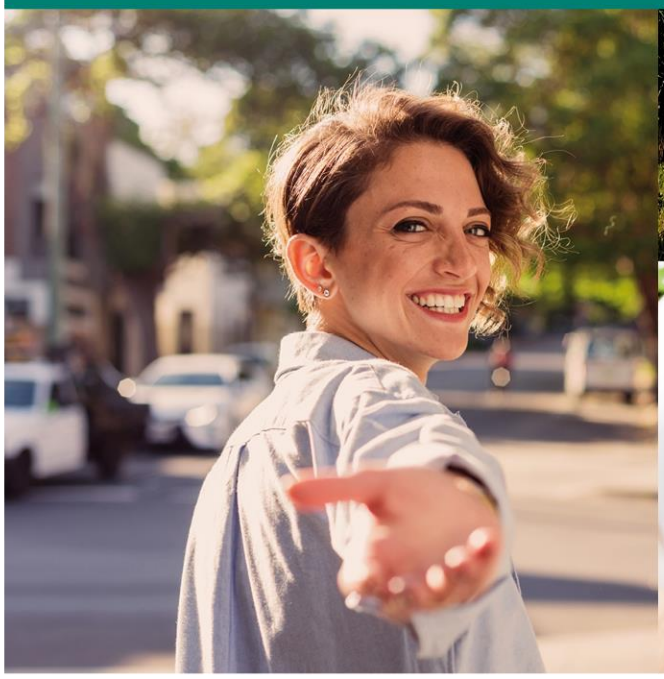
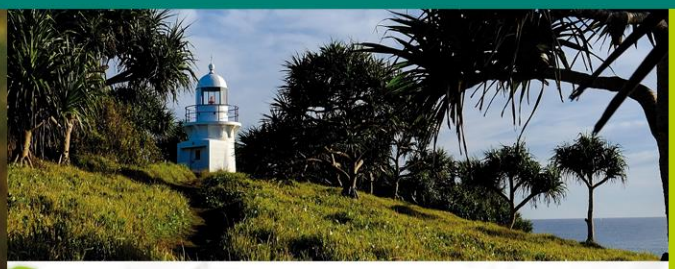
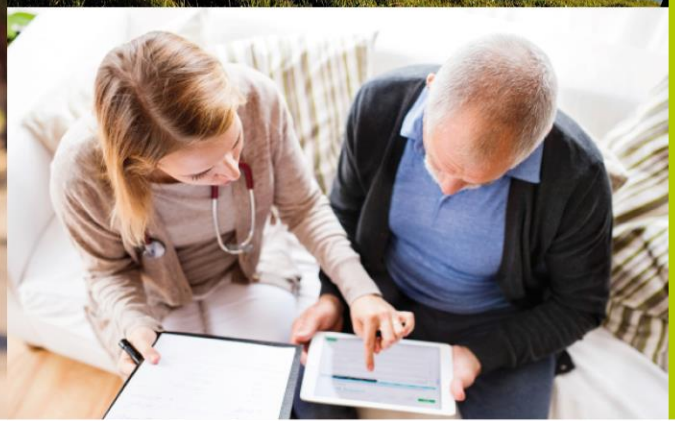
Data Governance Framework







Framework owner:	Director, Digital and Marketing
Framework contact:	Director, Digital and Marketing
Approved by:	Chief Executive Officer
Approval date:	06/01/2021

HEALTHY NORTH COAST

Healthy North Coast Limited
ABN 18 154 252 132
PO Box 957 Ballina NSW 2478
+61 2 6618 5400
hnc.org.au

Data Governance Framework

Healthy North Coast gratefully acknowledges Central Eastern Sydney PHN (CESPHN) — with permission, this Framework has been adapted from CESPHN's Data Governance Framework.

Table of Contents

1. Introduction

Healthy North Coast Ltd (HNC) recognises that data is a strategic asset that has value to the entire organisation and our service delivery partners. Data is the foundation of our planning and operational functions, and fundamental to quality, evidence and outcomes-based decision making. HNC is the custodian of a growing 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.

