Guideline

NSW Health Data Governance Framework

Summary	The NSW Health Data Governance Framework outlines the roles and responsibilties involved in data governance and the structures to be put in place to ensure effective and consistent management of the data assets of NSW Health.

Document type	Guideline
Document number	GL2019_002
Publication date	14 March 2019
Author branch	System Information and Analytics
Branch contact	(02) 9461 7307
Review date	14 March 2025
Policy manual	Not applicable
File number	H19/13472
Status	Review
Functional group	Clinical/Patient Services - Information and Data Corporate Administration - Governance, Information and Data
Applies to	Ministry of Health, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, Affiliated Health Organisations, NSW Health Pathology, Public Health System Support Division, Cancer Institute, NSW Ambulance Service, Public Hospitals
Distributed to	Ministry of Health, Public Health System, NSW Ambulance Service
Audience	Data Sponsor, Data Custodian, Data Stewards, Performance Staff, Data Collection Managers

NSW HEALTH DATA GOVERNANCE FRAMEWORK

PURPOSE

The NSW Health Data Governance Framework outlines the roles and responsibilities involved in data governance and the structures in place to ensure effective and consistent management of the data assets of NSW Health.

Effective data governance builds organisational capital, strengthens governance structures and ensures NSW Health data is managed, used and protected in line with legal and community expectations.

The Framework facilitates data quality and comprehensiveness, appropriate access to data, information security, and standardisation of concepts.

KEY PRINCIPLES

The Framework stipulates the accountabilities of all staff, contractors and other persons who, in the course of their work, contribute to or have access to a NSW Health state-wide data asset. These accountabilities extend to establishment and justification for data assets, preparation and publication of all metadata, as well as exhaustive processes for the maintenance and disclosure of data from all NSW Health state-wide data assets.

These accountabilities apply to staff in the Ministry, as well as in all Districts and Networks, Pillars and any contracted agencies with access to NSW Health state-wide data assets.

A data asset is within the scope of this Framework if it meets all of the following criteria:
- Holds all relevant information from across NSW Health entities
- Is made up of patient, staff, workforce, organisation, student or financial information
- Is mandated either by law or a policy recognised by NSW Health.

The Framework also provides the 'Principles of Data Governance for NSW Health' that support the structured and consistent management of data assets and outlines the essential components of data governance, including description of the roles of Data Sponsor, Data Custodian and Data Steward.

The authority of the NSW Health Data Governance Framework is subject to compliance with relevant statutes, regulations and policies, including the NSW Health Code of Conduct.

The Framework should be made available to all staff and contractors to whom it applies.

USE OF THE GUIDELINE

The key responsibilities of NSW Ministry of Health, Pillars and eHealth NSW are to:

- Provide data sponsorship, custodianship and stewardship of state wide data assets
- Ensure alignment of data and IT governance
- Manage IT architecture, data architecture, infrastructure and security
- Work with Data Sponsors and Data Custodians to align data and IT governance
- Ensure information system developments consider downstream impacts on state wide data assets
- Provide data governance advice and education
- Establish data governance policies and procedures
- Ensure relevant delegations are in place to permit release of data in strict compliance with all relevant legislation, policies and standards

The key responsibilities of Local Health District / Specialty Health Network Data Sources are to:
- Ensure compliance with all relevant legislation, policies and standards relating to data collection and supply
- Provide a timely response to any issues and matters raised by the Data Custodian or Data Steward
- Ensure that data is assessed and managed in line with data standards
- Inform Data Sponsors/Custodians of any local issues that will have an impact on data quality and integrity
- Provide data governance advice and education
- Designate a data asset co-ordinator or primary contact to liaise with the Data Custodian or Data Steward in relation to the data asset
- Establish local data governance processes, in compliance with relevant legislation, policies, standards and the NSW Health Data Governance Framework

It is the responsibility of all data users to:
- Ensure that data is recorded or collected according to data standards
- Report data errors and quality issues in a timely manner
- Ensure data security and privacy are maintained whenever data is accessed
- Ensure login details are kept confidential and are only used by the designated user
- Report any breach or suspected breach of data security or privacy
- Sign an acknowledgement of their obligations to protect data privacy
- Ensure compliance with all relevant legislation, policies and standards, including the NSW Health Code of Conduct
- Obtain approval from Data Sponsor or delegated authority for public release of data
- Abide by all terms and conditions associated with approval for access to data.

