phn CENTRAL AND EASTERN SYDNEY

An Australian Government Initiative

Information and Data Governance Framework

Version	2.0
Responsible Manager	General Manager Corporate Services
Approved By	Board
Effective Date	02 December 2025

EIS Health Ltd.

Contents

Introduction

Central and Eastern Sydney Primary Health Network (CESPHN) recognises that information and data is a strategic asset that has value to the entire organisation. Information/Data is the foundation of our planning, decision making and operational functions.

CESPHN is the custodian and steward of information/data assets. We rely on strong information and data governance to perform our functions effectively and maintain the trust of our information/data providers, information/data recipients and stakeholders in acquiring, handling, and releasing data.

Purpose and scope

This Framework outlines how CESPHN effectively governs information and data. This includes:

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

This Framework applies to all data assets listed in CESPHN's data asset registry. This includes data collected and/or enhanced by CESPHN, collected on behalf of CESPHN and data obtained from external sources.

Audience

The intended audience of this document is all CESPHN staff and CESPHN stakeholders, including commissioned service providers that provide, receive, or use data from CESPHN.

Definitions

Term	Definition
Data	Data is raw, unorganised facts that need to be processed. Data can be something simple and seemingly random and useless until it is organised. Usually existing at rest in a database.
Database	A database is an organised collection of structured information, or data, typically stored electronically in a computer system. A database is usually controlled by a database management system (DBMS).
Data Breach	Loss, unauthorised access, or unauthorised disclosure of personal information.
Data Linkage	The bringing together from two or more different sources, data that relate to the same individual, family, place or event.
Information	Data that has been processed, organised, structured, or presented in a given context so as to make it useful.
Managed Service Provider (MSP)	an external party in charge of managing, maintaining and supplying systems and services to CESPHN.
PaaS	Platform-as-a-Service

SaaS	Software-as-a-Service
Cloud Service Provider	is a company or organisation that offers cloud services often abbreviated aaS, 'as a Service', which includes infrastructure 'IaaS', platforms 'PaaS', and software 'SaaS' delivered over the internet. These services allow users to store data, run applications, and access computing resources without needing to manage physical hardware.

Legal and regulatory environment

CESPHN must comply with the federal and state legislation, and health industry standards with respect to how data is collected, managed, secured, shared, and protected. The key documents that are relevant to this Framework are listed in the Framework document control.

Guiding principles

The governance of information and data at CESPHN is supported by the following principles:

- **Accessible** – ensures that information and data is easily available and usable by authorised Staff member/s. This means that information and data should be stored in a way that allows for efficient retrieval and use, while also being protected against unauthorised access.
- **Integrity** - ensures information and data is accurate, consistent, and trustworthy, preventing unauthorised alterations and maintaining data authenticity.
- **Transparency** – ensures clear documentation of information and data sources, usage, purpose and governance policies.
- **Protection** – Implementation of robust data security measures (e.g., encryption, access controls and appropriate categorising and labelling of information) and compliance with privacy laws and regulations (e.g. Australian Privacy Act).
- **Accountability** - Defining roles and responsibilities for data ownership and stewardship and enforcing policies and tracking compliance through audits and reporting.
- **Standardisation** - Data is easy to find and re-used (avoiding duplication) wherever possible, and stored in one location to ensure there is a single version of truth
- **Lifecycle Management** - Managing data from creation and usage to archiving and deletion, applying retention policies, and ensuring proper disposal of obsolete data.
- **Continuous Improvement** - Regularly reviewing and refining data governance practices and using metrics and feedback to enhance data quality, usability, and compliance.

Governance structure

Organisation structure

CESPHN's Information Security and Data Governance Committee, chaired by the General Manager Corporate Services with membership from all streams, drives the work program. The Chair of the Information Security and Data Governance Committee reports to the Executive Leadership Team, who in turn reports through to CESPHN's existing governance arrangements - the Finance, Audit and Risk Committee and Board. The data governance structure at CESPHN is outlined in Figure 1 below.

