AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

Data Governance Framework

2023

Table of Contents

REVISION HISTORY

Version	Approved by	Amendment notes
1.0	Data Governance Committee	31 Jan 2023
1.1	CEO	15 March 2023
1.1	Board	Endorsed 3 April 2023

ASSOCIATED DOCUMENTS

1. ACSQHC Data Management Policy (D23-544)
2. ACSQHC Data Plan
3. Privacy Policy (D14-15168)

Executive summary

The Data Governance Framework has been developed to ensure the appropriate use of data and data sources which are required to fulfil the Commission's Work Plan items, support the Commission's strategic priorities and meet its obligations under the *National Health Reform Act 2011* and the *National Health Reform Agreement – Addendum 2020-25*.

The intended scope of the Australian Commission on Safety and Quality in Health Care's (the Commission) Data Governance Framework, along with underlying data management policies and procedures, is to support and direct the appropriate access, use, analysis, storage, retention, and deletion of data outlined under the Commission's Data Plan.

The Commission's Data Governance Framework provides an overview of its data governance arrangements comprising:

- Key data governance concepts including collection, handling and reporting of data in compliance with legislative, regulatory and policy requirements
- Commission structures and roles to support good data management practices
- Key data management principles
- An overview of policies, guidelines and procedures for data management including integrated data management.

It is important for data governance to exist at every level in which data is created and used. Data can be stored in a variety of methods including:

- Structured formats, such as databases, geospatial data, and maps
- Semi-structured formats, such as spreadsheets
- Published formats, including content on websites
- Non-structured formats, such as emails, documents, computers, disks, hard drives, and USB sticks.

The Data Governance Framework will ensure that data:

- Conforms to appropriate standards of data management and quality prior to use
- Is used in accordance with appropriate approvals.

The data governance arrangements apply to all data requested, collected, or funded by the Commission. The framework should also be read in conjunction with the Commission's Data Plan, datamanagement policies, guidelines, procedures and privacy policy

Data governance

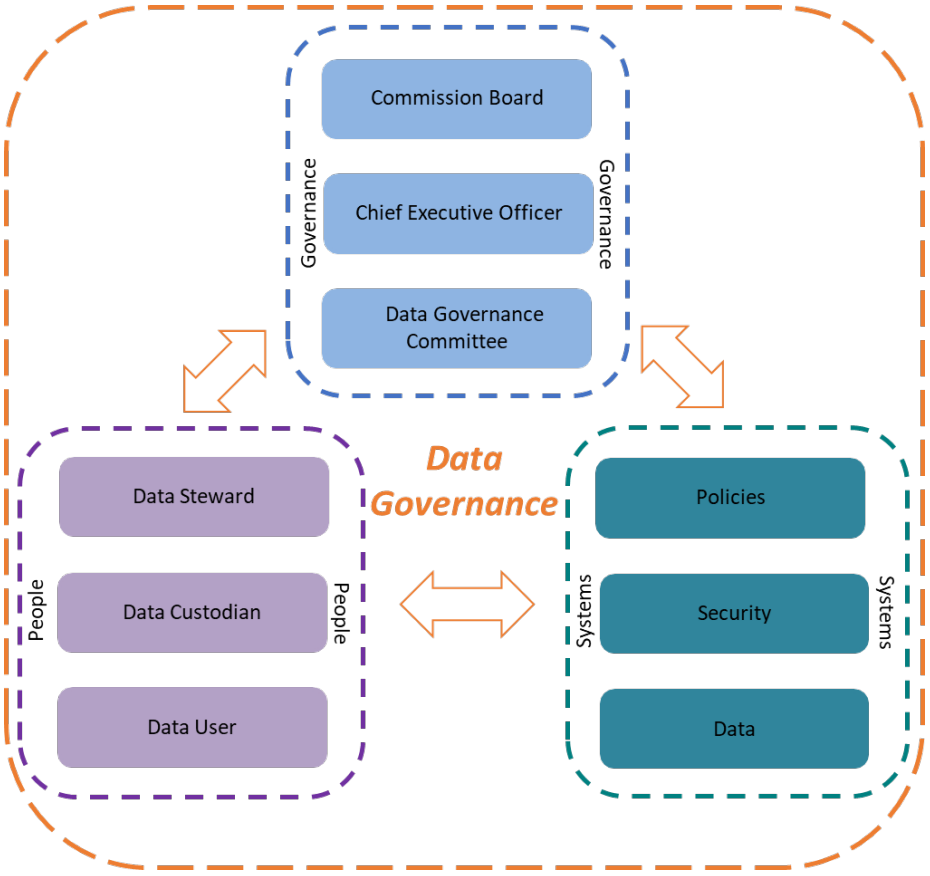
Data governance is "*the exercise of decision-making and authority for data-related matters. The organisational bodies, rules, decision rights, and accountabilities of people and information systems as they perform information-related processes".*[1]

Data management is the execution of data governance policies and procedures to use data to support decision making.

