

Neonatal Intensive and Special Care Units' Data Registry governance and management framework

**Integrated Digital Enablement Accelerator
Stream**

November 2025

The information in this resource should not replace a clinician's professional judgement.

The Agency for Clinical Innovation (ACI) works with clinicians, consumers and system leaders to improve the health system in NSW. We design and implement new ways to deliver care for patients.

The ACI partners with the Ministry of Health, pillar organisations, local health districts, specialty networks, clinicians, patients and carers. We work together to achieve better value in healthcare by:

- improving patient and provider experience
- improving patient outcomes
- delivering efficient and sustainable healthcare services.

The ACI is part of the Clinical Innovation and Research Division and works closely with the Office for Health and Medical Research.

aci.health.nsw.gov.au

AGENCY FOR CLINICAL INNOVATION

1 Reserve Road St Leonards NSW 2065
Locked Bag 2030, St Leonards NSW 1590
Phone +61 2 9464 4666
Email aci-info@health.nsw.gov.au | aci.health.nsw.gov.au

Further copies of this publication can be obtained from the Agency for Clinical Innovation website at aci.health.nsw.gov.au

Disclaimer: Content within this publication was accurate at the time of publication.

© State of New South Wales (Agency for Clinical Innovation) Year. Creative Commons Attribution-No Derivatives 4.0 licence. For current information go to aci.health.nsw.gov.au. The ACI logo is excluded from the Creative Commons licence and may only be used with express permission.

Title	Neonatal Intensive and Special Care Units' Data Registry governance and management framework		
Replaces	February 2025. Neonatal Intensive and Special Care Units' Data Registry governance and management framework		
Revised	November 2025. Updated links to data request form from NICUS to ACI form.		
Next review	2029		
Produced by	Integrated Digital Enablement Accelerator Stream		
Preferred citation	NSW Agency for Clinical Innovation. Neonatal Intensive and Special Care Units' Data Registry governance and management framework. Sydney: ACI; 2025.		
CM ACI/D23/3961	SHPN (ACI) 250754	ISBN 978-1-74231-228-6	ACI_12125 [10/25]

Contents

Introduction	4
Background	4
Objective	4
Purpose	5
Scope	5
Audience	5
Review of the Framework	6
Data governance context	6
Data governance concepts	6
Related NSW Health policy and supporting documents	6
Legislation	7
Policy directives and guidelines	7
Supporting documents	7
NICUS strategic governance	8
Guiding principles of the Framework	8
Purpose and uses of NICUS data	8
Data governance model for data held in NICUS	12
Data governance supporting roles	17
Parent and legal guardian control of data in NICUS	22
Access to NICUS	23
Use and disclosure of NICUS data	25
Protecting the privacy of individuals	26
Fit for purpose	27
Risk mitigation strategies	27
Effective governance	28
References	29
Appendix 1: Roles and responsibilities in applying the framework	30
Glossary	33

Introduction

Background

The Neonatal Intensive and Special Care Units' Data Registry (NICUS) was established in 1986, initially as a clinical research dataset, expanding the scope over time to become a data registry. NICUS prospectively collects maternal and infant data on all liveborn babies in NSW and the ACT who are admitted to a contributing Level 3, 4, 5 or 6 neonatal service in a public hospital in NSW within the first 28 days after livebirth. NICUS also collects follow-up data on a subset of eligible surviving children to school age. The primary purpose of NICUS is to collect clinical quality data on demographics, treatments and outcomes of newborn infants who receive care in a neonatal intensive and/or special care after birth in NSW and any agreed contributing jurisdictions, such as the ACT.

The governance of NICUS moved to the Agency for Clinical Innovation (ACI) in September 2021, to become one of the clinical quality registries managed by ACI.

NICUS has four core datasets.

- NICUS Clinical Dataset, which collects maternal and infant data on all newborn patients admitted to an intensive or special care unit in NSW and/or the ACT to document and follow up a newborn patient's clinical progress.
- NICUS Surgical Dataset, which collects clinical data on eligible infants who undergo surgery in the first 28 days after livebirth.
- NICUS 2-3-year Follow-up Dataset, which collects prospective neurodevelopmental assessment data from eligible surviving children at 2-3 years of corrected age and a medical assessment of eligible survivors.
- NICUS Five-year Follow-up Dataset, which collects prospective neurodevelopmental assessment data from eligible surviving children at five years of corrected age and a medical assessment of eligible survivors.

Objective

The focus of Neonatal Intensive and Special Care Units' Data Registry Governance and Management Framework (the Framework) is to establish the effective governance and management of NICUS data as an important strategic asset for the NSW health system. The Framework aims to answer the following key questions:

- What is the intended use of NICUS data?
- How will NICUS data be governed?
- What are the primary roles and who is accountable?
- What policies and procedures apply?

Purpose

The purpose of the Framework is to:

- outline the principles and arrangements for the NSW health system to ensure effective management and governance of the data held by NICUS. The Framework provides the stakeholders of NICUS data with an instrument to govern NICUS data assets effectively through the exercise of authority and control (planning, guiding and monitoring) over the management of these assets
- guide and direct all NICUS research related data requests through a streamlined process for the Centralised Data Custodian to make an informed decision to approve and release NICUS data.

The Framework has been developed in alignment with NSW Health Data Governance Framework, policy directives and is supported by the **ACI Data Request Form** and the NICUS Research Data Applications: a guide for researchers.

Additionally, the Framework defines the processes that acquire, control, protect, deliver and enhance the value of NICUS data as an important strategic asset for the NSW health system.

Detailed and high-quality data are vital for clinical quality activities, clinical operations, evidence-based clinical decision-making and future policy development and research.

Scope

The Framework:

- applies to all data held within NICUS
- establishes the guidelines in relation to data-related activities and functions in the governance and management of NICUS data, including the decisions on creating, modifying, retiring and business-as-usual management of data held in NICUS
- focuses on the roles and responsibilities of NSW Health entities in the management and governance of NICUS data, with recognition of the proposed role and responsibilities of clinicians, researchers and external organisations that use NICUS data.

This Framework does not apply to NICUS data included in NSW clinical or public health registries, such as e-Maternity and the Perinatal Data Collection. These assets are subject to their own data governance and management frameworks.

Audience

This document contains key information for all parties involved in the governance and management of NICUS data; particularly those who have delegated authority to make data-related decisions. It is also an important source of information for NSW Health, including local health districts, specialty health networks, pillars, Ministry of Health and agencies that provide data to, or receive data from, NICUS. This also includes stakeholders, end users and application support services of NICUS.

Review of the Framework

The Framework will be subject to regular review. This review will consider:

- the capacity and capability of NSW Health entities to meet the responsibilities of the data governance roles
- the role of NICUS in supporting non-tertiary special care nurseries
- any changes to the governance structure for NICUS within NSW Health.

Data governance context

Data governance concepts

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

- Data governance designates the source of authority for making decisions about data; the roles and/or 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 assets.
- IT governance describes processes that ensure the effective and efficient use of IT in enabling an organisation to achieve its goals.

Alignment of each of these concepts supports the NSW health system in achieving its strategic objectives and effectively developing and using data resources.

Related NSW Health policy and supporting documents

This Framework is compliant with relevant statutes, regulations and policies. It stipulates how the management and governance of NICUS data are handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law and how the project fits into community expectations.

Obligations regarding data governance arise from State and Commonwealth statutes including those listed below.