2. Purpose and Scope

The purpose of the Data Governance Framework (the Framework) is to outline how HNC effectively governs data. This includes:

- the legal and regulatory environment that mandates how we handle personal and sensitive information
- our guiding principles for governing data
- our governance structure including roles and responsibilities
- supporting policies and procedures
- systems and tools used to manage data throughout its lifecycle.

The Framework applies to all data assets listed in HNC's Data Asset Register. This includes data collected and/or enhanced by HNC, collected on behalf of HNC and data obtained from external sources.

2.1 Audience

The intended audience of this document is all HNC staff and HNC stakeholders, including, but not limited to, commissioned service providers, general practice, ACCHS and local health districts that provide, receive or use data from HNC.

3. Legal and Regulatory Environment

HNC must comply with the federal and state legislation, and health industry standards with respect to how data is collected, managed, secured, shared and protected. The following are key documents that are relevant to this Framework:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Health Records and Information Privacy Act 2002
- Freedom of Information Act 1982
- Australian Secure Cloud Strategy
- RACGP Computer and Security Standards
- Practice Incentives Program Eligible Data Set Data Governance Framework
- Framework to guide the secondary use of My Health Record system data.
- ISO/IEC 27001 Information Security Management standard

4. Guiding Principles

4.1 General Data Governance Principles

- **Data is secure and privacy is protected:** highest security standards are used to ensure data security and privacy. HNC's handling of personally identifiable data and information is kept to a minimum (most data sets are de-identified) and managed in accordance with relevant legislation.
- **Data is accessible:** data is available and accessible to authorised individuals when it is needed.
- **Data is discoverable and re-usable:** data is easy to find and re-used wherever possible and stored in one location to ensure there is a single version of truth.
- **Data is appropriately managed:** data is managed in a way that is transparent with clear roles and responsibilities to ensure accountability.
- **Data quality and integrity improvement is essential:** data is accurate and reliable. Data-related policies and processes focus on standardised ways to improve data quality and integrity.

4.2 Primary Health Care Data Governance Principles

Primary health care data:

- is a strategic asset critical to health planning
- is used appropriately to improve patient outcomes
- can be sensitive and must be governed with clear data stewardship throughout the data lifecycle; from creation to purge
- requires strong security standards and risk management frameworks to ensure professional obligations and legal requirements to keep patients' health information secure and private are upheld
- is de-identified and requires strong security standards and risk-management frameworks to ensure professional obligations and legal requirements to keep patients' health information secure and private are upheld
- is shared via secure digital systems and access to the data is highly controlled and limited to research that helps deliver insights on health trends and delivers population health improvements
- is governed by the principles of Indigenous Data Sovereignty
- is subject to a HNC Privacy Impact Assessment prior to publication on any shared data platform.

Referenced from Primary Health Networks Data Governance Framework Version: 1.0 – August 2020 release

5. Data Governance Structure

HNC's data governance structure is shown in Figure 1 below.

HNC's Data Governance Committee reports to the HNC Board Audit & Risk Subcommittee as needed.

