that contain results with a sample size less than 20 at the local government area level will not be reported.

Internal data will be analysed in the data warehouse and provided as an interactive report in aggregated detail via MPHN SharePoint Power BI program. Staff access to the relevant output will be maintained by the data custodian to inform contractual compliance and allow interpretation to guide service delivery.

Internal and external data will be aggregated for use in triangulating health needs assessment and consequently planning arising from the identified needs. No provider will be identifiable in the process of needs assessment nor planning of services.

DISSEMINATION

External data may be disseminated by any staff member of MPHN after approval from the CEO or their delegate provided it is released in Portable Document File (PDF). No raw data may be released to any external party. Any data released outside of MPHN must be aggregated.

All data reports may be shared with providers however will only be provided to providers with de-identified provider data (i.e. aggregated for all other peer providers).

DATA RESPONSIBILITIES

CONTEXT

Effective data governance requires an all of organisation approach to maximise data security. Roles that support effective data governance are outlined below.

RATIONALE

Simple, clear rules and guidance on the specific roles and responsibilities for data content, collection, use, access, aggregation, for MPHN data sets.

DETAILS

DATA CUSTODIAN

Description

The MPHN data custodian is the Senior Manager Planning and Data Analytics.

Responsibilities

- Ensures access to the data is authorised and controlled and is protected against unauthorised access or change
- Ensures data has approval of provisioning requests for access to source data
- Ensures technical processes sustain data integrity and technical controls safeguard data
- Ensures processes exist for data quality issue resolution
- Ensures data added to data sets are consistent with the common data model
- Ensures versions of master data are maintained along with the history of changes and can be audited
- Ensures data has clear and unambiguous data element definition and does not conflict with other data elements in the metadata registry (removes duplicates, overlap etc.)
- Ensures data is still being used (i.e. fit for purpose, remove unused data elements)
- Ensure there is a documented process for responding to breaches and implement as required
- Ensures data has adequate documentation including metadata, data dictionary, specifications and business rules and how to use guide
- Escalate risks and issue to data sponsor

DATA SPONSOR

Each MPHN data set will have a Data Sponsor, this will be the CEO or CEO delegate. Roles of the data sponsor include;

- Establish the basis for the Data Set
- Participate in the PIA
- Provide direction and guidance, and authorise appropriate resources for management of the Data
- Authorise any public release of data
- Ensure compliance with all relevant legislation, policies and standards
- Appoint a Data Custodian (or Data Steward) and ensure duties are fulfilled

DATA STEWARD

Each data set in addition to the data sponsor and data custodian will have a data steward.

Roles of the data steward include;

- Manage the Data Set in compliance with relevant legislation, policies and standards, and any conditions specified by the Data Sponsor
- Ensure there are up-to-date technical documents for the supply of data
- Work with stakeholders to develop and maintain metadata including a data dictionary, business rules and guide to use
- Co-ordinate stakeholder engagement and input into the business requirements for the Data Set
- Provide feedback to data suppliers in relation to data quality issues
- Escalate material risks and issue to the Data Custodian

MPHN STAFF

From time to time may be responsible for the collection of data or the receipt of data from service providers. Once data has been receipted into the MPHN from a service provider the role of the staff member is to ensure the data is forwarded to the Data Analytics team for storage in the data warehouse. No other copies of the data should be saved.

MPHN BOARD/DIRECTORS AND EXECUTIVE

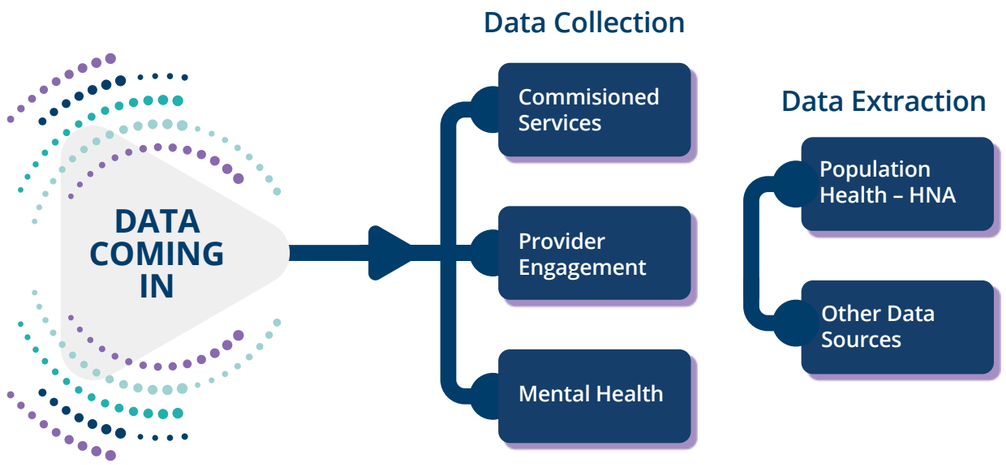
Directors and Executive staff have an obligation to ensure that the privacy, security, confidentiality, integrity of all MPHN data is maintained in line with highest standards. The Directors and Executive responsibility is to ensure that legislative compliance is adhered to at all times and that transparent and ethical data management practices are undertaken for all MPHN data.