Legislation

- **Government Information (Public Access) Act 2009 (NSW)**
- **Health Administration Act 1982 (NSW)**
- **Health Records and Information Privacy Act 2002 (NSW)**
- **National Health and Medical Research Council Act 1992**
- **Privacy Act 1988 (Commonwealth)**
- **Privacy and Personal Information Protection Act 1998 (NSW)**
- **State Records Act 1988 (NSW)**

Policy directives and guidelines

- **Guideline GL2019_002 NSW Health Data Governance Framework**
- **NSW Health Combined Delegations Manual**
- **Policy Directive PD2015_037 Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services**
- **Policy Directive PD2018_001 Disclosure of unit record data by Local Health Districts for research or contractor services**
- **Policy Directive PD2023_040 Data Breaches Involving Personal or Health Information**
- **Statutory Guidelines on Research, Health Records and Information Privacy Act 2002 (NSW)**

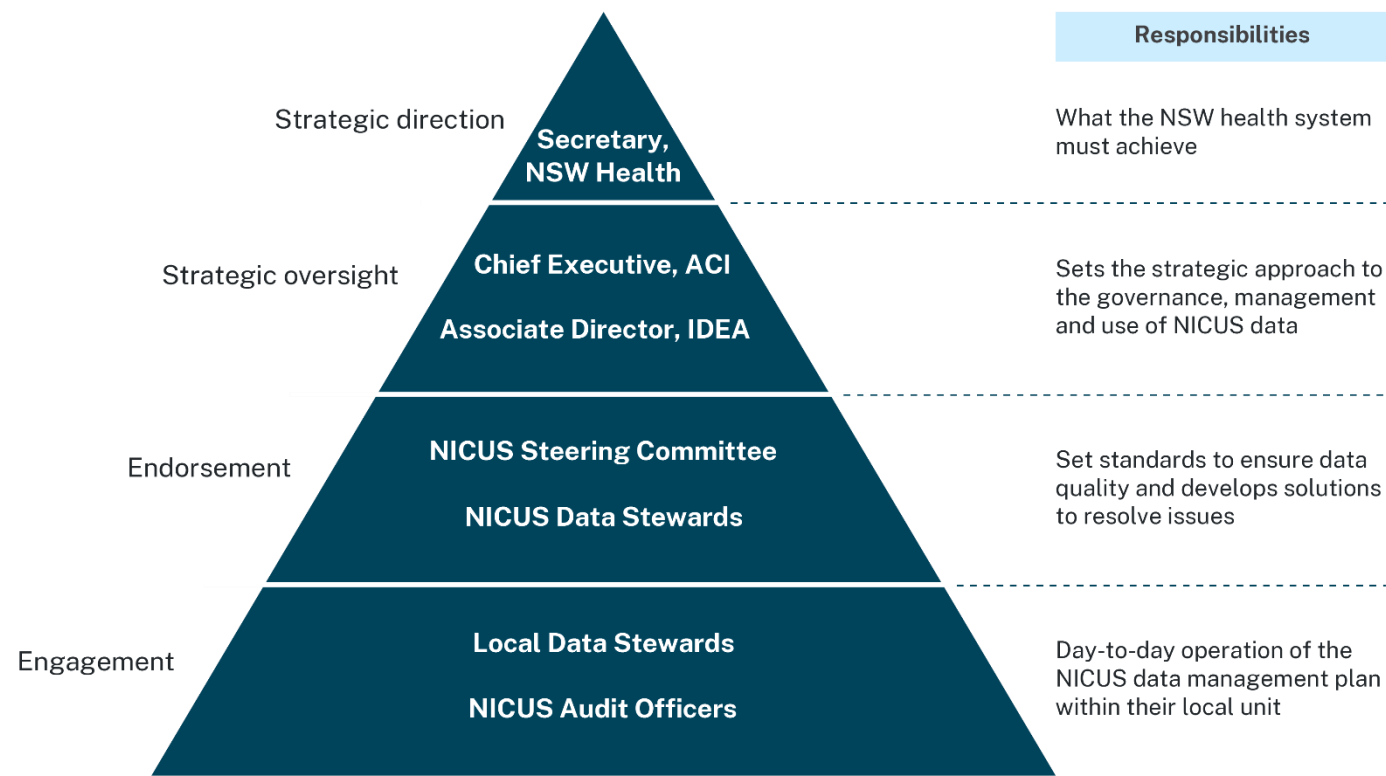
Supporting documents

- **Guideline GL2022_002 Maternity and Neonatal Service Capability**
- **Health Stats NSW - Privacy Issues and the Reporting of Small Numbers 2015**
- **Management of Data and Information in Research: a guide supporting the Australian code for the Responsible Conduct of Research 2019**
- **National Statement on Ethical Conduct in Human Research 2023**
- **The Australian Code for the Responsible Conduct of Research, 2018**

NICUS strategic governance

The strategic governance structure, with clearly defined roles and responsibilities, identifies the governance and working group that is accountable for achieving the strategic goals for NICUS within the NSW health system.

Figure 1: NICUS strategic model



Guiding principles of the Framework

Purpose and uses of NICUS data

Purpose

The primary purpose of NICUS is to collect clinical quality data on demographics, treatments and outcomes of newborn infants who receive care in a neonatal intensive and/or special care after birth in NSW and in agreed contributing jurisdictions.

Uses

Uses of NICUS data include quality improvement, research, health services planning, reports to the Ministry of Health and data submissions for national reporting by the Australian and New Zealand Neonatal Network (ANZNN). The ANZNN is considered a separate data asset and is subject to its own data governance and management processes.

Opportunities exist for secondary use or re-use of linked NICUS data for the purposes of funding, management, planning or evaluation of health services (dependent on the legal basis for linkage), including:

- measurement and monitoring of the impact of treatments for diseases and conditions
- measurement and monitoring of the impact of health services
- planning of health programs, or treatments or services
- evaluation of health programs, or treatments or services.