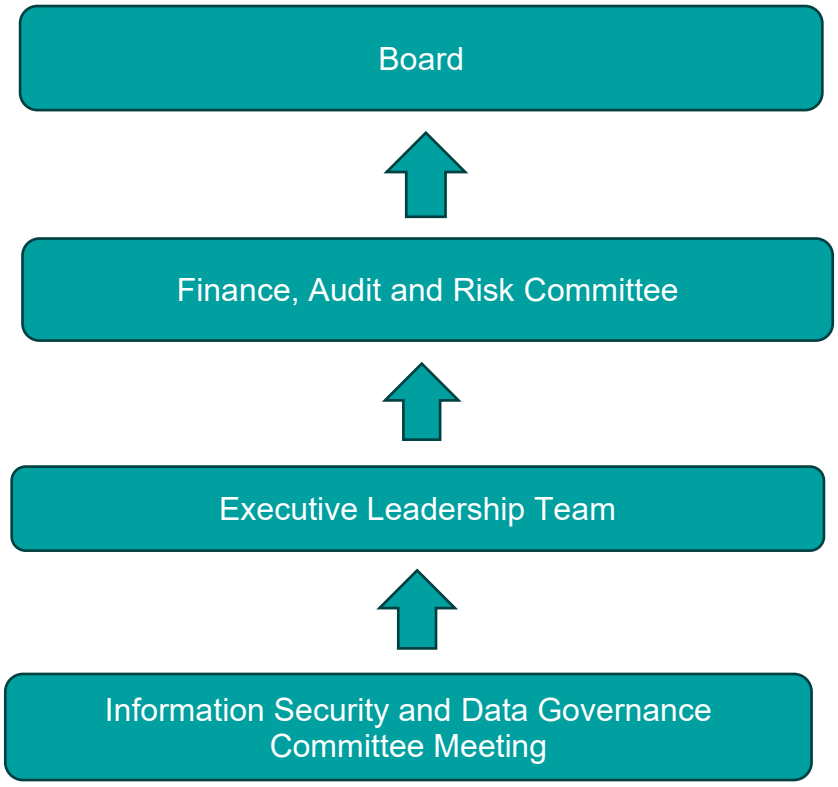

Figure 1: CESPHN's organisation structure

Board

The Board is responsible for setting the strategy and policy expectations for effective information and data governance, ensuring adequate resourcing and providing advice on major information security incidents and data breaches.

Finance, Audit and Risk Committee

The Finance, Audit and Risk is a committee of the Board and is responsible for oversight of information security and data governance and ensuring that information and data governance-related policies, systems and procedures are maintained and regularly reviewed.

Executive Leadership Team

The Executive Leadership Team comprises of the Chief Executive Officer and General Managers, and is responsible for:

- endorsing information security and data governance policies and procedures
- ensuring the resourcing and implementation of information security and data governance
- reporting information security and data governance and security and data related matters to the Finance, Audit and Risk Board Committee and Board.

Information Security and Data Governance Committee

The Information Security and Data Governance Committee is responsible for making recommendations to the Executive Leadership Team relating to information security, information and data governance and data related matters. The Committee is responsible for:

- ensuring compliance with relevant legislation, regulations, and standards
- determining resources to plan, implement, monitor, review and improve information security management and data governance
- builds Ensuring confidence in the quality and integrity of CESPHN's information and data assets
- overseeing efficient systems for collecting, storing, and validating data
- overseeing standard analytic and mapping tools
- monitoring emerging technologies and data sharing initiatives
- protects information and data through reviewing documented policies and procedures, and ongoing communication, education, and monitoring
- oversees the identification of risks and mitigation strategies including those associated with compliance, security, access, privacy, continuity, management, and cost
- oversees meaningful interpretation and reporting of information and data.
- Oversees the Information Security Management System (ISMS)
- Communicates the importance of meeting information security and data objectives, plans and continual improvement
- Maintains an awareness of business needs and major changes
- Oversees the continual improvement process with respect to information security and data governance
- Reviews major information security and data incidents, and oversees the actions and improvements
- Ensures external organisations/stakeholders that have access to information systems and services are based on a formal agreement that defines all necessary security and data requirements

Roles and responsibilities

Information security and data governance is everyone's responsibility – all staff have roles and responsibilities that are defined further in Figure 2 below.

Figure 2: CESPHN's data governance roles and responsibilities

Chief Executive Officer

The Chief Executive Officer is responsible for overseeing the implementation of the organisation's data governance responsibilities, including:

- ensuring the Board is provided with sufficient information to discharge its information and data governance responsibilities
- ensuring the policy and strategy frameworks established by the Board are effectively operationalised
- monitoring organisational compliance and performance
- authorising the release or sharing of data to third parties (Level 3 – Highly Confidential information and data) after an appropriate assessment has been undertaken.

Sponsor

The Sponsor is ultimately accountable for the information/data asset and is responsible for:

- establishing the rationale for CESPHN holding an information/data asset
- enabling the strategic management, governance, and operation of information/data assets
- providing direction and guidance, and authorising appropriate resources for management of an information/data asset
- ensuring adherence with all relevant legislation, policies, standards, and procedures
- appointing Custodians and ensuring the Custodian's duties are fulfilled.