REVISION HISTORY

Version	Approved by	Amendment notes
GL2019_002	Deputy Secretary, System Purchasing and Performance	The DGF Framework is considered mandatory for all state-wide data collections and is considered best practice for development of data collection governance. Determined that a

		guideline instead of a policy directive was the best method of release for this document type.

ATTACHMENTS

1. NSW Health Data Governance Framework

NSW Health Data Governance Framework

Contents

1. Introduction

1.1 Data Governance for NSW Health

Data Governance describes how data related decisions are made within NSW Health; it refers to the organisational roles, decision rights, and accountabilities of people and systems as they perform information related activities.

1.2 Scope

The NSW Data Governance Framework (the Framework) applies to state wide data assets that support the delivery of high quality safe patient care, enable timely response to population health issues, and promote the prevention and control of disease.

A state wide data asset is a data collection, data stream, or dataset, held by a NSW Health entity; including the Ministry of Health, Local Health Districts, Specialty Health Networks, Shared Services, Agencies and Pillars. A state wide data asset may be made up of patient, staff, workforce, organisation, student or financial information collected from all relevant health services. The data is likely to originate from various sources and its collection is mandatory by law or policy. Linked datasets and value-added copies of other state wide data assets are considered separate data assets for the purposes of data governance.

The Framework applies to all staff, contractors and other persons who, in the course of their work, contribute to or have access to a NSW Health state wide data asset.

A data asset is within the scope of this Framework if it meets all of the following criteria:

- Holds all relevant information from across NSW Health entities

- Is made up of patient, staff, workforce, organisation, student or financial information

- Is mandated either by law or a policy recognised by NSW Health.

Data collections, data streams or datasets that do not meet the definition of a state wide data asset are not strictly governed by the NSW Health Data Governance Framework, however it does represent a best practice approach and should be adhered to wherever possible.

A list of state wide data assets can be found on the System Information and Analytics (SIA) Intranet.

1.3 About the Framework

Data is one of NSW Health's most important strategic assets. Health data, including that obtained as a by-product of clinical care is critical to the ability of the health system to manage, monitor, improve and fund the services it delivers.

Effective data governance is essential in making available authoritative information about the NSW Health system and ensuring compliance with legal and regulatory obligations in acquiring, handling, storing and releasing data. The NSW Health Data Governance Framework outlines the roles and responsibilities involved in data governance and the structures in place to ensure effective management of NSW Health's data assets.

This Framework directly supports the Ministry of Health in its role as system manager, as well as other health entities in their roles within the health system. Data governance is a foundational enabler of the NSW Analytics Framework. NSW Health entities that contribute to the design, specification, collection, reporting and storage of data are critical to the Data Governance Framework's utility and effectiveness.

1.4 Data Governance Concepts

There is a distinction between the related concepts of data governance, data management and IT governance. Alignment of each of these concepts supports NSW Health in achieving its strategic objectives and effectively developing and utilising data resources.

• **Data governance** designates the source of authority for making decisions about data; the roles/structures authorised to make decisions; and the basis upon which decisions are made.

• **Data management** is the planning, execution and oversight of policies and processes that acquire, store, protect, and deliver data and information assets.

• **Information Technology governance** describes processes that ensure the effective and efficient use of Information Technology in enabling an organisation to achieve its goals.

1.5 Compliance

The authority of the NSW Health Data Governance Framework is subject to compliance with relevant statutes, regulations and policies, including the NSW Health Code of Conduct.

Obligations regarding data governance arise from State and Commonwealth statutes including:

• *Government Information* (Public Access) *Act 2009* (NSW)

• *Health Records and Information Privacy Act 2002* (NSW)

• *Health Administration Act 1982* (NSW)

• *Higher Education Support Act 2003* (Cth)

• *Higher Education Standards Framework* (Threshold Standards) *2015* (Cth)

• *Mental Health Act 2007* (NSW)

• *Privacy Act 1988* (Cth)

• *Privacy and Personal Information Protection Act 1998* (NSW)

• *Public Health Act 2010* (NSW)

• *State Records Act 1998* (NSW)

NSW Health also has common law obligations in relation to information obtained as part of the treating relationship.

Data governance roles specified in this document are also subject to the:

• NSW Health Combined Administrative Financial Staff Delegations Manual

• Health System Support Group Delegations Manual

• HealthShare NSW Delegations Manual

• Health Infrastructure Delegations Manual

• District, Network or Pillar Delegations manual

• Public Health Act Delegations Manual

2. Benefits of Data Governance

Effective data governance builds organisational capital, strengthens governance structures and ensures NSW Health data is managed, used and protected in line with legal and community expectations.