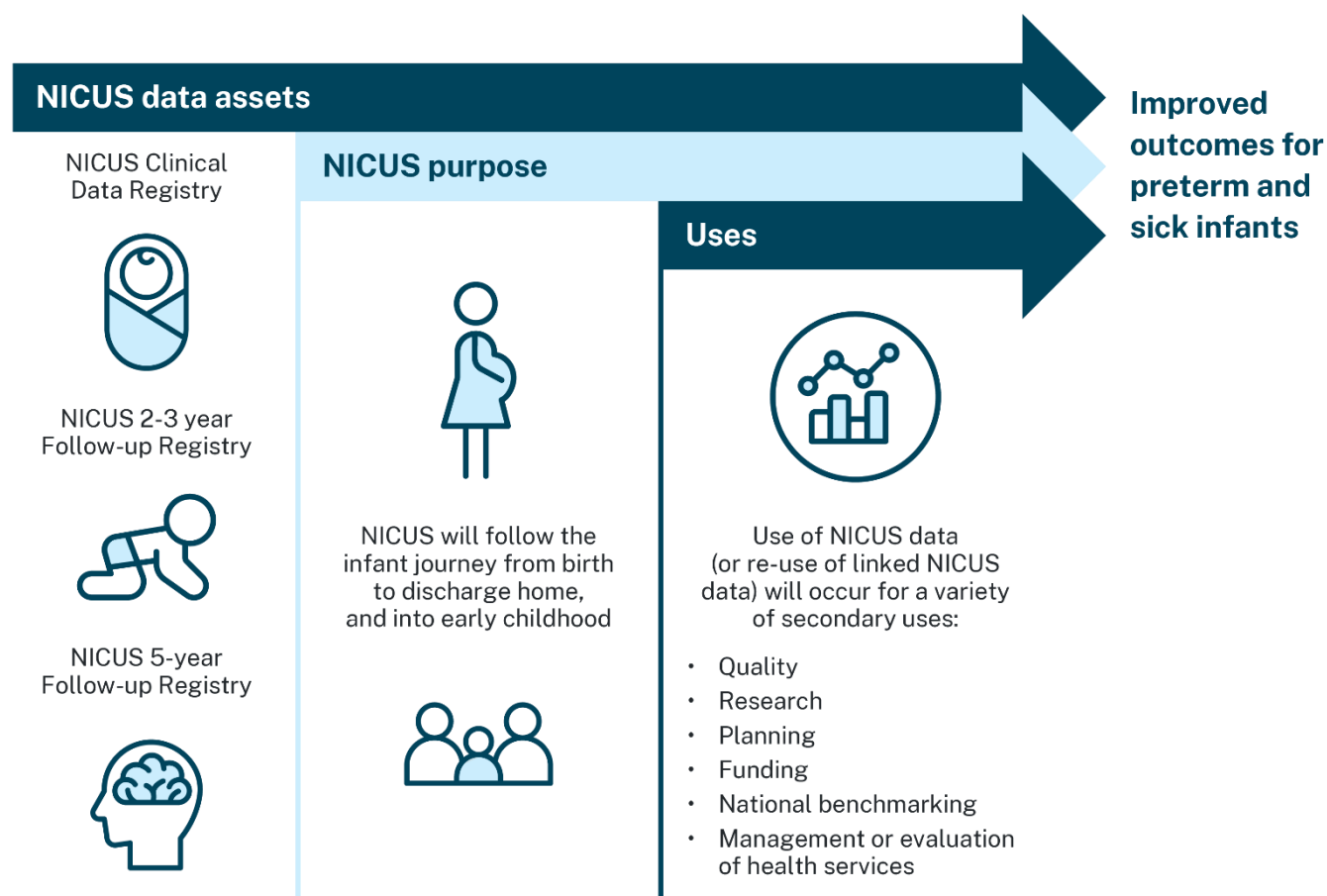
For NICUS data to be used for a secondary purpose (other than the primary purpose it was collected), there must be a legal basis for the use and disclosure of the data. Health Privacy Principle 10 and 11 of the Health Records and Information Privacy Act 2002 (NSW) state the legal basis for the use or disclosure of NICUS data. This includes but is not limited to:

- **Consent.** The need for 'opt-out' consent from an infant's parent or legal guardian whom the NICUS data relates to for the use or disclosure of NICUS data.
- **Direct relation.** The secondary purpose being directly related to the primary purpose of NICUS data.
- **Management of health services.** The use or disclosure of NICUS data for the secondary purpose is reasonably necessary for the funding, management, planning, quality improvement or evaluation of health services.
- **Training.** The use of NICUS data for the secondary purpose is reasonably necessary for the training of employees of the NSW Health entity.
- **Research.** The use or disclosure of NICUS data for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest consistent with existing processes for the use of any health data for research purposes.¹

The following information about secondary uses is provided as guidance only. Any decision to use NICUS data for a secondary purpose must be in accordance with the Privacy Manual for Health Information, Health Records and Information Privacy Act 2002 and its statutory guidelines, and the NSW Health Combined Delegations Manual. If there is uncertainty as to the legal basis for the use and disclosure of data, the Ministry of Health's Legal and Regulatory Service branch should be consulted.

NICUS data holdings and intended use

NICUS has four key datasets: the NICUS Clinical Dataset, the NICUS 2-3-year Follow-up Dataset, and the NICUS Five-year Follow-up Dataset. Data are collected for the purpose and uses outlined in Figure 2.

Figure 2: NICUS data assets and their intended purposes

Secondary uses that are permitted

Permitted secondary uses of NICUS data include some that are considered directly related to the primary purpose, such as quality assurance. While others can be more remote, for instance management of health services and research with data linkage from other datasets.

NSW Health entities may use and disclose NICUS data for any secondary purpose if an infant's parents or legal guardian have not opted-out of having data collected by NICUS. NICUS data can be used or disclosed without consent when there is a directly related secondary purpose that is within the reasonable expectations of the infant's parents or legal guardian.

Permitted secondary uses that fall within a directly related purpose to the primary purpose include but may not be limited to:

- disclosing NICUS information to the infant's nominated paediatrician, other treating health services or medical specialists involved in the care and treatment of an infant
- sending reminders to a parent or legal guardian so they can complete an outcome questionnaire before presenting to a health service for follow up care and treatment
- improving existing health services, for example to evaluating the healthcare in terms of clinical effectiveness and impact of intervention and care over time

- using information for quality assurance or clinical audit activities carried out by the health service. For instance, monitoring, evaluating, auditing the provision of a particular service the health service has or is providing to the infant
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating, auditing the provision of a particular clinical service the health service has provided, or is providing, to the infant. Disclosing such information is only permissible if the individual reviewing the health records is bound by privacy legislation.

Secondary uses that fall outside a directly related purpose and are related to the management of health services, training and research that are permitted include but may not be limited to:

- provision of data for linkage for agreed purposes, e.g. those purposes specified in the Public Health Act or research
- development of clinical decision support systems to influence treatment choices at point of care
- evaluation of health interventions and/or health programs, e.g. determine if an intervention or service is generating outcomes or benefits consistent with investment decisions
- quality improvement in healthcare service delivery, e.g. to better enable benchmarking between services and interventions for continuous quality improvement
- health services research relevant to public health, e.g. aggregated NICUS data used for evaluation and research to understand patient needs, preferences and adherence or impact of treatment and care
- construction of registries, e.g. create or supplement data in registries, such as those established under the provisions of the Public Health Act, for example other clinical quality registries or other existing registries
- development or enablement of technology innovations, e.g. new software applications that support clinicians' decision-making for interventions aimed to improve infant outcomes
- development of health policy, e.g. establish and evaluate policies to benefit whole populations
- preparation of publications, e.g. educate on the appropriateness and value of established health care services.

Secondary uses that are not permitted

Secondary uses that are not permitted include but may not be limited to:

- remuneration of individual clinicians, e.g. to make or modify payments.

Data governance model for data held in NICUS

Data governance roles are consistent with the NSW Health Data Governance Framework.