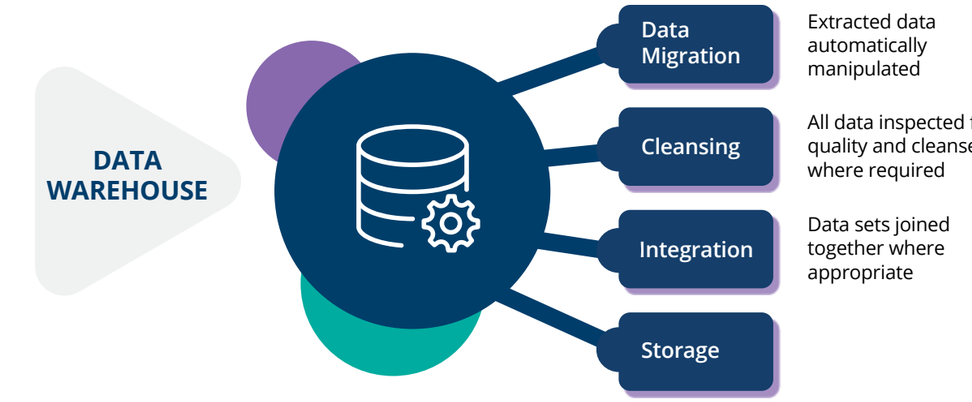
DEFINITIONS

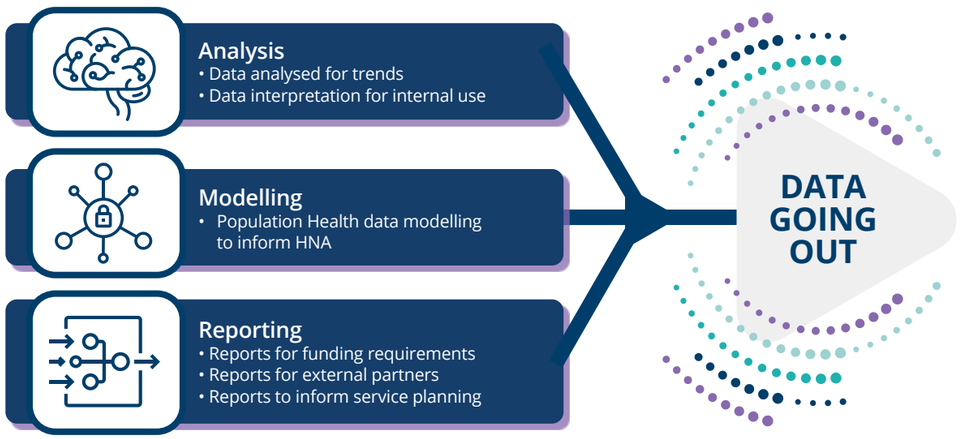
This policy applies to the management of data in any medium.