The Framework facilitates data quality and comprehensiveness, appropriate access to data, information security, and standardisation of concepts.

The NSW Data Governance Framework will enable NSW Health to achieve the following:

- Clarity on roles, responsibilities and accountabilities relating to data governance

- Clear articulation of data governance processes and structures

- Alignment between data governance and information technology governance

- Production of better quality, more standardised, better understood and better utilised data assets

- Assurance of data security and privacy

- Appropriate access to data

- Efficiency of data management

- Responsible financial stewardship

3. Principles of Data Management for NSW Health

NSW Health has adapted the NSW Information Management Framework to provide principles that support the structured and consistent management of data assets. These are outlined in Figure 1 below:

Figure 1: Principles of Data Management for NSW Health

Governance Principles

- Management of information in keeping with strategic, operational and administrative value to NSW Health, in a transparent and accountable manner
- Demonstration to NSW Parliament and the people of NSW that information held by the Government is appropriately protected and handled
- Compliance with relevant legislation, regulations, cabinet conventions, policies and contractual obligations dictating how information is made available, safeguarded and/or lawfully used
- Clear identification of data governance roles

Collection Principles

- Documentation and facilitation of delivery of health services and the functions of the Ministry of Health as system manager
- Minimisation of collection burden, adhering to the principal of 'collect once and use multiple times'
- Respect for the privacy of NSW citizens and the confidentiality of NSW Health services
- Compliance with agreed standards so the data is fit for purpose, reliable, and can be, where appropriate, re-used to improve service delivery or management reporting

Organisation Principles

- Management of data repositories so there is a single source of truth, and data is easy to find, access, use and share
- Compliance with published metadata including data dictionary, business rules and guide for use

Security Principles

- Protection of the integrity of data and against unauthorised access, alteration, loss or deletion
- Application of controlled and auditable processes that demonstrate protection of sensitive data and information

Principles of Use

- Support for planning, decision making, resource allocation, reporting and communication at all levels of the health system
- Process and analysis by NSW Health agencies to develop evidence-based policy, deliver targeted services to NSW citizens and assess the performance of the health service
- Publishing of reports to ensure the highest standards of public accountability and transparency in the health system
- Use and re-use of information, to derive maximum benefit from investment

Sharing Principles

- Provision of access to NSW Health personnel with a legitimate purpose to access the information
- Respect for the privacy of NSW citizens and the confidentiality of NSW Health services
- Compliance with all relevant state and commonwealth legislation, the NSW Health delegations manual, and any other relevant statutory delegations

Maintenance Principles

- Availability and reliability of information
- Assurance that information collected and held by NSW Health remains current and fit for purpose

4. Essential Components of Data Governance for NSW Health

NSW Health Data Governance is driven and informed by the key components represented in Figure 2.

Figure 2: Data Governance Components diagram

4.1 Structure and Accountability

4.1.1 NSW Data Governance Structure

Each state wide data asset must have an identified and articulated data governance structure that is consistent with the NSW Health Data Governance Framework and the NSW Health Delegations Manual.

This structure should address business-as-usual management and escalation pathways.