Figure 3: NICUS data governance model

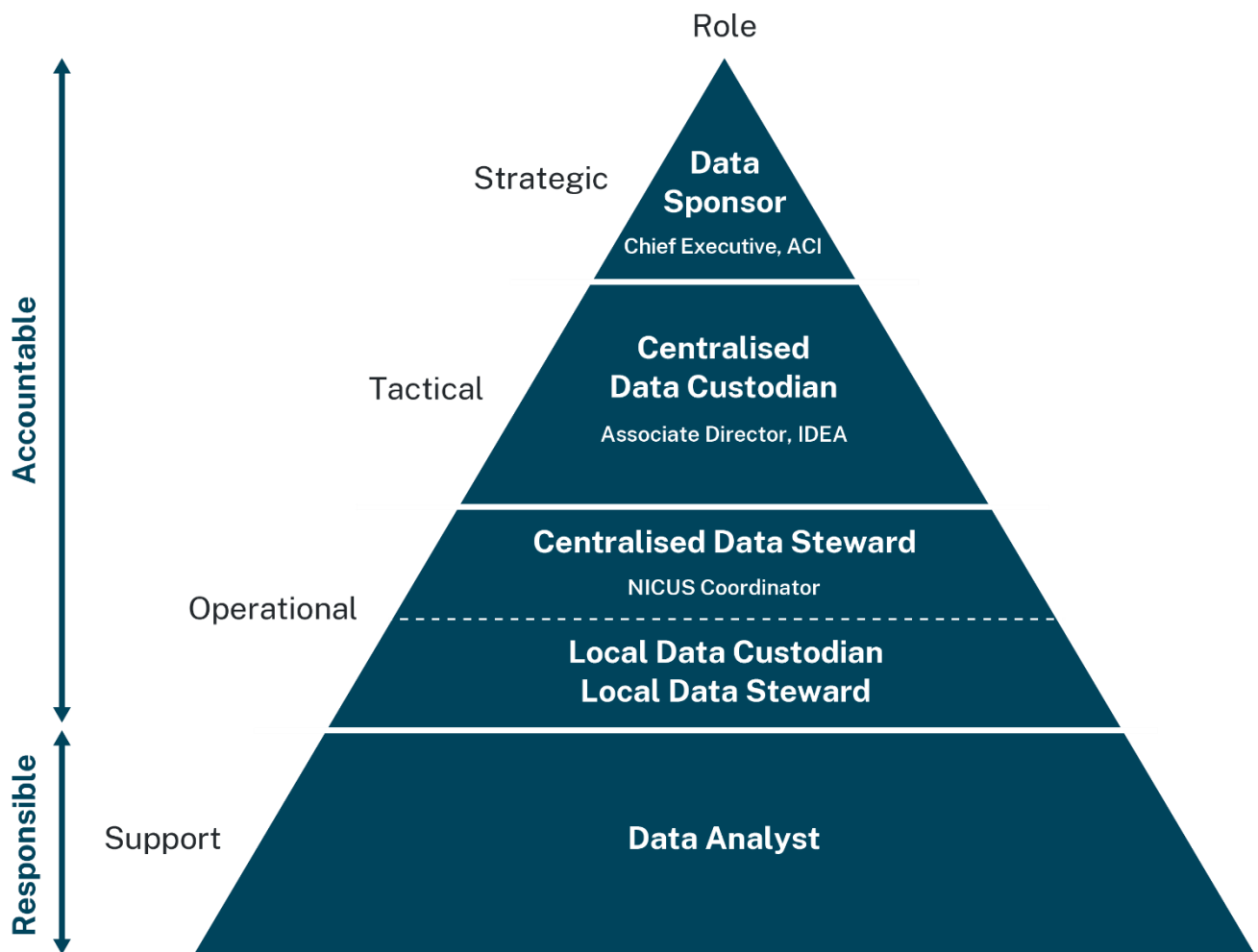


Table 1: Data governance roles held in NICUS

Role	Responsible party	Key responsibilities
Data Sponsor	Deputy Secretary, Clinical Innovation and Research and Chief Executive, ACI	Controls the strategic direction of NICUS. Responsible for overseeing the continuous improvement of NICUS data governance and management.

Centralised Data Custodian	Associate Director, IDEA stream	Approval of access to the NICUS dataset. Overall responsibility for quality and security of NICUS data.
Centralised Data Steward	NICUS Coordinator	Day-to-day management and operation of the NICUS data, its completeness and quality. Ensuring that the collection, use, sharing and release of NICUS data is performed according to policies and practices as established by the Framework.
Local Data Custodian	LHD and SHN Chief Executives (or their nominated delegate)	Day-to-day management and oversight of the NICUS data asset. Approval of access to local unit NICUS data. Responsible for quality and security of local unit NICUS data.
Local Data Steward	Appointed by the Local Data Custodian	Oversee day-to-day management of local NICUS data, its completeness and quality. Responsible for maintaining and protecting privacy of local data.
Data Analyst	NICUS Business Analyst	Day-to-day management and operation of the NICUS database and its security and updates.

Accountability responsibilities

The key roles and responsibilities for governing the collection, use, sharing, security and maintenance of data held within NICUS are summarised below.

Data Sponsor

The Data Sponsor controls the strategic direction of NICUS and has full accountability on behalf of the NSW health system. The Data Sponsor champions the importance of NICUS and associated information management and is responsible for overseeing the continuous improvement of NICUS data governance and management.

Key accountabilities

- Establish the basis for the NICUS data asset held by NICUS
- Enable strategic management, governance and operation of the NICUS data
- Provide direction and guidance and authorise appropriate resources for management of NICUS data
- Implement the NICUS Data Governance and Management Framework for the NICUS data
- 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 Data Custodians and ensure the Data Custodians' duties are fulfilled

- Have legal rights and control all NICUS data and information assets captured, stored, generated and approved for release for primary and secondary uses, including research

Responsible party

- Deputy Secretary, Clinical Innovation and Research and Chief Executive, ACI

Contact when:

- New or changes in policy or legislation are proposed
- Compliance issues arise
- Resourcing approval is required for strategic or operational purposes

Centralised Data Custodian

The Centralised Data Custodian has operational responsibilities of day-to-day oversight of NICUS data, approval of access to NICUS data, approval of access to data and the overall quality and security of the data.

Key accountabilities

- Ensure that any use of the NICUS data aligns with the purpose for which it was collected
- Ensure there are up-to-date technical documents explaining the supply and storage of NICUS data
- Ensure NICUS data remains relevant to system and business needs
- Ensure the value of NICUS data is maximised through sharing
- Control access to data in compliance with all relevant legislation, policies and standards and any conditions specified by the Data Sponsor
- Consider requests for the secondary use of NICUS data, approve or deny these requests and specify what data are available for secondary use
- Classify and approve the use of NICUS data to Data Users based upon the appropriateness of the user's role and the intended use (refer to NICUS roles)
- Regularly undertake a user access review ensuring only legitimate users have access to NICUS data
- Establish and maintain an acceptable level of protection to ensure privacy, security and confidentiality of NICUS data
- Ensure there is a documented process for responding to breaches and potential breaches of data security, or that it is embedded in the data assets policies and procedures
- Approve new functionality within the NICUS data registry
- Approve all NICUS multi-site data requests for the purpose of approved research projects, audit or quality improvement activities. The Centralised Data Custodian will be supported with advice from the Centralised Data Steward and the NICUS Research Committee.

Responsible party:

- Associate Director, IDEA stream, ACI.

Contact when:

- Scope of the NICUS business model requires significant review

- Issues arise concerning data policy, privacy compliance and security.

Local Data Custodian

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

Key accountabilities:

- Control local (LHD or SHN) access to data generated by relevant LHD or SHN entity in compliance with all relevant legislation, policies and standards and any conditions specified by the Data Sponsor
- Approve the use of unit level NICUS data to Data Users, in the local neonatal unit based upon the appropriateness of the user's role and the intended use
- Regularly review local users with access to data and the ongoing need and appropriateness of access
- Establish and maintain a local acceptable level of data protection to ensure privacy, security and confidentiality of information
- Ensure there is local policy for responding to breaches and potential breaches of data security
- Appoint a local Data Steward
- Escalate material risks and issues to Centralised Data Custodian and/or Data Sponsor

Responsible party

- LHD or SHN Chief Executive

Contact when:

- Local operational needs arise
- Local issues arise concerning data policy, privacy compliance and security

Centralised Data Steward

The Centralised Data Steward is an inclusive role that accepts one or more negotiated stewardship activities on behalf of the Centralised or Local Data Custodians. The Centralised Data Steward has the operational or technical ability to collect, deliver or maintain NICUS data.