Data	Data is typically comprised of numbers, words or images. The representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing.
Data Management	Data management is concerned with valuing and managing data as a strategic asset.
Data Quality and Integrity	Data quality and Integrity is concerned with ensuring methodical data collection and practices to enhance quality and integrity with respect to accuracy and validity.
Data Custodian	Roles and responsibilities described in document
Data Sponsor	Roles and responsibilities described in document
Data Steward	Roles and responsibilities described in document
Data Capture/ Collection	Data capture is concerned with the collection, maintenance and storage of data. Data capture in the MPHN is automated where possible.
Data Extraction	Data extraction is the process of taking data from another source and importing it into the MPHN Data Warehouse for storage.
Data Migration	Data migration is concerned with transferring data between either storage types, formats or computer systems.
Data Conversion	Data conversion is the process of converting data from one format to another.
Data Storage/ Warehouse	Data storage in the MPHN is within a 'Data Warehouse'. The MPHN Data warehouse will be password protected and will be accessible by a minimum amount of staff.
Data Cleansing	Data cleansing may be used for standardising data from multiple sources or a process undertaken to ensure the validity of the collected data. Data cleansing is concerned with detecting and correcting or removing corrupt or inaccurate data.
Data Integration	Data integration is the process of combining data residing at different sources and providing the user with a unified view.
Data Maintenance	Data maintenance refers to the control of data versions to ensure the most up-to-date data is used.
Data Analysis	Data analysis refers to the interpretation of given data in the context of which it is being used.
Data Modelling	Data modelling is a method used to define and analyse the data requirements needed to support agency processes and service delivery.
Data dissemination	Data dissemination refers to the provision of data in its own format or as analysed data in the form of information to another person or organisation.
Low risk de-identified data	All de-identified health data is presumed to be able to be released to the public unless restricted by statute or other regulation, or where an individual has advised that their personal information cannot be used for purposes other than for which it was supplied.
High risk identifiable data	Access to identified and identifiable data is restricted by legislation and cannot be used for secondary purposes unless agreed by the individual or as specified under legislation.
Data suppression	Data that contain results with a sample size less than 20 at the local government area level will not be reported.
External data	This refers to any data source that is held by an agency, Commonwealth, State, University or other that provides data related to health or health services.
Internal data	This refers to any data source that is held or collected by any member of MPHN staff related to health or health programs. This includes all data collected from commissioned services of MPHN and includes all general practice data collected by MPHN.
Quantitative Data	This refers to data that is traditionally numbers and can be counted.
Qualitative data	This refers to data in the format of words which can be grouped into themes.
Raw Data`	This is data that is in its original format. Data has not been cleaned. This data may be identifiable or may include de-identified data.

DATA ROADMAP







TYPES OF DATA COLLECTED BY MPHN

MPHN has extensive data sets of both external and internal data that is utilised across the organisation to support its functions. Data is used in both health needs assessment, planning of services and monitoring of services.

EXTERNAL DATA

Health Murrumbidgee Local Health District	Population level health and risk factor data
Census	National Health Performance Authority, Healthy Communities
Australian Institute of Health and Welfare	
govdex	Demographic Data
PHIDU	Social Atlas
NSW cancer institute NSW	Cancer Data
Australian Government Department of Health	Commonwealth Health data Australian Immunisation Register data
NSW Health / HealthStats NSW	NSW health stats data
Australian Early Development Census	Child education and development data
The University of Sydney	General Practice and workforce data - Primary Heath Care Research & Information Service
Australian Government Department of Health	Primary Mental Health Data Set National Mental Health Service Planning Framework

INTERNAL DATA

PenCS	General Practice Data
Microsoft Dynamics 365	Local primary care engagement data
myob	Finance data
Excel	Commisioned services data
Access	Specific project data Stakeholder data

APPENDIX A

In 2019 MPHN undertook a data governance assessment with Deloite in preparation for moving into the Primary Health Insights platform. This details MPHNs result.

Assessment of PHN Current State Assessment Reponses			
Current State Data Platform	Data Governance	Privacy	Data Security
Based on answers in CSA Green = Maturity in platform capability, already cloud based, low number of data sets to migrate, small data volumes Amber = Medium maturity or medium complexity to migrate data, average numer of data sets to migrate, medium data volumes Red = On POLAR (their DB), very basic platform capability maturity (ie excel, Access DB), high number of data sets to migrate, high data volume, On PENCS (PHN DB)	Maturity Scale assessed based on answers in CSA Green = High Maturity. Has a comprehensive Data Governance Framework. Has a Data Governance roadmap, multiple data governance and data management policies, procedures, and processes, roles and responsibilities defined, data governance committee or council exists and meets regularly Amber = Medium Maturity. Has a simple Data Governance Framework, a few policies and working on others, has roles for data custodian and data steward but not documented roles and responsibilities, aiming to form a data governance committe but dont have one yet, working on a DG roadmap Red = Low Maturity. No formal data owners identified, no data governnace framework, no roles and responsibilities, very few policies and procedures for data governance and data management, no DG committee/ council	Maturity Scale assessed based on answers in CSA What legislation do they operate under, do they have any specific Privacy Policies. Do they mention they work with identified data. Green = High Maturity or in WA (No current Privacy legislation), Have classifications for Data based on sensitivity of data, have a privacy management framework, comprehensive privacy and security policies include data breach process, roles and responsibilities. Do annual Privacy Impact assessments (PIA), Proactive Amber = Medium Maturity. Have some privacy and or security policies, have some roles and responsibilities defined. Not handling undentifiable data. Or have classifications for data sensitivity. Planning to do a PIA. Controlled. Red = Low Maturity or in Victoria under their privacy legislation, handling identifiable data. No data breach preventaion or data breach notification process. No Privacy management framework, no knowledge of Privacy impact assessments. Reactive	Maturity Scale assessed based on answers in CSA Green = High Maturity, Data Security Committee assigned to each business unit. Or Every employee is held responsible for data security. Access to database accounts is well defined process. Utilise principles of least privilege to grant access. Amber = Medium Maturity. Some Access controls are defined. Who is granted access is logged. Red = Low Security Awareness, Access is at discretion of IT, IT handles Data securty risks. Informal Processes.
G	G	G	G
PENCS, Local server with Data Warehouse and DataMart. Small data volumes	Have a DG framework, no DG Committee, no archiving standard or retention procedure, no standard patient consent form, Data Custodian role well defined and documented, DG roadmap is more of a process flow then a forward looking roadmap of DG improvements they plan to make.	Have a privacy policy, understand their privacy legislation, have a privacy officer, no PIA or privacy management framework. Privacy one of the DG framework principles. Do they have a data breach prevention process/ policy and data breach response procedure? One of their training for onboarding people is privacy. All councils or committee members and staff sign privacy and confidentiality agreements. Have a data breach prevention and procedure.	Data Security part of culture every employee held accountable, strong controls, CEO approval required access granted by role. Logged access. Manage data security risks.