The Data Governance Framework is outlined in **Figure 1**. The components of the framework are:

- Governance – The Commission's Board and CEO determine the objectives, required outcomes and scope of the Commission's work.
- People – Responsible for acquiring, storing, managing, analysing and disseminating data according to data management policies. These people include data stewards, data custodians and data users.
- Systems – In the form of policies, procedures, security software and hardware to support data management.

Figure 1: Commission's Data Governance Framework



[1] The Data Governance Institute, datagovernance.com/the-data-governance-basics/data-governance-glossary/, accessed 8 August 2022.

Definition of data

Data is "*factual information used as a basis for reasoning, discussion or calculation*".[2]

A data holding is defined in the Commission as:

> *A cohesive set of data, designed to address specific business needs, which may be created externally and provided to the Commission, or generated internally, either by direct collection or modification of existing data.*

A data holding will:

- Be used for a defined purpose or set of purposes
- Be identified within the Commission as an asset using agreed metadata
- Have an identified data steward with responsibility for management of the data within the organisation
- Have one or more identified data custodians responsible for the operational aspects of handling the data
- Be held in one location (i.e. not stored multiple times within the Commission)
- Have a community of people who use the data
- Have policies and procedures that define how the data is created, updated, retrieved, checked, used, and destroyed, and metadata that records how and when these processes occurred.

Data collected, stored and used by the Commission may be raw or processed. Raw data, also know as primary data, refers to data collected directly from the source that has not been cleaned, organised, reformatted or translated into information. Raw data that has been altered or transformed into a format that is used for analysis and/or visualisation, is processed data. Processed data is information that can be used to support program areas and generate project outputs.

The scope of the Data Governance Framework is the life-cycle management of all of these types of data. This excludes data related to the Commission's administrative and operational functions, such as financial or human resources data.

[2] http://www.merriam-webster.com/dictionary/data, accessed on 28 August 2022.

Legislation and agreements

The Data Governance Framework deals with all health information and sensitive information. The Commission's Privacy Policy specifies requirements regarding personal information.

Health information' is a subset of 'personal information' and includes:

- information collected in connection with the provision of a health service;
- information or opinion about the health or disability of an individual;
- an individuals expressed wishes about the provision of health services; and
- any information about health services provided to an individual.

The Commission operates under a number of agreements and legislation, including:

- *Privacy Act 1988*
- *Protective Security Policy Framework*
- *Freedom of Information Act 1982*
- *National Health Reform Act 2011*
- *National Health Reform Agreement and Addendums (2011 to present)*
- *Australia Health Performance Framework*
- *National Healthcare Agreement 2012*
- *National Health Information Agreement 2013*
- *Data Accessibility and Transparency (DAT) Act (DATA) 2022.*

Obligations under the *National Health Reform Act* apply to the Commission's use and disclosure of information. However, the Commission has specific obligations under the *National Health Reform Agreement,* and subsequent *Addendums,* in respect to the use and disclosure of 'protected Commission information'.

Protected Commission information means information that:

- Was obtained by a person in the person's capacity as an official of the Commission
- Relates to the affairs of a person other than an official of the Commission.

Security and privacy

The Commission is committed to using data and information in accordance with relevant legislation and national privacy principles, ethical guidelines and practices.

Security

Systems and processes used for collection, analysis and storage of data and information have been designed to ensure that the confidentiality, integrity and availability of data and information is protected. Data and information must be maintained in a secure environment and in accordance with the:

- Australian Government Protective Security Policy Framework
- Australian Government Information Security Manual
- Data security aspects of the data user 'accreditation' process of the DAT Act 2022
- Commission's Agency Security Plan (D15-3999).