Note: A Data Custodian cannot transfer accountability to the Centralised Data Steward, although a Data Steward may be responsible for specific activities.

Key accountabilities

- Manage the NICUS data in compliance with relevant legislation, policies and standards and any conditions specified by the Data Sponsor and Centralised Data Custodian
- Ensure all Data Users are appropriately trained and are aware of their obligations in the protection of NICUS data
- Provide advice to Data Custodians and the Data Sponsor on the management of NICUS data as required

- Establish a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the data held within NICUS
- Ensure processes are in place to provide feedback to local Data Custodians, local Data Stewards, and local NICUS Audit Officers about data quality, including issues requiring rectification
- Provide feedback to local Data Custodians, Local Data Stewards and local NICUS Audit Officers in relation to data quality issues
- Work with stakeholders to develop and maintain metadata, including data dictionary, business rules and guide for use of NICUS data for research
- Coordinate stakeholder engagement and input into NICUS and research data requests
- Monitor and report on NICUS data-related projects
- Assist in developing new policy directives, standards and/or information communication for NICUS
- Provide consultation for researchers seeking feasibility of requesting data for research projects
- Evaluate the feasibility of data related requests in collaboration with the NICUS Business Analyst
- Assist researchers throughout the application, approval and data release process to complete all required documentation for the research project
- Act as the key liaison person between researchers, the NICUS Research Committee and the Centralised Data Custodian to facilitate timely assessment and processing of data requests
- Represent ACI on the NICUS Research Committee to assess and prioritise data requests, document objections to data release and communicate these to the Centralised Data Custodian and to identify potential conflicts of interest arising from a data request
- Release data via secure file transfer or a secure access environment as applicable, following approval from the Centralised Data Custodian
- Identify potential or actual data breaches and inform the Centralised Data Custodian and NICUS Research Committee. Potential or actual data breaches must also be reported within 24 hours to the ACI Privacy Officer and Associate Director, IDEA in accordance with the ACI's Interim Procedure, MNDB – December 2023 (Mandatory Notification of Data Breach).

Responsible party

- NICUS Centralised Data Steward

Contact when:

- Operational issues require central escalation
- Data policy, privacy compliance or security issues require escalation
- Multi-site data is requested
- Data management planning or additional data is required to meet business needs

Local Data Stewards

The role of Local Data Stewart for each neonatal unit is appointed by the Local Data Custodian. The local Data Steward undertakes day-to-day operation and implementation of NICUS data management plans within their local healthcare provider organisation, as appointed by Local Data Custodian. They

have detailed knowledge of data structure, content and appropriate use of the information for their areas. They develop and set data management standards approved by the Data Custodian.

Key accountabilities

- Manage and oversee the data held in NICUS to help provide Data Users with high-quality NICUS data that are easily accessible in a consistent manner
- Ensure that all local NICUS Audit Officers and local Data Users are appropriately trained and are aware of their obligations in the protection of NICUS data
- Provide advice to the Local Data Custodian and Central Data Stewards on the management of data held within NICUS as required
- Provide feedback to the local NICUS Audit Officers and local Data Users in relation to data quality issues
- Ensure processes are in place to provide feedback to the local NICUS Audit Officers and local Data Users about data quality, including issues requiring rectification
- Escalate material risks and issues to the Local Data Custodian and Central Data Steward
- Conduct local clinical audit of unit level data

Contact when:

- Data access is required within the scope of their organisation
- Operational, business or data definition issues arise and cannot be resolved, or data errors are perceived
- Further detailed information about their organisation's NICUS data is required
- Local data management planning is required, or additional data may be encompassed within their business scope

Data governance supporting roles

Table 2: Data governance supporting roles

Role	Role fulfilled by
Working Group	The NICUS Business Analyst, Centralised Data Steward and the NICUS Steering Committee members, acting in the role of a Working Group, will engage with key business and technology stakeholders to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.
Privacy Contact Officer	The ACI Privacy Contact Officer is the first point of contact regarding privacy at the ACI. The Privacy Contact Officer will be responsible for providing advice on privacy issues to the NICUS team, helping ensure privacy compliance on the collection, use and sharing of NICUS data.
Security Officer	The NSW Health entity's Security Officer, ensuring security compliance on the collection, use and sharing of NICUS data, will be responsible for providing assurance and advice on security issues.

Data Specialists	The NICUS Business Analyst and NICUS Data Steward and NICUS Coordinator, supported by e-Health, acting in the role of Data Specialists, will provide ongoing support to NICUS through analysis and problem solving of NICUS data related topics.
Data Users	Clinicians, managers or administrators and NICUS Audit Officers who access, input, amend, delete, extract and analyse NICUS data are responsible for the safety, privacy, security and integrity of the NICUS data in their local neonatal unit.
Third Parties	Organisations and individuals requesting access to NICUS data for secondary use purposes are responsible for preparing an access request and committing to participating in the monitoring and assurance arrangements as stipulated by a conditions of use agreement.
System Administrators	The NICUS Business Analyst and eHealth NSW Program Delivery team, acting in the role of System Administrator, will be responsible for the analysis, design, implementation and maintenance of new and changes on existing NICUS data structures, and the storage and operations of data held within NICUS.

Accountability responsibilities

The key roles and responsibilities of data governance supporting roles within NICUS are summarised below.

Working Groups and/or NICUS Business Analyst

Engage with key business and technology stakeholders to make informed decisions on what solutions and standards should be adopted to ensure data quality and resolve issues.

Key accountabilities

- Make decisions on data concepts for NICUS data, for instance the taxonomy and data dictionary
- Make decisions on the data architecture and data sharing standards

Responsible parties

- NICUS Centralised Data Steward
- NICUS Business Analyst
- IDEA stream, ACI
- e-Health NSW
- ACI

Contact when:

- A need for a new business function or new application function is identified

Privacy Officer

Responsible for enterprise-wide approach to privacy and is responsible for providing leadership, assurance and advice on privacy issues.

Responsibilities

- Be the first point of contact regarding privacy at the ACI
- Provide advice on privacy issues to the NICUS team
- Help ensure privacy compliance on the collection, use and sharing of NICUS data
- Engage with the Office of the Privacy Commissioner and clients
- Support strategic and operational privacy activities
- Establish and promote the organisation's privacy policies, in alignment with NSW policies and standards

Responsible parties

- Privacy Contact Officer, ACI

Contact when:

- Privacy compliance issues arise
- Suspected or actual data breaches occur
- NICUS changes may have privacy impacts
- Information management policy amendments or new policies are required

Security Officer

Responsible for enterprise-wide approach to security and for providing leadership, assurance and advice on security issues.

Responsibilities

- Set the vision for security across the organisation
- Ensure security compliance with the strategic direction of NSW government
- Ensure strategic and operational plans for security are developed
- Establish and promote the organisation's security policies, in alignment with national and state policies and standards

Responsible parties

- NSW Health entity Security Officer and ACI Security Officer

Contact when:

- Security compliance issues arise
- NICUS changes have potential security impacts
- Information management policy amendments or new policy is required

Data Specialists

The Data Specialists are the business and technical subject matter experts responsible for providing ongoing support through analysis and problem solving NICUS data related topics, including data design, data relationships, data quality and data modelling. Data Specialists have access to and make sense of information contained, albeit hidden, in the organisation, as delegated by the Centralised Data Custodian.