The diagram below illustrates NSW Health's overarching data governance structure

Figure 3: NSW Data Governance Structure
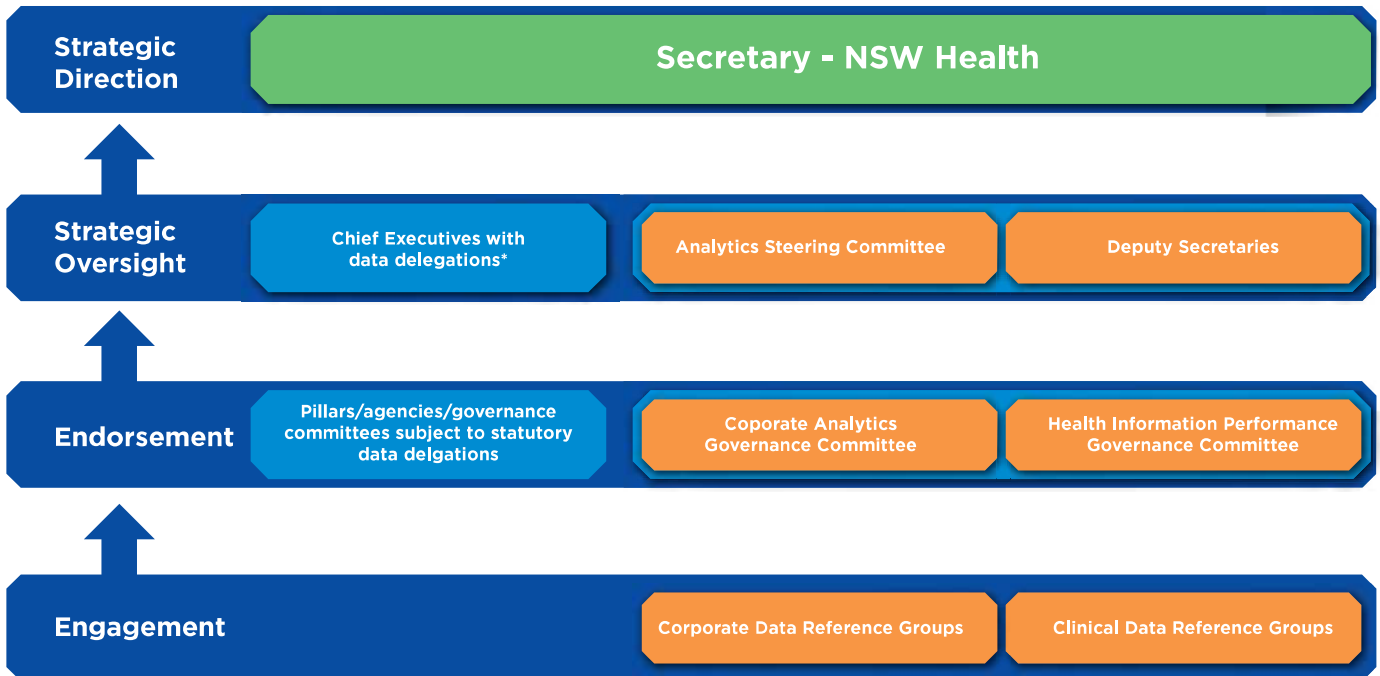
*Includes responsibility regarding the management, use, or release of data specified in a delegations manual listed at section 1.5 of this document.

4.1.2 Governance within data assets

Figure 4: Example Governance Structure for a data asset

4.2 Data Governance Roles

Clarity of roles and responsibilities ensures efficient and effective use of resources in managing the data asset. It ensures standardisation of data and reduction of unnecessary effort in data acquisition, maintenance and distribution.

Each state wide data asset must have a designated Data Sponsor, Data Custodian and Data Steward. For each data asset the contributing agencies should identify a Data Custodian and Data Steward.
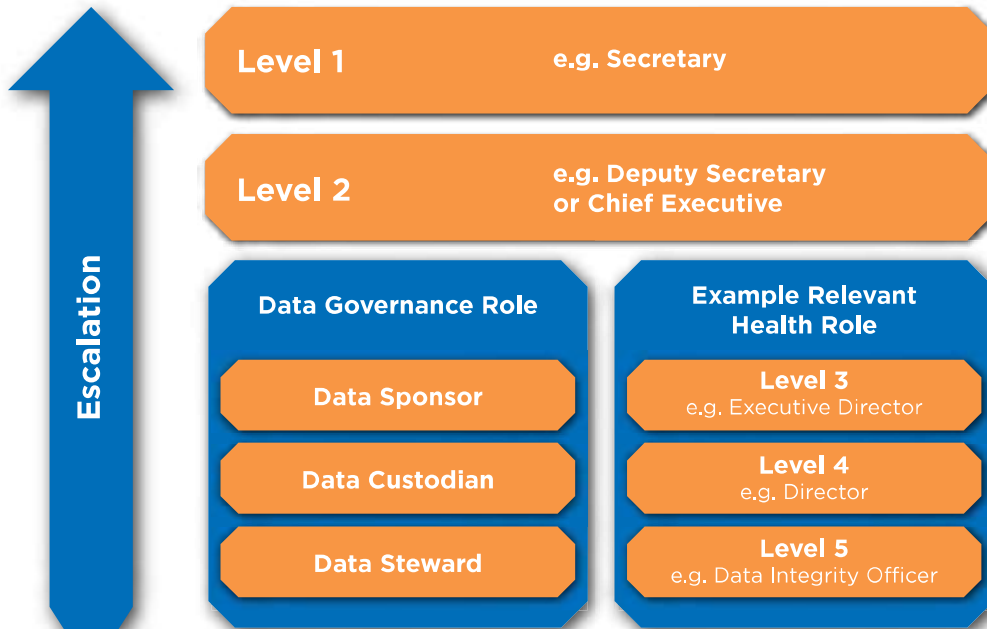
4.2.1 Data Sponsor

Data Sponsors are generally high level executives with control over strategic direction, who undertake duties of ownership on behalf of the organisation.