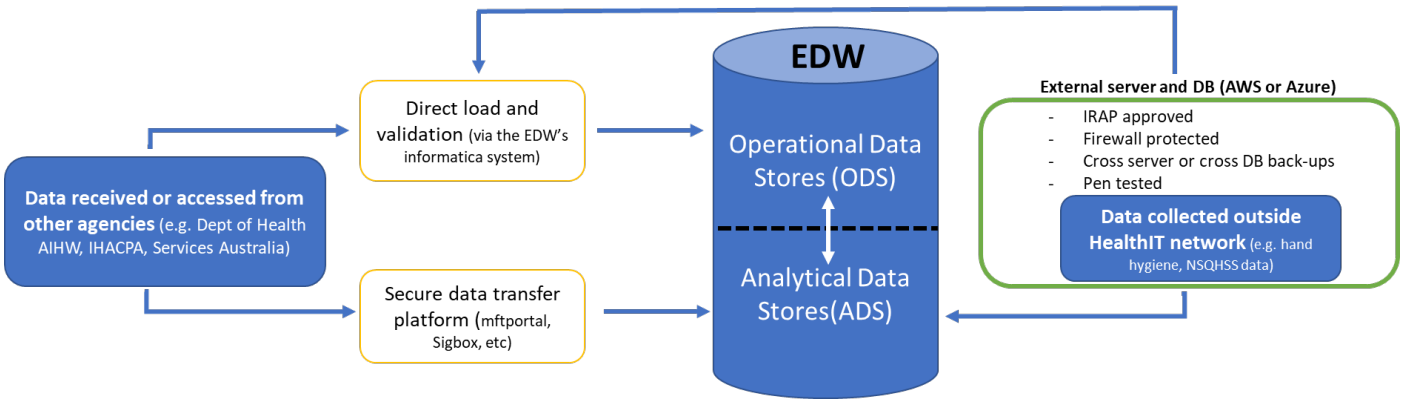
The Commission utilises the Commonwealth Department of Health and Aged Care's (the Department) IT Network and Enterprise Data Warehouse (EDW) under the existing shared

services agreement, for the access, storage and analysis of data collections. The EDW complies with all Commonwealth Government data and IT infrastructure privacy and security regulations and principles. Under the shared services agreement, updates to the IT network, EDW and relevant software and systems are undertaken by the Department. The Department also manage licensing and undertakes periodic IT security tests and audits.

For data collected and stored in databases outside of the EDW in Commission owned servers, initial and periodic independent security assessments and penetration testing is undertaken to ensure the appropriate security controls are in place for the systems and servers that hold these databases. The most recent assessment was completed in June 2022.

A recommendation from the June 2022 assessment was implementing cyclical penetration testing, over a two-year cycle, on systems that are deemed higher risk (such as the NSQHS Standards data portal). None of the systems and data the Commission accesses outside the EDW were classified above Official Sensitive, therefore yearly penetration testing is not required.

Database and data flow diagram



Privacy

The Commission is subject to privacy obligations under the *National Health Reform Act, the Privacy Act 1988* and the *Privacy Amendment (Enhancing Privacy Protections) Act 2012*.

The *Privacy Act 1988* sets out 13 Australian Privacy Principles (APPs) which apply to the collection, use, disclosure and other aspects of handling personal information. These principles apply to and must be complied with by the Commission.

Data accessed by the Commission to fulfil its work programs and legislated functions is deidentified and any analysis for publication purposes ensures appropriate confidentiality and small cell related suppression protocols be applied.

The Commission operates within the DATA Scheme for accessing and sharing Australian Government data, established through the *DAT Act 2022*. This works in conjunction with the *Privacy Act 1988* to protect the sharing, collection and use of personal information. The DATA Scheme requires that data requested and/or shared must be in the public interest and for one of

three purposes:

- Government service delivery
- Informing government policy and programs
- Research and development.

Data and information obtained and held by the Commission as an employer or for operational purposes, such as personal details and documents of staff and committee members, are handled and retained in accordance with the Commission's Privacy Policy (D14-15168) and relevant Commonwealth legislation and records management processes. These include alignment with the:

- *National Archives Act 1983*
- *Privacy Act 1988*
- Protective Security Policy Framework (PSPF)
- Records Authority 2020/00352226 Australian Commission on Safety and Quality in Health Care (TRIM D21-22649)
- ACSQHC Information and Records Management Strategy (D20-31679)
- ACSQHC Information and Records Management Policy and Framework (D20-31680).

Metadata Online Registry

The Metadata Online Registry (METeOR) is Australia's web-based repository for national metadata standards for the health, community services and housing assistance sectors. Hosted by the Australian Institute of Health and Welfare (AIHW), METeOR provides users with a suite of features and tools, including online access to a wide range of nationally endorsed data definitions. The AIHW also provides user support and assistance.