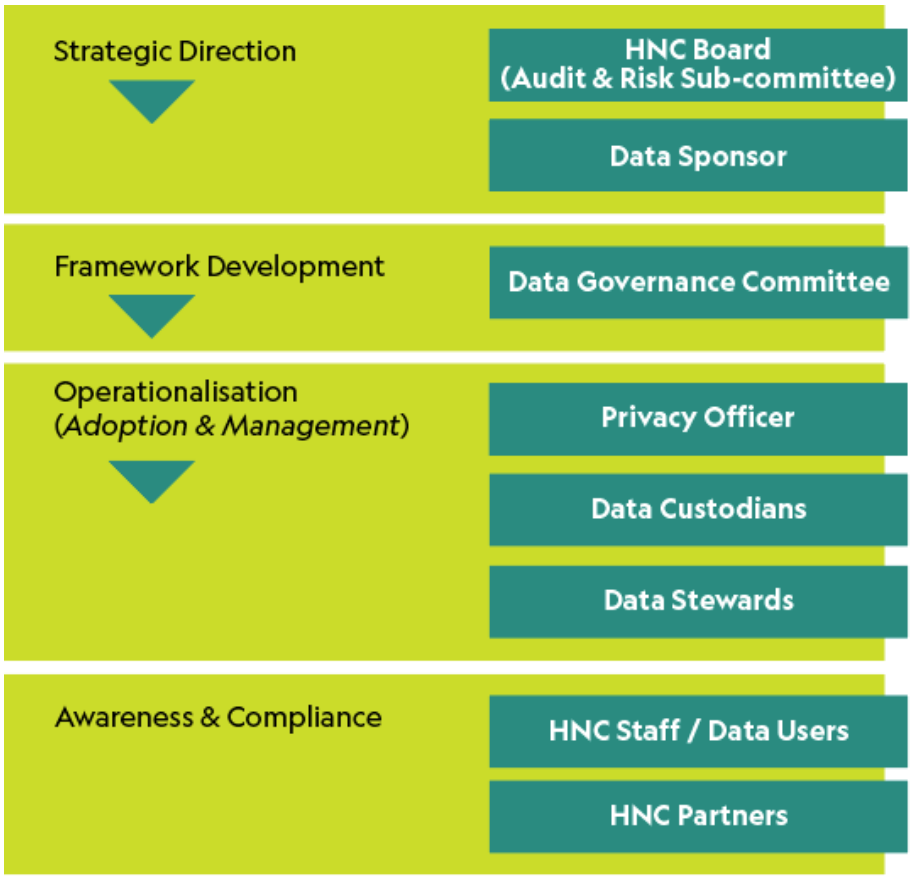


Figure 1: HNC's organisation structure.

6. Roles and Responsibilities

Data governance is everyone's responsibility – all staff have roles and responsibilities that are defined further below.

6.1 HNC Board (Audit and Risk Sub-committee)

The Board is responsible for setting the strategy and policy expectations for effective data governance and ensuring adequate resourcing.

HNC's Board has appointed the CEO to provide oversight and strategic direction of the development of a data governance strategy and management.

6.2 Data Sponsor

The Data Sponsor is responsible for the strategic direction and who undertakes duties of ownership on behalf of the organisation. Within HNC, this role is filled by the CEO.

The key accountabilities of the Data Sponsor include:

- Endorsing data governance policies and procedures
- Ensuring the resourcing and implementation of data governance
- Reporting data governance and data-related matters to the Board
- Establishing the basis for a Data Set
- Enabling the strategic management, governance, and operation of a Data Set
- Providing direction and guidance, and authorising appropriate resources for management of a Data Set
- Ensuring that the HNC Data Governance Framework incorporates that Data Set
- Authorising any public release of data, after the appropriate privacy impact assessment has been undertaken
- Ensuring compliance with all relevant legislation, policies and standards
- Appointing Data Custodians and ensuring the Data Custodian's duties are fulfilled

6.3 Data Governance Committee

The Data Governance Committee is responsible for setting the strategic direction and making recommendations relating to data governance and data-related matters, including data governance policies, procedures, initiatives and projects.

The key accountabilities of the Committee include:

- Compliance with relevant legislation, regulations and standards
- Clear roles and responsibilities in relation to data management
- Confidence in the quality and integrity of Healthy North Coast's data assets
- Efficient systems for collecting, storing and validating data
- Standard analytic and mapping tools
- Monitoring emerging technologies and data sharing initiatives
- Protection of data through documented policies and procedures, and ongoing communication, education and monitoring
- Risks are identified and mitigated including those associated with compliance, security, access, privacy, continuity, management and cost
- Meaningful interpretation and reporting of data.

6.4 Privacy Officer

The Privacy Officer is the first point of contact for advice to staff on privacy matters. The role is performed by the Director, Corporate Services.

The key accountabilities of HNC's Privacy Officer include:

- Ensuring privacy related policies and procedures are reviewed, communicated and kept-up-to-date
- Providing leadership for privacy compliance
- Collaborating with HNC's Director Digital Health and Marketing to ensure alignment between security and privacy compliance programs including policies, practices, and investigations

- Leading the response team in the event of a data breach; reporting to the Data Sponsor and (if deemed necessary) notifying the OAIC
- Having strong understanding of privacy dispute resolution and complaint-handling methods and processes

6.5 Data Custodians

Data Custodians are responsible for day-to-day management and oversight of a Data Set, approval of access to data and the overall quality and security of a Data Set.