The key accountabilities of the Data Sponsor are to:

- Establish the basis for the asset

- Enable strategic management, governance and operation of the asset

- Provide direction and guidance, and authorise appropriate resources for management of the asset

- Implement a data governance framework for the asset

- Authorise any public release of information, except where this authority is delegated by the Combined NSW Health Delegations Manual

- Ensure compliance with all relevant legislation, policies and standards

- Appoint a Data Custodian and ensure the Data Custodian's duties are fulfilled.

4.2.2 Data Custodian

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

The key accountabilities of the Data Custodian are to:

- Ensure that:
    - there is a published policy directive and/or information bulletins outlining the purpose of the asset
    - the asset has published metadata, including a data dictionary, business rules and guide for use
    - any use of the data aligns with the purpose for which it was collected
    - there are up-to-date technical documents for the supply and storage of the data
    - the asset remains relevant to system and business needs

- Control access to data in compliance with all relevant legislation, policies and standards, and any conditions specified by the Data Sponsor

- Regularly review users with access to data and the ongoing need and appropriateness of access

- Establish a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the data

- Work with eHealth to align data and IT governance for the asset

- Ensure processes are in place to provide feedback to data suppliers about data quality including issues requiring rectification

- Establish and maintain an acceptable level of data protection to ensure privacy, security and confidentiality of information

- Ensure there is a documented process for responding to breaches and potential breaches of data security

- Ensure there is a documented process for responding to breaches and potential breaches of the data asset's policies and procedures

- Provide advice and direction on the technologies used in data management business functions

- Ensure ongoing development, maintenance and review of data assets

- Advise on the use of the information contained within the asset

- Appoint a Data Steward

- Escalate material risks and issues to Data Sponsor.

4.2.3 Data Steward

Data Stewards are responsible for the day to day management and operation of the data asset, its completeness and quality.

The key accountabilities of the Data Steward are to:

- Manage the data asset in compliance with relevant legislation, policies and standards, and any conditions specified by the data sponsor

- Develop and issue a policy directive and/or information bulletins for the asset

- Ensure there are up-to-date technical documents for the supply and storage of the data

- Work with stakeholders to develop and maintain metadata including a data dictionary, business rules and guide for use

- Co-ordinate stakeholder engagement and input into the business requirements for the data asset

- Provide advice to Data Custodian and Data Sponsor on the management of the asset as required

- Provide feedback to data suppliers in relation to data quality issues

- Convene a stakeholder working group to help manage the asset

- Maintain a work plan for the asset, aligned with NSW Health's strategic direction

- Escalate material risks and issues to Data Custodian.

4.2.4 Data Asset Working Groups

Data collection working groups are stakeholder forums convened to assist the Data Custodian and Data Steward to manage the data asset.

The key accountabilities of a working group are to:

- Provide opportunities for stakeholder engagement

- Provide advice to the Data Steward in relation to data asset policies and procedures

- Review proposals for modifications to the asset and provide advice

- Progress work plan items that support the objectives and strategic direction set out by the Data Sponsor and Data Custodian

- Advise on local collection, reporting, information system and data quality issues

- Escalate material risks and issues to relevant Data Governance Committee.

4.3 Accountability and Responsibilities

4.3.1 NSW Ministry of Health, Pillars and eHealth NSW

The key responsibilities of NSW Ministry of Health, Pillars and eHealth NSW are to:

- Provide data sponsorship, custodianship and stewardship of state wide data assets

- Ensure alignment of data and IT governance

- Manage IT architecture, data architecture, infrastructure and security

- Work with Data Sponsors and Data Custodians to align data and IT governance

- Ensure information system developments consider downstream impacts on state wide data assets

- Provide data governance advice and education

- Establish data governance policies and procedures

- Ensure relevant delegations are in place to permit release of data in strict compliance with all relevant legislation, policies and standards.

4.3.2 Local Health District and Specialty Health Network Data Sources

The key responsibilities of Local Health District/Specialty Health Network Data Sources are to:

- Ensure compliance with all relevant legislation, policies and standards relating to data collection and supply

- Provide a timely response to any issues and matters raised by the Data Custodian or Data Steward

- Ensure that data is assessed and managed in line with data standards

- Inform Data Sponsors and Custodians of any local issues that will have an impact on data quality and integrity

- Provide data governance advice and education

- Designate a data asset co-ordinator or primary contact to liaise with the Data Custodian or Data Steward in relation to the data asset

- Establish local data governance processes, in compliance with relevant legislation, policies, standards and the NSW Health Data Governance Framework.