Custodian

The Custodian is responsible for the day-to-day oversight of an information asset including the location of information/data and metadata, approval of access to information/data (please refer to the Access Management Procedure) and the overall quality and security of the information/ data. Key accountabilities include:

- establishing a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency, and reliability of the data
- establishing and maintaining an acceptable level of information/data protection to ensure privacy, security, and confidentiality of information
- ensuring the information/data asset has metadata, including an information/data dictionary, Standard Operating Procedure, business rules and guide to use
- ensuring any use of the information/data aligns with the purpose for which it was collected
- controlling access to data in compliance with all relevant legislation, policies and standards, and any conditions specified by the System Sponsor
- ensuring processes are in place to provide feedback to data suppliers about data quality including issues requiring rectification
- escalating material risks and issues to the Data Sponsor
- notifying the Data Governance Committee secretariat of any new data assets that need to be added to the asset registry or changes to existing data assets
- appointing Stewards and ensuring the System Steward's duties are fulfilled
- regularly reviewing users with access to data and the ongoing need and appropriateness of access, including:
- Staff commencements and exits
- Maintaining the System Access Request folio forms for a particular system
- Ensuring these requests are up to date and managed in accordance with this Framework

Steward

The Steward is responsible for the day-to-day management and operation of an information/data asset, its completeness and quality. Key accountabilities include:

- managing the information/data asset in compliance with relevant legislation, policies and standards, and any conditions specified by the Sponsor
- developing and maintaining metadata including a data dictionary, Standard Operating Procedure, business rules and a guidance document
- co-ordinating stakeholder engagement and input into the business requirements for a information/data asset
- maintaining the quality, integrity, and safety of the data
- providing feedback to information/data suppliers in relation to information/data quality issues
- conducting privacy impact assessments
- escalating material risks and issues to the information/Data Custodian.

User

The User is the person who uses information/ data to perform work duties. The User is responsible for and undertakes to:

- handling information and data in accordance with CESPHN's policies and procedures
- using information/data in accordance with purpose for which their use is approved
- taking reasonable steps to protect any confidential information from inappropriate or unauthorised use, access, or disclosure and is appropriately classified and labelled
- reporting any security incidents or weaknesses to the IT Manager
- attending training related to information and data governance.

Third party providers

Where third party providers are engaged in the capacity of a Managed Service Provider, Cloud Service Provider or to provide a SaaS or PaaS to CESPHN, it is the responsibility of Custodians to request certain actions outlined within this Framework be taken by third party providers on their behalf.

Third-party providers are accountable for:

- implementing and enforcing their own IT policies and procedures, Information/ Data Governance Framework, Information Security Policies and Procedures, Business Continuity Plans and providing a copy of these documents to CESPHN if requested.
- providing risk reports on information and data, security and CESPHN systems, they manage routinely
- having a process that is followed to notify CESPHN quickly of any suspected or actual information or data breaches and or security incidents
- following reasonable direction from CESPHN arising from any incident investigations
- ensuring that their staff understand and implement the information and data governance security requirements outlined in the contract with CESPHN
- providing information regarding accreditation with ISO-27001 and regular reports to CESPHN when requested
- ensuring all systems include access to audit trails and activity logs to assess integrity of system configuration, information and data accuracy
- ensuring systems include processes and mechanisms for fraud detection and vulnerability assessments
- Ensuring appropriate levels of insurance to cover professional indemnity or errors and omissions are always maintained
- ensuring information and data governance security requirements are understood and built into projects.

This does not prevent other contractual obligations being imposed.

Privacy Officer

- CESPHN's Privacy Officer is the first point of contact for advice to staff on privacy matters. The role is performed by the General Manager Corporate Services.
- Reporting to the Information Security and Data Governance Committee on all security, privacy and data governance related matters on a regular and ad-hoc basis when required
- Communicates the information security policy and ISMS related matters to all relevant interested parties where appropriate, including stakeholders
- Implement the requirements of the information security and data governance framework
- Manages risks associated with access to information/data and systems
- Ensures that security controls are in place and documented
- Establishes and maintains and reports on a continual improvement/no compliance action list and targets
- Declares Information Security incidents and data breaches, brings to management attention, and manages to negate/reduce the impact
- Attends and provides reports for management review meetings on a regular basis including quantify and monitor the types, volumes and impacts of security incidents and malfunctions, and reporting against objectives and targets.