Under the *National Health Reform Act* 2011, the Commission is required to 'formulate, promote, support and encourage the use of indicators'. In addition, the *National Health Reform Agreement* requires the Commission to 'recommend national datasets for safety and quality, and to report publicly on the state of safety and quality'. To ensure national consistency and availability of resources, the Commission uses METeOR to maintain indicator specification and data set specifications.

As of July 2016, the Commission has been established as an autonomous Registration Authority in METeOR to enable the Commission to register, develop and endorse its own metadata content for local and national indicators of safety and quality in health care.

Data governance structures and roles

Commission Board

The Commission's Board governs the organisation and is responsible for the proper and efficient performance of its functions. The Board establishes the Commission's strategic direction, including directing and approving its strategic plan and monitoring implementation of the plan. It also oversees the Commission's operations and ensures that appropriate systems and processes are in place so that the Commission operates in a safe, responsible and ethical manner, consistent with its regulatory requirements. The Board is established and governed by the provisions of the *National Health Reform Act* and the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

Chief Executive Officer

The Chief Executive Officer manages the Commission's day-to-day administration and is supported by an executive management team, internal management committees and staff members. The Commission's internal governance arrangements include internal management, risk management, fraud control and internal audit.

Security executive

The Chief Operating Officer acts as the security executive and is responsible for the Commission's protective security policy and oversight of the protective security practices, as outlined in the Commission's Agency Security Plan (D15-3999).

Data Governance Committee

As part of its role to develop and oversee the implementation of the Commission's data policies and procedures under the Data Governance Framework, the Data Governance Committee will assume responsibility for:

- Developing, implementing and maintaining the Commission data management policies and procedures manual
- Developing and delivering appropriate education, training and support activities for data stewards, data custodians and data users
- Establishing and reviewing an overall program of standards, monitoring and compliance, which encompasses:
  - Ensuring data holdings are allocated to Data Stewards and Data Custodians
  - Setting, implementing and monitoring standards for:
    - the storage and use of data holdings (including reference and master data sets)
    - security of data holdings
    - data standards/quality
    - metadata requirements and solutions
    - other data management compliance measures as required
- Resolving issues raised by Data Stewards and Data Custodians
- Initiating and participating in the development of IT solutions for data management activities
- Provide advice to Commission staff on best practice management and reporting of data
- Provide guidance and approval to any metadata standards (including METeOR)
- Ensuring the Commission's data user accreditation status and obligations under the DAT Act 2022.

The membership of the Data Governance Committee includes the:

- Chief Operating Officer
- Director, Safety and Quality Improvement Systems
- Director, Intergovernment Relations (Chief Privacy Officer)
- Director, Healthcare Variation
- Director, Strategy and Innovation
- Director, eHealth and Medication Safety (Chief Information Officer)
- Manager, Data Analytics and Patient Safety Measurement (Data Custodian)
- Manager, Data and Reporting Strategy, Healthcare Variation.

Data Steward

A Data Steward manages the usage and quality of one or more data collections from a management perspective. A Data Steward is often a subject matter expert. A Data Steward will understand the business requirements for collecting and holding data, as well as its permitted uses, publication and dissemination.

Data Stewards have dual roles in education and training. Collectively they are responsible for ensuring that Data Custodians and Data Users have an awareness and understanding of the Commission's data management policies and procedures, and access to appropriate education and training in order to implement those policies and procedures. For each of the data holdings under their care, Data Stewards also have a responsibility to ensure that their users have access to the information (mostly in the form of metadata) and skills they require to correctly access and use that data.

A Data Steward will provide clear delegation and instructions to data custodians so that access and security privileges to their data holdings are maintained and monitored.

Under the Data Governance Framework, data stewardship is provided by programs areas. As such the Data Steward roles and responsibilities sit with Program Directors and can be delegated to relevant staff when required.

The current program areas with data stewardship responsibilities include:

- Healthcare Variation
- Intergovernment Relations
- HAI/IPC and Emerging Issues
- National Standards
- eHealth and Medication Safety
- MedicineInsight
- Safety and Quality Improvement Systems.

Data Custodian

A Data Custodian performs operational management of the collection, storage and use of one or more data collections. Data Custodians should have high levels of data literacy, as well as skills in data management software system, analytical methods and tools.

The Data Custodian is responsible for:

- Approving access to, and use of, data collections for which they have delegated authority
- Ensuring data collections are protected from unauthorised access, alteration or loss

- Providing advice to users of the data, including any caveats on the use of the data
- Submitting all data acquisition requests on behalf of the Commission.