Responsibilities

- Understand high-level requirements of the business and provide solutions related to business strategies
- Translate business and technical jargon to understandable language for different audiences
- Create NICUS data entry dashboards
- Identify data quality issues and implementing application fixes
- Assist local Audit Officers and Data Users in their requirements
- Promote comprehensive NICUS data use within the NSW Health system

Responsible parties

- NICUS Business Analyst
- ACI data and information managers assigned the role of ACI administrator

Contact when:

- Insight is needed for changed or new strategies to meet business outcomes for NICUS

Audit Officers and Data Users

Audit Officers and Data Users are local clinicians, managers or administrators in each neonatal unit who access, input, amend, extract and analyse local NICUS (unit specific) data held by NICUS. Appropriate security and approval are required from the NICUS Data Steward to maintain the quality and integrity of NICUS data.

Any Audit Officer or local Data User that has access to NICUS data, is also entrusted with the protection of that data.

Responsibilities

- Ensure that NICUS data are 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
- Abide by all terms and conditions associated with approval for access to NICUS data

Responsible party

- NSW Health entity local NICUS Audit Officers or healthcare professional and support staff acting in the role of Clinician, or Audit Officer or Clerk
- NSW Health entity data analysts

Contact when:

- Local neonatal unit-level data-related queries are required
- Local neonatal unit-level support is required through analysis and problem solving NICUS data related topics

Third Parties

A Third Party is an organisation or individual requesting access to NICUS data for secondary use purposes, including research requests. The Third Party is responsible for preparing an access request and committing to participating in the monitoring and assurance arrangements as stipulated by a conditions of use agreement.

Responsibilities

- Obtain approval from Local or Centralised Data Custodian for access to NICUS data by preparing a NICUS research data request application requesting access to NICUS data and supporting the risk assessment of the request for the secondary use of NICUS data. Local Data Custodians can approve requests for local unit level data. The Centralised Data Custodian approves requests for NICUS data from more than one LHD or statewide data.
- Sign an acknowledgement of their obligations to protect data privacy (where access to NICUS data for secondary use as been approved) as part of a conditions of use agreement
- Abide by all conditions of use associated with approval for access to NICUS data
- Ensure data security and privacy are maintained whenever NICUS data are accessed and analysed
- Report any breach or suspected breach of data security or privacy

Responsible party

- Clinicians and researchers requesting to use NICUS data for research purposes

System Administrators

System Administrators are responsible for the analysis, design and implementation of new and changes to existing data and information structures and applications. They are also responsible for administration and backup. They plan, coordinate and implement security measures and manage the performance and efficiency of data storage underpinning NICUS.

Responsibilities

- Ensure alignment of data and IT governance
- Manage IT architecture, data architecture, infrastructure and security
- Accountable for access control and derive the best possible business benefit from the use of underlying technology of the NICUS

- Identify data quality issues and implement application fixes
- Conduct impact analysis and coordinate changes to the NICUS to avoid adverse impacts on NICUS data assets
- Ensure that efficient data structure design and disaster recovery and backup procedures are effectively tested and implemented
- Ensure the transition from test environment to production environment is implemented effectively
- Review physical data structures in consultation with the data or information architect and database developers
- Ensure security administration through monitoring and administering database management system security constraints, such as removing users, administering quotas, auditing and checking for security problems
- Analyse data stored in the database and make recommendations relating to performance and efficiency of that data storage

Responsible party

- NICUS Business Analyst
- eHealth NSW program delivery, application support services

Contact when:

- Physical data models are ready for implementation
- Need for new business functions or new application functions are identified
- Expertise is required to resolve issues related to data management anomalies occurring in the operation, physical data security, disaster recovery or back-up, system migration or platform standards and performance degradation

Parent and legal guardian control of data in NICUS

Conditions of consent

Parents and legal guardians of eligible individual infants are invited to participate in NICUS. Participation in NICUS is subject to agreeing to the conditions of consent, which states the intended primary and secondary use of the maternal and infant data collected by NICUS.

Withdrawal of consent

Parents and legal guardians of eligible infants who have data collected by NICUS will be able to withdraw from NICUS and the use of their data for the primary purpose. Where maternal and infant data have been recorded in NICUS, but consent has subsequently withdrawn, the data held within NICUS will no longer be available for the primary purpose and future secondary uses.

Impact on access to NICUS data

The impact of parents and legal guardians removing consent to participate in NICUS and their NICUS data being used for the primary purpose it was collected include:

- Clinicians and health services that scheduled infant follow-up appointments will no longer be able to access the clinical data collected in NICUS from the infant's primary admission. They will still have access to NICUS data to respond to access notices and court orders.
- Maternal and infant data in NICUS data may continue to be used for secondary purposes where data for projects was requested, collected and approved for release during a period of time when consent had been provided.

Access to NICUS

Conditions of access

NSW Health entities and individual staff members who require access to NICUS in their local unit for the purpose of data entry and data cleaning will need approval from their line manager for a NICUS profile and password. Extraction of local unit NICUS data requires approval from the local Data Custodian.

NSW Health entities and their designated staff who require access to NICUS are required to complete an access application form. These will be stored in the ACI document management system (Content Manager) by the NICUS Data Stewards.

Local Data Stewards will identify the person who will be the Local Audit Officer. The local Data Steward is accountable for the NICUS data held within NICUS in their neonatal unit. The Local Data Custodian can delegate specific data and information roles and responsibilities to individual positions within their organisation related to using NICUS. This includes assigning employees, healthcare professions and healthcare support staff in the roles of Local Data Stewards, Audit Officers and Data Users.

Protection of individuals' privacy

The Local Data Stewards, appointed by Local Data Custodian will ensure that the privacy of individuals is protected.

User roles of NICUS

The roles and responsibilities of NICUS system users are listed in Table 3. It is the responsibility of the Centralised NICUS Data Steward to assign Data Users to a user role in the NICUS system that provides the right level of access to NICUS data and responsibilities over the management of that data.

Table 3: Support roles and responsibilities related to NICUS

User role name	Has a role in	Data governance equivalent role	Roles and responsibilities
NICUS System Administrator	All operational procedures related to IT governance and management of IT architecture, data architecture, infrastructure and security	System administrator	• Upon receipt of approval from the Data Sponsor, establishes the ACI Administrators

			Provides ongoing technical support of NICUS
Local Data Steward	All NICUS data related to their NSW Health entity	Local Data Steward	- Abides by all terms and conditions associated with the conditions of use agreement for access to NICUS data - Must have completed training in privacy and information security - Reports any breach or suspected breach of NICUS data security or privacy
Local Audit Officer	All day-to-day operations and NICUS data management within their healthcare provider organisation	Local Audit Officers Data User	- Assigns, maintains and re-assigns health service roles and permissions - Ensures that all NICUS users are appropriately trained and are aware of their obligations in the protection of NICUS data - Has high level knowledge and expertise in NICUS - Reports any breach or suspected breach of NICUS data security or privacy
NICUS Follow-up Clinicians	NICUS data (developmental and medical assessment results) they input into NICUS	Data User	- Agrees to all terms and conditions associated with the consent to collect NICUS data - Reports any breach or suspected breach of NICUS data security or privacy

Use and disclosure of NICUS data

Secondary use of NICUS data from a local unit

For applications requesting access to local NICUS data, that is, NICUS data managed by the local NSW Health entity, the application should be directed to the local Data Custodian for the requested data held within NICUS. The Local Data Custodian will perform a data risk assessment and an assurance process to assess the request for the secondary use of NICUS data, approve or deny the request and specify in an agreement what NICUS data are available and the conditions of use and data release. The documented conditions of data release will align with the schedule set out in the NSW Health Policy Directive, PD2018_001.