Data Custodians are currently specific to each data set as referenced in HNC's Data Asset Register (DAR).

The key accountabilities of the Data Custodian include:

- Establishing a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the data
- Establishing and maintaining an acceptable level of data protection to ensure privacy, security and confidentiality of information
- Ensuring the data asset has metadata, including a data dictionary, business rules and guide to use
- Ensuring any use of the data aligns with the purpose for which it was collected
- Controlling access to data in compliance with all relevant legislation, policies and standards, and any conditions specified by the Data Sponsor
- Ensuring processes are in place to provide feedback to data suppliers about data quality including issues requiring rectification
- Escalating material risks and issues to the Data Sponsor
- Notifying the Data Governance Committee secretariat of any new data assets that need to be added to the asset registry or changes to existing data assets
- Appointing Data Stewards and ensuring the Data Steward's duties are fulfilled.
- Regularly reviewing users with access to data and the ongoing need and appropriateness of access.

6.6 Data Steward

Data Stewards are responsible for day-to-day management and operation of a data asset, its completeness and quality. This role will be filled within HNC by Senior Data Analysts.

The key accountabilities of the Data Steward include:

- Managing the data asset in compliance with relevant legislation, policies and standards, and any conditions specified by the Data Sponsor
- Developing and maintaining metadata including a data dictionary, business rules and guide to use
- Co-ordinating stakeholder engagement and input into the business requirements for a data asset
- Maintaining the quality, integrity and safety of the data
- Providing feedback to data suppliers in relation to data quality issues
- Conducting privacy impact assessments

- Escalating material risks and issues to the Data Custodian.

6.7 HNC Staff / Data User

The Data User is the person who uses data to perform work duties. The Data User is responsible for:

- Handling data in accordance with HNC's policies and procedures
- Using data in accordance with purpose for which their use is approved
- Taking reasonable steps to protect any confidential information from inappropriate or unauthorised use, access or disclosure
- Reporting any security incidents or weaknesses to the Data Custodian
- Attending training related to data governance

7. Policies and Procedures

HNC's internal data governance-related policies, guidelines and procedures are designed to ensure compliance with the legal and regulatory environment and to provide staff, especially those with delegated authority as custodians 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 HNC policies and procedures that include:

Data Governance

- HNC Data Governance Committee Terms of Reference
- HNC Data Asset Register

Data Privacy and Data Security

- HNC Privacy Impact Assessment Process
- HNC Laptop and Device Security Policy
- HNC Document Control and Management Policy
- HNC Privacy Policy

Data Breach

- HNC Data Breach Response Plan

Data Sharing

- HNC Data Sharing Agreements

Data Use

- HNC Information Technology User Policy
- HNC Information and Knowledge Management Policy

Data Quality

The following cycle indicates how HNC utilises data as an integral theme within its Quality Management cycle.

HNC Quality Management Cycle

Induction procedures for HNC staff include an overview of the Data Governance Framework, related policies and procedures, and user responsibilities and accountabilities. Staff are made aware of their information security responsibilities and the consequences of breaching confidentiality.

8. Data Management

Data management includes the administrative processes throughout the lifecycle of data – from the creation or acquisition, storage, protection, release and destruction – to ensure the integrity, quality and appropriate access of data. A plan documenting these processes must be developed for each data asset.

8.1 Data Acquisition

HNC 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 HNC's functions or activities.

All new or significantly changed data assets are recorded in HNC's data asset registry. The registry identifies the Data Custodian of each data asset, its storage location, and whether it contains identifiable data.