This means that they may be involved in the design of data acquisition, receipt and storage, processing, analysis, reporting, dissemination and perhaps archival or deletion of data. Data custodians generally have considerable skills in using data and the associated software tools and systems. They are required to follow the Commission's policies and procedures on the secure storage and transfer of data to external stakeholders.

Data Custodians require IT support tools to allow them to view and monitor their role. This includes access to effective metadata so that they can fully understand the context, definitions, meaning and data quality indicators for the data they are using.

It is possible for the same person to perform the dual roles of Data Steward and Data Custodian.

The role of Data Custodian for the Commission is currently assigned to the *Manager, Data and Analytics*, approved by the COO in October 2019 (TRIM: D20-23044). The Data Custodian role is reviewed when necessary, such as when there is a staffing change to the current role.

Data Users

Data Users are those staff within the Commission who need access to the data for analysis but who are not custodians or stewards of the data. Data Users normally have varying levels of data literacy and data management skills.

A Data User is often referred to as a 'read-only user' as they may have access to specific data holdings to be able to analyse and report on the data, but they generally do not have the authority to update (edit), copy or delete the data.

By being provided with access to data, Data Users are assuming responsibilities for its correct use, analysis, interpretation and reporting and they must be supported in this role through effective IT systems, education, training and support.

Where a Data User is unsure of their authority to access, analyse, report or disseminate data they should refer issues to the appropriate data custodian in the first instance.

The actions of Data Users must be visible to the Data Custodians of the data they are using.

It is possible that an individual may be a Data Steward, a Data Custodian and a Data User, though for different data holdings.

The Commission recognises the potential risks associated with staff performing a Data Steward and/or Data User role in addition to their program area work and responsibilities. To minimise this risk, the Commission ensures the appropriate training, resources, guidance and Data Custodian support is made available to staff undertaking these data related roles (as outlined in the Data Management Policy).

Data management principles

A data management principle is a fundamental statement that serves as the foundation for a system of behaviour. These principles are required to obtain and maintain an organisation's

'accredited status' under the *DAT Act 2022*. The Commission's data management principles (listed below) therefore provide an organisation-wide basis for data management behaviour.

- Data will only be collected, stored, used, published and archived with appropriate authority and for appropriate purposes.
- Data will be collected, stored, used, and archived according to defined procedures.
- Data will be defined and documented in a consistent form (metadata), including quality indicators.
- International and national standards and conventions for data and data management will be formally recognised and adopted where appropriate. Best-practice solutions (e.g. METeOR for metadata) will be adopted for specific aspects of the Commissions business.
- Wherever possible, data will be collected once, from one source and stored for a defined purpose.
- Data will be protected with appropriate security systems and procedures, including the application of reasonable security standards depending on the type and sensitivity of data as well as protections to prohibit re-identification of de-identified data.
- Data will be made easily accessible to users to promote and support re-use, in accordance with authorisation principles and agreements, while ensuring said users are appropriate persons with a reasonably necessary need to access such information.
- The input of stakeholders and experts (e.g. in the form of advisory groups) will be used to continually monitor and improve data management practices, particularly in the development of new data sources, safety and quality indicators, collection methodologies, and METeOR specifications.
- Staff will be supported in their data management responsibilities and activities through appropriate and well-resourced systems, procedures, induction materials, education, training and support.
- Data management activities will be subject to routine audits to monitor the effectiveness of the implementation of policies and procedures. This process will be facilitated by the Data Governance Committee.

Policies, guidelines and procedures

The Commission has developed a Data Management policy (TRIM: D23-544) and a suite of procedures to align with key data management principles of:

- Data governance
- Data development
- Data acquisition, storage and management (including deletion)
- Data security
- Reference and master data management
- Data quality management
- Data processing
- Data disclosure and reporting
- Metadata management
- Staff education, support and training.

Measuring data management and compliance

Over time the Commission will develop and measure compliance with data management policies and procedures, based on the assessment of risks. As an organisation, the Commission will need to determine the highest risk data management activities and ensure that there are checks and safeguards in place.

In addition to systems support for compliance, the Commission will implement reviews and audits of specific aspects of data management in order to assess our levels of compliance, and any issues which may be limiting the Commission's ability to comply.

The Data Governance Committee has responsibility for implementing data management compliance systems and support, as well as for initiating reviews and audits (when required).