Secondary use of NICUS data from multiple units

For applications requesting access to statewide NICUS data, that is, NICUS data owned by more than one NSW Health entity, the application should be directed to the Centralised NICUS Data Stewards for data held within NICUS. After review of the application by the NICUS Data Stewards (and NICUS Research Committee for research requests), a recommendation will be made to the Centralised NICUS Data Custodian to approve or deny the request. The Centralised Data Custodian will perform a data risk assessment and assurance process to assess the request for the secondary use of NICUS data, approve or deny the request and specify in writing what NICUS data are available and the conditions of use and data release. The documented conditions of data release will align with the schedule set out in the NSW Health Policy Directive, PD2015_037.

Secondary use of NICUS data

Secondary uses of NICUS data include quality improvement, research, health services planning and reporting to the NSW Ministry of Health.

Statewide NICUS data, for example pasteurised donor human milk data, are submitted to the Ministry of Health quarterly. The NICUS Data Stewards are responsible for preparing and sending these data to the Centralised Data Custodian. The Centralised Data Custodian will review and approve the data prior to the Data Steward submitting the report to the Ministry of Health.

NICUS data are also submitted to the ANZNN for national reporting. The ANZNN is considered a separate data asset and is subject to its own data governance and management processes.

Process for approval of NICUS data for secondary use

Several processes are needed to consider, determine, monitor and report on a request to use NICUS data for secondary purposes. The Centralised Data Custodian assessing applications requesting access to NICUS data is responsible for:

- assessing the request based on the intended use of the data
- performing a data risk assessment and assurance process to assess applications to access NICUS data for secondary use

- ensuring that NICUS data that are accessed or released for secondary use have the appropriate security controls in place commensurate with the conditions of use identified from the data risk assessment and assurance process
- putting a set of processes in place to provide assurance to stakeholders and clients that the use of NICUS data is in accordance with the approved primary and secondary purposes.

All initial enquiries regarding access to statewide NICUS data, such as NICUS data managed by more than one NSW Health entity, for purposes other than research are to be submitted in writing to the NICUS Data Stewards via email: aci-nicusregistry@health.nsw.gov.au. These will be reviewed by NICUS Data Stewards and the NICUS Data Custodian who will advise on the feasibility of the data request and will provide essential documentation to progress the process.

Any decisions made on the secondary use and disclosure of NICUS data must be in accordance with the Privacy Manual for Health Information and the Health Records and Information Privacy Act 2002 (NSW). Also, where applicable, the Statutory Guidelines on Research, the NSW Health Combined Delegations Manual, Policy Directive PD2015_037 Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services and Policy Directive PD2018_001, Disclosure of unit record data by local health districts for research or contractor services.

Conditions of data release must align with the schedules established in the policy directives PD2015_037 and PD2018_001.

Appendix 1 provides guidance of the processes, and the roles and responsibilities of the parties involved in requesting and accessing NICUS data for secondary use.

All applications for NICUS data for research requests, including required supportive documentation of ethics approval from a Human Research Ethics Committee are made via the **ACI Data Request Form**. Further information on the process for applying for NICUS data for research is available in the NICUS Research Data Applications: a guide for researchers. An overview of the process from application to approval of release of NICUS data for research is outlined in Appendix 2.

Exclusions

Data used for local clinical audit.

NICUS Audit Officers who conduct clinical audit of their own local unit-level data and report only to their local Data Custodian on non-research related activity.

Protecting the privacy of individuals

Data safety

NSW Health entities are required to meet the Health Privacy Principles as set out in the Health Records and Information Privacy Act 2002 (NSW) with respect to the collection, storage, security, access, use and disclosure of personal information. The Centralised Data Custodian will regularly reconsider the privacy protection processes around primary and secondary use of NICUS data, to maintain an acceptable level of protection to ensure privacy, security and confidentiality of NICUS data. Proven methods should be used to reduce the risk of breaching an individual's privacy to very low levels.

Data storage

NICUS data that are disclosed must always be stored by the recipient Third Party or other systems securely. Acceptable secure storage includes storage on physically secure file servers that are configured in such a way that password protection is universally enforced, or in files that are encrypted by strong encryption software. Storage on portable media, laptops and desktop computer hard drives is not acceptable.

NSW Health recommends and is in the process of implementing procedures supporting the use of **secure access environments** for approved access to data by researchers, consultants and other instances where the data are being disclosed by NSW Health entities.

Fit for purpose

Data quality

Data quality has a direct impact on the Data User. Incomplete or inaccurate data may result in adverse or invalid decisions or findings that have an unexpected or even detrimental impact.

NICUS data must be fit for the primary and secondary uses it is intended. The Centralised Data Custodian and the Centralised Data Steward are responsible for ensuring each NICUS 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 NICUS data asset
- Regular assessment of data quality against each of the intended uses and communication of results to Data Users
- Timely advice to Local Data Custodians, Local Data Stewards Local Audit Officers and Data Users in relation to data quality and rectification actions required
- Regular review and update of the NICUS data dictionaries by the NICUS Steering Committee and the Centralised Data Steward.

Quality assurance

The Centralised Data Steward will put a set of processes in place to provide feedback to local Data Stewards and Audit Officers about data quality including issues requiring rectification.

The Local Data Stewards and Audit Officers will ensure that NICUS data collected are of sufficient quality to support the intended primary and secondary use of the data.

Risk mitigation strategies

Risk of breach

Data breaches may arise from:

- Loss or unauthorised access, modification, use or disclosure or other misuse
- Malicious actions, such as theft or hacking
- Internal errors or failure to follow information handling policies that cause accidental loss or disclosure
- Not adhering to the laws of NSW or the Commonwealth of Australia.

The Centralised Data Custodian and the Centralised Data Steward will ensure that the risk of a breach of privacy for an individual is reduced to an acceptable level by minimising the risks associated with the collection, use, sharing (and release) of NICUS data for primary and secondary purposes. This includes the use of **secure access environments** for the release of, and access to, data in accordance with NSW Health recommendations.

Data security and protection

The maternal and infant data held within NICUS must have processes in place to protect the privacy and confidentiality of data through access management and security controls. It is the responsibility of the Centralised Data Custodian, in consultation with the NICUS Business Manager and/or Data Analyst, to ensure that the necessary penetration testing and other security assessment is undertaken to guarantee that NICUS data are 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.

Risk assessment and assurance process

The Centralised Data Custodian, in consultation with the NICUS Business Analyst, must undertake an appropriate data risk assessment and assurance process to consider, determine, monitor and report on a request to use NICUS data for secondary purposes. The requirement for the Centralised Data Custodian to undertake a data risk assessment and assurance process is to ensure that:

- An assessment of the impact of privacy can be performed; privacy and security concerns are managed through application of this NICUS Data Governance and Management Framework; and that the proposed technology security controls for the storage of NICUS data have been verified using an information security assessment.
- The monitoring and assurance process and conditions of use are defined and clearly understood by all parties.

Effective governance

Framework review

As part of the ongoing practice of effectively managing and governing NICUS data, the Framework will be reviewed every four years or when there are material changes either to either the strategic governance of NICUS or to policies and legislation that impact on data governance.

