2023

Capital Health Network Data Governance Framework

External Data Governance Framework: This document is for use with external stakeholders to communicate CHN's approach to Data Governance.

Contents

Purpose

The CHN Data Governance Framework lays out guiding principles, the operating model, and enabling mechanisms for CHN to be an entrusted data acquirer and provider. This Framework is designed to ensure effective, formal, and consistent risk-based management of data assets. It supports CHN, in its role as a data custodian, provide assurance about its data governance practices to external stakeholders and partners including general practices, other data suppliers or recipients, professional bodies and government agencies.

Data governance is focused on supporting ongoing business operations, legislative compliance, and responsiveness to new opportunities. It creates accountability, and enables harnessing the power of data received, generated, provided and reported by CHN. The Framework assists CHN balance data privacy and security expectations, with safe and efficient sharing of data, and continuous delivery on PHN Programme Objectives.

Data is managed, secured, and accounted for as a strategic asset. This entails implementing and maintaining appropriate access controls, privacy management measures, and security standards which can provide assurance and generate confidence for data providers sharing data with CHN.

Applicability

This document contains key information for all CHN staff and in particular those who have delegated authority to make data-related decisions. It is also an important source of information for those many organisations and agencies that provide data to, or receive data from, CHN, as well as its partners, stakeholders and end-users of CHN data and information. This data governance framework and related policies apply to all CHN data sets.

Data governance implementation

Principles

The following principles frame and guide the implementation of data governance at CHN:

- Accountability: Data assets are governed by formal organisation stewardship, with oversight and management applied throughout the data lifecycle.
- Data for good: CHN uses and shares data to benefit the community and with the aim of improving health services and outcomes. CHN does not commercialise its data.
- Indigenous data sovereignty is recognised and incorporated in data governance and management practices.
- Usability: The value of data assets is based on how they are used at the program and corporate level.
- Due diligence: Data-related risks, with a special focus on privacy, security and access across the data lifecycle and environments, are continuously monitored and reported.
- Quality: Data integrity and quality is maintained consistently and reflects standardisation required across primary health networks.

Data Management Policies and Procedures

Data management policies and procedures are designed to help manage privacy and security-based risks during data acquisition, access, storage, use, distribution, archival and destruction. These

procedures are also supported by various tools such as Privacy Impact Assessments, CHN's Data Inventory, CHN's Data and Reporting Dashboard. Relevant internal documents include:

- Aboriginal and Torres Strait Islander Data Governance Framework
- PHI National Data Governance Principles
- CHN internal data management policies
- Digital Health Strategy
- CHN Quality Improvement policies

Data Governance Structures

CHN's Data Governance Council provides cross-organisational leadership and oversight to data governance activities. The Data Governance Committee (DGC) brings together representatives of Capital Health Network (CHN) from all business areas within the organisation to ensure effective, efficient, and approved, acquisition, use, and management of CHN's data assets. The DGC monitors data risks, oversees privacy impact assessments, and assesses suitability of control measures to reduce inherent risks and makes recommendations to the CHN Executive Team. Key functions of the Data Governance Council are to:

- Oversee effective, efficient, and approved acquisition, use, and management of CHN's data assets.
- Ensure responsibilities associated with use and management of data are understood and accepted.
- Enable shared understanding of enterprise-level priorities for data management and data analytics, such that these align with CHN strategic objectives.
- Recommend for sponsorship and support realisation of value creation opportunities.
- Oversee and enable uplift of data analytics capabilities,
- Oversee governance of data collection and sharing arrangements.
- Monitor CHN data risks, assess adequacy of and recommend improvements to control mechanisms.
- Assess and manage disclosure risks inherent in data sharing arrangements with external agencies.
- Monitor response to notifiable data breach incidents, recommending improvements to data management practices, and capabilities to prevent recurrence.
- Oversee and monitor projects to improve CHN's data management, storage, and use.

The Data Governance Council is chaired and championed by an Executive Sponsor and the Council is accountable to the CHN Executive Team. CHN's Executive reports regularly to CHN's Audit and Risk Committee and Board. CHN's Data Governance Council also has representation on the National Data Governance Council convened the PHN Cooperative.

Data roles and responsibilities

CHN maintains a Data Inventory to support the monitoring and use of all priority data sets across the data lifecycle. The Data Inventory holds important and standard information to ensure all CHN staff are supported in the appropriate use of the data. Each data set has an appointed Data Steward and Custodian to oversee the use and management of the data set.