8.2 Data Storage and Security

HNC stores data on-site and using secured cloud-based storage solutions. HNC's Laptop and Device Security Policy and Document Control and Management IT Infrastructure Policy provides a detailed description of:

Security requirements for internally and externally hosted systems

- Hosting requirements for cloud-based solution data centres
- Data centre backup and restoration requirements
- Administrative access levels to servers
- Proper use of IT systems.
- Security is an important component of maintaining data integrity whereby the appropriate security measures protect data from unauthorised access and alteration or corruption. HNC ensures data integrity through data security by:
- Authorising access to data according to permissions determined by the Data Custodian
- Regularly updating security protection on all devices
- Providing online safety awareness training to staff.

8.3 Data Quality

Data quality management encompasses the activities and processes to optimise and enhance the quality of data held by HNC. Data 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 data users to ensure appropriate caveats are considered.

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

Data custodians are responsible for documenting data quality metrics. Metrics must include the measures of accuracy, completeness, consistency, timeliness, availability and fitness of use.

8.4 Data Access, Use and Analysis

Data Custodians are responsible for approving internal access to and use of datasets of which they have custodianship. In considering approval to access data, the custodian must seek to maintain a balance between allowing appropriate levels of data access to meet work requirements and minimising exposure to risks, such as accidental loss or damage, unauthorised access, malicious misuse, and inadvertent alteration or disclosure.

The core principles of data access and use include:

- **Ethical:** Data Custodians must meet their ethical obligations and consider risks and burdens to individuals the data relates to, informed consent, privacy and whether ethical review is required
- **Need to know:** Data Custodians must ensure users are granted the minimum requirements for data use to undertake their business role or for approved purposes
- **Specific and authorised:** the data must not be used by persons other than the specified authorised persons

- **Approved disclosure:** authorised persons must not disclose data to any other persons without prior approval from the Data Custodian
- **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 as required by the relevant classification
- **Duration of access:** the data must not be kept for longer than approved without additional approval from the Data Custodian.

8.5 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, ensure Data Governance Committee approval has been granted where applicable, and assess privacy and security risks, such as accidental loss or damage, unauthorised access, malicious misuse, and inadvertent alteration or disclosure.

8.6 Data Archiving and Destruction

Archiving and destruction of personally identifiable data under HNC's custody is governed by the *Privacy Act* 1988 (Cth) (*Privacy Act*) and the *Health Records and Information Privacy Act 2002 (NSW).* Records are kept in accordance with the record-keeping obligations that apply to the category of record. For health data relating to clinical services provided, the following data retention rules apply:

- If the data was collected from an individual as an adult, it must be retained for 7 years from the last occasion of service delivered
- If the data was collected from an individual under the age of 18 years, it must be retained until the individual has turned 25 years of age
- If the data is destroyed a record must be made of the name of the individual, the period the service was provided, and the date it was destroyed
- If the data is transferred to another organisation and the data is no longer held by HNC, a record must be made of the name and address of the organisation it was transferred to.

9. Compliance

HNC regularly monitors compliance with its data management and security requirements. The Data Governance Committee reviews its data asset and risk registries at each meeting. The Data Governance Committee also regularly reports progress against its workplan and the organisation's compliance with data governance arrangements to the Chief Executive and Board.

9.1 Data Breaches

In the event that a data breach occurs, HNC has a data breach response plan to ensure it can act swiftly to mitigate risk and prevent recurrence. The procedure includes the notification of a data breach if it is likely to result in serious harm to an individual as required under the Notifiable Data Breaches scheme.

10. Supporting Information

Related Information	
Legislation, Standard and/or Government Directive	Privacy Act 1988 (Cth) Australian Privacy Principles Privacy Amendment (Notifiable Data Breaches) Act 2017 Health Records and Information Privacy Act 2002 Freedom of Information Act 1982 Australian Secure Cloud Strategy RACGP Computer and Security Standards Practice Incentives Program Eligible Data Set Data Governance Framework Framework to guide the secondary use of My Health Record system data. ISO/IEC 27001 Information Security Management standard
Forms & Templates	Privacy Impact Assessment Register Data Sharing Agreements Register Data Sharing Agreement
Supporting Documents / Resources	Governance Framework Code of Conduct Policy IT Security Policy Laptop and Device Security Policy Document Control and Management Policy Privacy Policy Information Technology User Policy Information and Knowledge Management Policy Privacy Impact Assessment Procedure Data Breach Response Plan