4.3.3 Data Users

Although Data Custodians play a central role in the management of data assets, all personnel have a responsibility to maintain and protect the privacy, quality and efficacy of data.

It is the responsibility of all data users to:

- Ensure that data is recorded or collected according to data standards

- Report data errors and quality issues in a timely manner

- Ensure data security and privacy are maintained whenever data is accessed

- Ensure login details are kept confidential and are only used by the designated user

- Report any breach or suspected breach of data security or privacy

- Sign an acknowledgement of their obligations to protect data privacy

- Ensure compliance with all relevant legislation, policies and standards, including the NSW Health Code of Conduct

- Obtain approval from Data Sponsor or delegated authority for public release of data

- Abide by all terms and conditions associated with approval for access to data.

4.4 Critical Enablers

4.4.1 People

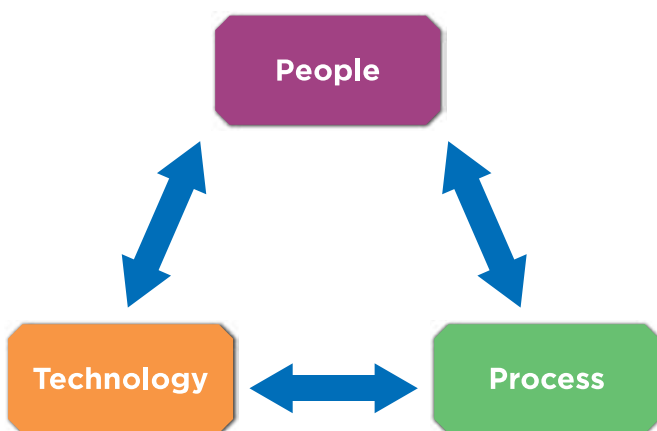Each state wide data asset must have:

- A data sponsor, data custodian and data steward

- A stakeholder working group with representation from the principal data suppliers

- A data asset co-ordinator or primary contact within the principal agencies supplying data

- Data and information system support and development personnel.

Collaborative relationships between the above are essential to effective data governance.

4.4.2 Processes

Each state wide data asset must have in place:

- A documented governance structure to support the collection, organisation, storage, security, use, sharing and maintenance of data

- Processes for developing and updating metadata

- Documented and readily accessible processes for securing, accessing and releasing data

- Documented data quality standards and strategies.

4.4.3 Technology

Each state wide data asset must be supported by information communication technology (ICT) infrastructure and platforms that facilitate efficient data capture, data quality validations, transfer and secure storage. Appropriate analytic tools, technologies and services must support access to data and information for management, monitoring and improving NSW Health services. Each ICT upgrade or new system must maintain data asset integrity and quality and also consider opportunities to improve data assets and governance.

4.5 Central Components

4.5.1 Standards

To support the consistency and meaningfulness of data, each state-wide data asset must:

- Have a published policy directive and/or information bulletins outlining:

    - the purpose of asset;

    - the people processes and technologies which support the asset;

    - the data standards and governance arrangements in place to manage the data

- Have published metadata including a data dictionary, business rules and guide for use

- Have protocols for the use and disclosure of information

- Have up-to-date technical documents for the supply and storage of the data

- Comply with all relevant state and commonwealth legislation, the NSW Health Combined Delegations Manual, and any other relevant statutory delegations.

4.5.2 Access

Use and disclosure of data must be in compliance with all relevant state and commonwealth legislation, the NSW Health Combined Delegations Manual or Public Health Act Delegations Manual, the NSW Health Code of Conduct, and any other relevant statutory delegations.

Approval for the disclosure of unit record data must, at a minimum, comply with: PD2015_037: Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services; PD2018_001: Disclosure of Unit Record Data held by Local Health Districts for Research or Contractor Services and the NSW Health Combined Delegations Manual

In making a decision to provide access to data, the Data Custodian, Data Sponsor, Deputy Secretary, Chief Executive or other role as specified by the relevant delegations manual must consider:

- The purpose for which the data is to be used

- The level of data requested in relation to the use case provided

- The level of identification appropriate to the purpose i.e. identified, de-identified, or aggregate data

- The need for further assessment by an accredited Ethics Committee, such as the NSW Population Health Services Research Ethics Committee

- The applicant's understanding of privacy, confidentiality, security and appropriateness of use

Access to data, within NSW Health, for the purpose of health service planning, management and improvement can be approved by the Data Custodian.