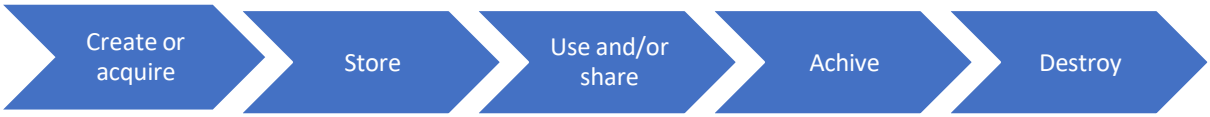

Figure 1: Data Lifecycle

Data User: A person who is an authorised user of a data collection. A data user is responsible for:

- Ensuring that their access to the data 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 or accessing data on behalf of any other person; (any person who wishes to access data should apply to the data custodian for authorisation).
- Understanding their obligations with regard to consent, data sharing, data management.

Data Stewards: A Data Steward is a person designated by the Data Custodian for each of the data sets, who is responsible for data held within that single system, or as a part of a larger system/ application/ database. Data Stewards are responsible for:

- Understanding their obligations with regard to consent, data sharing, data management.
- Defining the lifecycle to the data
    - What data is accepted to their system?
    - What meta data is required?
    - What data can be shared (internally/externally)?
    - What data can be linked to other systems or applications?
    - When are records closed?
    - When can records be archived?
    - Can the data be destroyed?
- Monitoring data sets and data sharing agreements
- Ensuring meta data is captured by the data registry
- Reviewing new data sets and leading Privacy Impact Assessment
- Semi-annual review of all data sets and sharing agreements
- Recommending sharing requests within CHN:
    - What is the request?
    - Does the request align with CHN's data governance policies and any data sharing agreements?
    - What will the data be used for?
    - How will the data be shared and how will it be protected?

Data Stewards are likely to be a Manager or Senior Manager. Ideally there will be one assigned Data Steward for each data set. However, in some instances Data Stewardship may be shared, where a data set may be used for very different functions, e.g. the Primary Care Data Set as used for quality improvement and PiPQI versus the use for the Needs Assessment and/or research.

Data Custodian: A CHN Data Custodian is the CEO or a staff member with delegation from the Chief Executive Officer to exercise overall responsibility for a specified data collection, in accordance with policies, guidelines and any specific conditions for use applicable to that data collection, with the power to release data to other bodies or persons.

A data custodian is responsible for:

- Ensuring access to the data is authorised and controlled
- Ensuring data stewards are identified for each dataset
- Guiding Data Stewards in establishing escalation process
- Ensuring technical processes sustain data integrity
- Ensuring processes exist for data quality issue resolution in partnership with Data Stewards
- Ensuring prompt actions on breaches of policy (outlined in the policy)
- Coordinating responses to management of data breaches
- Ensuring change management practices are applied in maintenance of the database
- Authorising data and information sharing requests
- Reviewing and authorising completion of Privacy Impact Assessments

Monitoring and quality improvement

All CHN staff are responsible for monitoring and contributing the data quality improvement by

- Identifying data related risks
- Reporting real or potential data breaches
- Notifying data stewards and/or custodians of issues, errors or inaccuracies with regard to data sets or data sharing agreements
- Providing accurate information when requesting information to be shared externally

CHN's approach to quality improvement will be responsive and proactive:

- Data stewards will continuously monitor data sets and undertake review and analysis of identified problems. Issues, actions, and outcomes will be documented as part of the Data Governance Councils Risk, Issues, and Decisions register.
- The Data Governance Council will undertake regular proactive reviews and audits of policies, the data inventory, privacy impact assessments and data sharing agreements.

Associated documents

Legislation and policy guidance

- The Privacy Act - Home (oaic.gov.au)
- Australian Privacy Principles - Home (oaic.gov.au)
- Five Safes framework | Australian Bureau of Statistics (abs.gov.au)
- Territory Privacy Principles - Home (oaic.gov.au)
- Department of Health and Aged Care | PIP QI Incentive guidance
- Framework to guide the secondary use of My Health Record system data
- Resources - PMHC-MDS

Resources

- Data Governance Framework 2021 (aihw.gov.au)
- De-identification Decision-Making Framework - Home (oaic.gov.au)
- Privacy-and-managing-health-information-in-general-practice.aspx (racgp.org.au)

Acknowledgement

CHN would like to acknowledge Southwest Sydney PHN for providing examples of their Standard Operating Procedures and forms and allowing CHN to review and revise these for our organisation.

References

- The Privacy Act - Home (oaic.gov.au)
- Australian Privacy Principles - Home (oaic.gov.au)
- Five Safes framework | Australian Bureau of Statistics (abs.gov.au)
- Territory Privacy Principles - Home (oaic.gov.au)
- Data Governance Framework 2021 (aihw.gov.au)
- ABS Data Quality Statement Checklist

Versions

Version	Date Commenced	Change Description	Approved by Executive
V1.0	December 2020		
V2.0	January 2023	Roles and responsibilities, definitions, Data Steward SOP	16 January 2023