References

1. Health Records and Information Privacy Act 2002 (NSW)
2. NSW Government. NSW Government Data Strategy: Glossary. Sydney: NSW Government [cited 14 Jan 2025; updated 17 Jul 2024]. Available from: <https://data.nsw.gov.au/nsw-government-data-strategy/glossary>
3. DAMA International. DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition). Technics Publications, LLC; 2017.
4. Australian Bureau of Statistics. Linking and merging of data. Statistical Data Integration. Canberra: ABS [cited 6 Nov 2025]. Available from: <https://statisticaldataintegration.abs.gov.au/project-delivery/linking-and-merging-of-data>

Appendix 1: Roles and responsibilities in applying the framework

Role	Responsibilities
Centralised Data Custodian	The Centralised Data Custodian will apply this Framework in making decisions around approving access to NICUS data for secondary use. The Centralised Data Custodian will also apply this Framework by: • overseeing the NICUS data approval process, including data for research • convening a stakeholder working group or NICUS Research Committee to help manage the data assets.
Centralised Data Steward and NICUS Coordinator	The Centralised Data Steward and NICUS Data Coordinator will apply this Framework in making recommendations to the Centralised Data Custodian around approving access to NICUS data for secondary use. The Centralised Data Steward will also provide guidance to third parties on availability of NICUS data and the feasibility of proposed research studies. The Centralised Data Steward will also apply this Framework when: • providing consultation for data requestors, including researchers • checking all applications submitted to the ACI Data Request Form, including compliance with ethics, approved protocol and data security plan • working with the Centralised Data Custodian to review, approve and release data in a timely manner • working with the NICUS Business Analyst to extract, clean and de-identify data in response to data requests • sending data to requestors following approval of data release by the Centralised Data Custodian • maintaining records of all NICUS data used for research in the ACI Data Request Form.

NICUS Project Support Officer	The NICUS Project Support Officer will apply this Framework when managing NICUS data assets for primary and secondary purposes. The NICUS Project Support Officer will also apply this Framework when: - obtaining data from non-tertiary neonatal units for NICUS registrants in those units - providing consultation for data requestors, including researchers - working with the Centralised Data Steward and NICUS Coordinator and NICUS Business Analyst to facilitate data requests.
Local Data Custodian	The Local Data Custodian will apply this Framework, including when managing local unit-level data held in NICUS. The Local Data Custodian will also apply this Framework when approving use of local unit level data for secondary use including local audit, quality improvement and research purposes.
Local Data Steward	The Local Data Steward will apply this Framework, including when managing data held in NICUS with the oversight of the Local Data Custodian. The Local Data Steward will also apply this Framework when making recommendations to the Local Data Custodian around approving local unit level data for secondary use, including local audit, quality improvement and research purposes.
NICUS Audit Officers	The NICUS Audit Officers will apply this Framework, including when managing data held in NICUS with the oversight of the Local Data Custodian. The NICUS Audit Officers will also apply this Framework by: - ensuring data are recorded and collected according to data standards - identifying and rectifying data errors and quality issues in a timely manner - obtaining approval from the Local Data Custodian for release of local unit-level data for audit, quality assurance or research purposes - providing local expertise on the feasibility, clinical impact change and overall capacity of the staff to facilitate collection of new or amended variables collected by NICUS

NICUS Research Committee	The NICUS Research Committee will apply this Framework when: • reviewing research requests and providing advice and recommendations to the Data Custodian for the use of NICUS data assets for research purposes • supporting timely access to NICUS data for approved research projects through a structured governance sign-off process • identifying and prioritising research projects using NICUS data, through assessment of the potential impact of the research projects in improving health outcomes of neonates • engaging and collaborating with members of the neonatal community to produce high-quality research designed to improve health outcomes of neonatal patients • providing mentorship opportunities for early career researchers interested in using data assets held by NICUS.
Third Party and/or Principal Investigator	The Third Party is an organisation or individual requesting access to NICUS data for secondary use purposes. The applicant is responsible for preparing the application and committing to participating in the monitoring and assurance arrangements as stipulated by the Data Custodian.
Data User	Acting as the data integrator, the Data User is responsible for conducting the necessary data analysis with data approved by the Data Custodian.
System Administrator (NICUS Business Analyst)	The NICUS Business Analyst will apply this Framework when managing NICUS data assets for primary and secondary purposes. The NICUS Business Analyst will also apply this Framework when: • working with the Centralised Data Steward and NICUS Coordinator and NICUS Support Officer to facilitate data requests • providing consultation for researchers seeking feasibility of requesting data for research projects • assisting the Centralised Data Steward and NICUS Coordinator and NICUS Support Officer with complex data extractions to facilitate data requests. This role includes preparing and providing de-identified data for research and public health purposes. Other authorisations provide the basis for the disclosure of identified information for secondary use with individual consent.

Glossary

Term, acronym or abbreviation	Definition
ACI	NSW Agency for Clinical Innovation
ANZNN	Australian and New Zealand Neonatal Network
Clinical quality registry	A clinical quality registry systematically monitors the quality (appropriateness and effectiveness) of healthcare, within specific clinical domains, by routinely collecting, analysing and reporting health-related information. Data collected are used to identify benchmarks and variation in clinical outcomes and are provided back to clinicians, patients and health system managements to inform clinical practice and decision making. Note: It is the strategic intent of NSW Health to support virtual registries that use linked data to provide clinicians, patients and health system managers with timely feedback on clinical practice against agreed indicators of quality that are benchmarked, risk-adjusted and based on reliable data.
Data asset	"A data asset is a structured collection of data developed for a broad purpose. An enduring data asset (or enduring linked data asset) is a subset of this category, denoting the linkage of a larger range of data that is designed for potentially many purposes and users. An example of this is the NSW Human Services Data Set. A data asset could also include models, methodologies and algorithms."²
Data governance	Is "...a system of decision rights and accountabilities for information related processes, executed according to agreed-upon models which describe who can take what actions, with what information, and when, under what circumstances, using what methods."³
Data linkage	Is the bringing together of two or more datasets to create a new, richer dataset. When patients use different health services, information about them is captured in different datasets. Data linkage brings together multiple sets of data about patients to provide a more complete picture of their journey in the health system, including the outcomes of their healthcare.

	By bringing together sets of data that were previously isolated, researchers, clinicians and governments can deepen their understandings of the ways people use the healthcare system.
Data management	Is "...the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets." ³
Disclosure	Refers to the communication or transfer of information outside an organisation.
IDEA	Integrated Digital Enablement Accelerator Stream, ACI
IT	Information technology
Neonatal service	Neonatal services encompass low-dependency care (which may be a model of care and/or located in a special care nursery or special care unit), high-dependency care and neonatal intensive care provided in NICUs.
NICU	Neonatal intensive care unit. A tertiary service, which provides the highest level of care for neonatal patients. In NSW, there are two tiers of neonatal intensive care units: Level 5 and Level 6. Level 5 NICUs provide medical intensive care for newborn infants from 22 weeks' gestation. Level 6 NICUs are located in specialist children's hospitals where neonatal surgery and complex genetic and metabolic services are located or in NICUs co-located with specialist children's hospitals. Level 6 and Levels 6/5 neonatal services hold supra-local health district roles and provide statewide specialist services. They provide leadership within tiered perinatal networks and act as peak referral services.
NICUS	Neonatal Intensive and Special Care Units' Data Registry
Service capability	The planned activity and clinical complexity that a facility is capable of safely providing.
Statewide data asset	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.
Secondary use of health data	When personal health information is used outside of direct care delivery. It includes such activities as analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing and other business applications.

Transport and retrieval services	NSW Ambulance Service and Newborn and Paediatric Emergency Transport Service (NETS) provide transport and retrieval services for patients requiring urgent or non-urgent transfer between maternity and neonatal services.
Use	Refers to the communication or handling of health information within an organisation.