4.5.3 Disclosure of Data

Disclosure of data must be compliant with the Health Privacy Principles outlines in the Health Records and Information Privacy Act (2002). In part, these principles outline that health information may only be disclosed for the purpose for which it was collected unless:

• The individual to whom the information relates has consented

• The individual would reasonably expect the organisation to disclose the information

• The disclosure of the information is reasonably believed to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or a serious threat to public health or public safety

• Disclosure of the information is reasonably necessary for the funding, management, planning or evaluation of health services

• Disclosure of the information is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest.

The NSW combined delegations' manual provides advice in relation to approval for disclosure of data.

There must be a legal basis for disclosure of unit record data. If there is uncertainty as to the legal basis for disclosure, the request should be referred to the Ministry's Legal and Regulatory Services Branch.

4.5.4 Transmission and storage of electronic data

Unit record data must be transferred using encryption technologies approved by the Data Custodian, such as Secure File Transfer, and stored by the recipient in a secure fashion at all times. Acceptable secure storage includes storage on physically secure file servers or in files that use strong encryption software. Storage on portable media, laptops and desktop computer hard-drives is not acceptable.

4.5.5 Security

Each state wide data asset must have in place processes to protect the privacy and confidentiality of data through access management and security controls. It is the responsibility of the Data Custodian to ensure that the necessary penetration testing and other security assessment is undertaken to guarantee that the data is appropriately secured, backed up and disposed of according to agreed and documented protocols. Alignment of data and IT governance must enforce regulatory, architectural and security compliance requirements.

4.5.6 Data Quality

Data must be fit for the purpose(s) it is intended. Data custodians are responsible for ensuring each data asset has defined data quality standards. Data quality strategies must address the accuracy, completeness, timeliness, relevance, consistency and reliability of data.

Data quality may be facilitated by:

• Publication of metadata including a data dictionary, business rules and guide for use

• Regular communication with stakeholders regarding changes to the data asset

• Regular assessment of data quality and communication of results to stakeholders

• Timely advice to data suppliers in relation to data quality and rectification actions required.

5. Creating, modifying or retiring a state wide data asset

A data asset can be created, modified or retired by the Deputy Secretary/Chief Executive with responsibility for the strategic or policy area to which the data applies.

5.1 Creating a new state wide data asset

The approval process for creating a new state wide data asset comprises five stages; development of business case, pilot testing, decision to proceed, implementation plan, and implementation. A state wide data asset that arises as a by-product of an ICT or data project must undergo the same approval process.

5.1.1 Development of business case

The business case should identify the strategic or policy requirement for the creation of the asset. It should outline the potential benefits to the health system, the projected costs and resource requirements and operational impact. In this stage, Data Sponsors, Custodians and Stewards must be identified and a working group identified or established as required. Appendix 1 outlines the criteria for selecting an appropriate Data Custodian.

5.1.2 Pilot testing

The pilot should confirm that the data meets the strategic or policy requirement and allow for the refinement and validation of requirements, metadata, supporting resources, and data management processes. The pilot should test the business and technical processes supporting the data asset, include appropriate project planning, and involve relevant ICT stakeholders. Evaluation of the pilot should assess the efficiency of business and technical components.

5.1.3 Decision to proceed

At the conclusion of the pilot, the Data Sponsor and other relevant stakeholders must make a decision as to whether to proceed to implementation.

5.1.4 Implementation plan

The project plan should give a detailed explanation of the roles and responsibilities, ongoing resources, processes for collection, reporting, storage and access to data, and the chain of custody. It should include:

• Development of metadata, including a data dictionary, business rules and guide for use.

• Development of ICT solutions.

• Engagement with eHealth and other relevant ICT stakeholders.

5.1.5 Implementation

To implement a new data asset, the following must be completed:

• The publication of metadata, including a data dictionary, business rules and guide for use.

• Approval and execution of any necessary amendments to the combined NSW Delegations Manual.

The final step in the implementation stage is to complete the transition to a business-as-usual data governance model, in compliance with this framework.

| Development of Business Case | Pilot Testing | Decision to Proceed | Implementation Plan | Implemenation |

5.2 Modifying a state wide data asset

On occasion it will be necessary to modify a NSW Health data asset. This may occur in response to changes in clinical care, service delivery, community or policy priority, or system management imperatives.