		Current State Data Platform	Data Governance	Privacy	Data Security	Analytics Tools	BT Reporting Tools	Cyber Security
TOTALS	GREEN	1	1	1	1	1	1	1
TOTALS	AMBER	0	0	0	0	0	0	0
TOTALS	RED	0	0	0	0	0	0	0
TOTALS	N/A	0	0	0	0	0	0	0
	TOTAL	1	1	1	1	1	1	1

Data Validation
G
A
R
N/A

Assessment of PHN Current State Assessment Reponses			
Analytics Tools	BI Reporting Tools	Cyber Security	Overall Readiness Rating
Based on answers in CSA Green = Many analytics tools used, higher number of data analysts and data scientists on staff Amber = Moderate amount analytics tools used, moderate number of data analysts and data scientists on staff Red = No analytics tools or very low number used, small staff of data analysts	Based on answers in CSA Green = Many reporting tools used, higher number of data analysts and data scientists on staff Amber = Moderate reporting tools used, moderate number of data analysts and data scientists on staff Red = No reporting tools or very low number used, small staff of data analysts	Based on answers in CSA Green = Low Risk • Formal Cyber Strategy is in place and monitoring is performed on a periodic basis • Cyber capabilities is in line with industry best practice • Vendor Management is formalised and compliance is monitored • Enhanced Network security capability with near real-time monitoring Amber = Medium Risk • Cyber Strategy is in place and being monitored on an Adhoc basis • Some internal Cyber capabilities • Informal vendor management process is in place • Limited Network security capability Red = High Risk • Cyber Strategy not in place • Cyber Capability is reliant on vendor • Limited vendor management • Basic Network security capability	Based on the heat map rating from the current state technical landscape across the dimension of Data Governance, Privacy, Data Security, Analytics tools, BI reporting tools and Cyber security columns. The following numbers have been calculated to represent the magnitude of transition complexity between current state at PHNs and the desired future state. 1 = Transition complexity is low. Mostly Green ratings 2 = Transition complexity is medium. Mostly Amber ratings. 3 = Transition complexity is high. Mostly Red ratings. Where No response was given, this has been assessed as a Red rating because it suggests a high degree of effort from the program team to firstly gather the information on their current state and also a high degree of ambiguity around the current state.
G	G	G	1
Have a data team and use analytics in day to day operations and key decision making. Report to CEO. Not using R or Python or advanced analytics (AI or machine learning). 2 people use SPSS and SASS.	Dedicated BI team and resources use Power BI extensively have 25 licenses.	Cyber strategy is in place and assessed periodically. Access to data is by user group and restricted to appropriate people. System security is tightly managed by vendor and vendor compliance monitoring is performed. System vulnerability and hardening is tested on monthly basis and network security is monitored by single gateway firewall with internet filtering enabled. Physical access to server room is controlled and requires access permission.	Transition is low Complexity

phn
MURRUMBIDGEE
An Australian Government Initiative

mphn.org.au

Tel 02 6923 3100

Fax 02 6931 7822

1/185 Morgan Street, Wagga Wagga NSW 2650