A proposal to modify a state wide data asset should include

- Identification of a strategic or policy requirement for change

- Consultation with stakeholders (including Data Steward, Source System Advisory Groups, eHealth and relevant ICT personnel) to develop and specify the change and likely impact

- Development of an implementation plan considering the projected impact, any necessary changes to metadata, delegations, governance of the asset, and increase or redeployment of resources

- Endorsement of change request/business case from the relevant governance committees (e.g. HIPGC)

- Approval from Data Custodian, Data Sponsor, Deputy Secretary or Chief Executive as relevant to the nature of the change

- Publication of updated metadata including a data dictionary, business rules and guide for use, and communication of changes to relevant stakeholders.

5.3 Retiring a state wide data asset

The retirement of a state wide data asset must be approved by the Data Sponsor and Deputy Secretary/ Chief Executive with responsibility for the data asset.

A proposal to retire a state wide data asset should include:

- Strategic and policy rationale for retirement, including why the asset is no longer required and outline of alternative data sources if required

- Consultation with stakeholders (including data users) to consider the impact

- Plans for continued storage and maintenance or disposal of existing data

- Re-deployment of asset resources as required

- Plans for repeal or amendment of any relevant asset-specific delegations

- Formal rescission of relevant governance instruments and communicate to all data users.

6. References

1. Data Governance – in-brief (Australian Institute of Health and Welfare)
2. Data Governance Policy (October 2015) – Cancer Institute NSW
3. Disclosure of unit record data by Local Health Districts for research or contractor services (PD2018_001)
4. eHealth Governance Framework Policy Directive (2015) – Government of South Australia
5. eHealth Strategy for NSW Health 2016-2026
6. Electronic Information Security Policy – NSW Health (PD2013_033)
7. Health Information and Performance Governance Committee (HIPGC) Terms of Reference and Business Rules (January 2016)
8. Health Infrastructure Delegations Manual
9. Health System Support Group Delegations Manual
10. HealthShare NSW Delegations Manual
11. Information Management Framework
12. Information Security Management System ISMS Incident Management and Actions Procedure (HS 2013_07)
13. NSW Government Digital Information Security Policy V2.0 (April 2015)
14. NSW Health Analytics Framework (January 2016)
15. NSW Health Combined Administrative Financial Staff Delegations Manual
16. Privacy manual for Health Information (March 2015)
17. The Data Management Association Guide to The Data Management Body of Knowledge (DAMA_DMBOK Guide). First Edition
18. The DGI Data Governance Framework – The Data Governance Institute

6.1 Legislation

1. *Government Information (Public Access) Act 2009 (NSW)*
2. *Health Administration Act 1982 (NSW)*
3. *Health Records and Information Privacy Act 2002 (NSW)*
4. *Higher Education Standards Framework (Threshold Standards) 2015 (Cth)*
5. *Higher Education Support Act 2003 (Cth)*
6. *Mental Health Act 2007 (NSW)*
7. *Privacy Act 1988 (Cth)*
8. *Privacy and Personal Information Protection Act 1998 (NSW)*
9. *Public Health Act 2010 (NSW)*
10. *State Records Act 1998 (NSW)*

Appendix 1

Criteria for selecting a Data Custodian for the asset

The *2013 NSW Data & Information Custodianship Policy* outlines the criteria for selecting a custodian. The Data Custodian should be a role within a branch, pillar or agency that:

• Has responsibility for the capture and maintenance of the data/information;

• Has the greatest operational need for the data/information;

• Is the first to record changes to the data/information;

• Is the most competent to capture and/or maintain the data/information;

• Is in the best economic position to justify the collection of the data/information at source;

• Requires the highest integrity and accuracy of the data/information; and/or

• Is able to meet the responsibilities of custodianship.

In agreeing to provide custodianship, an agency needs to take into account the roles and responsibilities of custodianship, and whether it is appropriate for the agency to take on these responsibilities. If it cannot meet these requirements, or finds that meeting these requirements unreasonably constrains its operations, the agency should consider relinquishing its custodianship to another agency.

Transfer of custodianship

The *2013 NSW Data & Information Custodianship Policy* outlines the following process for transfer of custodianship:

In the interests of maintaining completeness in the information holdings within NSW, the party relinquishing its custodianship has the responsibility of working with another agency to take on the role of custodian.

A custodial agency wishing to relinquish its custodial responsibilities for a nominated dataset needs agreement by all relevant parties involved, including the other agency that is prepared to assume custodianship duties. Documentation, licences, records and databases may need amendment to reflect the new custodial arrangements. All parties affected by the changes should be notified, and any issues relating to data and information management – including any transfer of funding – will need to be addressed at an agency level.