Policies and procedures

CESPHN's internal information security and data-related policies, guidelines and procedures are designed to ensure compliance with the legal and regulatory environment described above and to provide staff, especially those with delegated authority as custodians and stewards, with clear sources of information to perform their roles effectively and appropriately.

It is the responsibility of all staff to observe and comply with this Framework and associated CESPHN policies and procedures that includes but is not limited to:

Information and Data governance

- Data Roles and Responsibilities
- Systems and Asset Registry

Information and Data privacy and security

- Privacy Policy
- Information Security Policy and Procedure
- Privacy Impact Assessments

Information Security Incidents and Data breaches

- Information Security Assessment and Response Procedure

Information and Data Sharing

- Information and Data Sharing and Release Procedure
- Data Sharing Agreements Registry
- Research Policy and Procedure
- For a complete list of information security and data governance policies refer to the REG Summary of Management System Documentation Register (limited access)

Information and Data use

- Acceptable Use Policy
- Access Management Procedure

Data quality

- Information and Data Quality Metrics

Induction procedures for CESPHN staff include an overview of the Information Security and Data Governance Framework, related policies and procedures, and user responsibilities and accountabilities. Additionally, new staff will undertake Information Security and Data Governance Framework training and complete online Privacy training. This is in addition to all staff signing contracts at the time of employment and acknowledging the Staff Code of Conduct that outlines their information security and confidentiality and privacy requirements in relation to all information and the consequences of breaching confidentiality, information security, data governance and policies and procedure.

Lifecycle Management

Information and Data Lifecycle Management includes the administrative processes throughout the lifecycle of information and data – from the creation or acquisition, storage, protection, release, and destruction – to ensure the integrity, availability, confidentiality, quality and appropriate access of information and data. A plan documenting these processes must be developed for each information/data asset within the Standard Operating Procedure of the system which the information/data asset resides.

Information and Data acquisition

CESPHN collects information and data to better understand and improve the health system Information and data is only collected and held if it is necessary for or directly related to one or more

of CESPHN's functions or activities. Information and data are stored alongside metadata and information/data dictionaries to accurately define and describe it.

All new or significantly changed information/data assets are recorded in CESPHN's System and Data Asset registry. The registry identifies Custodian of each information/data asset, its storage location, and whether it contains identifiable information/data. Privacy Impact Assessments are completed for each information/data asset when implemented or if there is a change process to assess information/data risks and identify appropriate controls.

Refer to the Privacy Policy for more information.

Information and Data storage and security

CESPHN stores information and data using secured cloud-based storage solutions. CESPHN's ICT Policies, Information Security Policies and Procedures and Information Security in relation to Third-parties provide a detailed description of:

- security requirements for internally and externally hosted systems
- hosting requirements for cloud-based solution data centres
- information and data backup and restoration requirements
- administrative access levels to servers
- proper use of IT systems.

Security is an important component of maintaining information and data integrity whereby the appropriate security measures protect information and data from unauthorised access and alteration or corruption. CESPHN ensures information and data integrity through information security by:

- authorising access to information and data according to permissions determined by the Custodian and to the level of classification as outlined in the Information Classification Policy and Procedure
- regularly updating security protection on all devices
- providing online safety awareness training to staff.

Information and Data quality

Information and data quality management encompasses the activities and processes to optimise and enhance the quality of information and data held by CESPHN. Users should have access to information and data that is accurate, complete, consistent, and up to date. Information about the quality of an information/data asset should be accessible to Users to ensure appropriate caveats are considered.

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

Custodians are responsible for documenting data quality metrics as required by the data set. Metrics must include the measures of accuracy, completeness, consistency, timeliness, availability, and fitness of use.

Information and Data access, use and analysis

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

inadvertent alteration or disclosure. The core principles of information and data access and use include:

- **Ethical**: Custodians must meet their ethical obligations and consider risks and burdens to individuals the information and data relates to, informed consent, privacy and whether ethical review is required.
- **Need to know**: Custodians must ensure users are granted the minimum requirements for data use to undertake their business role or for approved purposes.
- **Specific and authorised**: the information and data must not be used by persons other than the specified authorised persons.
- **Approved disclosure**: authorised persons must not disclose information and data to any other persons without prior approval from the Custodian.
- **Specified use**: the information/data must only be used for the purpose specified.
- **Secure and controlled use**: the information and data must always be protected by the appropriate security and controls as required by the relevant classification.
- **Duration of access**: the information and data must not be kept for longer than approved without additional approval from the Custodian.

Refer to the Access Management Procedure for more information.

Ethical considerations (including triggers for ethical review by a Human Research Ethics Committee (HREC) are outlined further in CESPHN's Evaluation Framework requests to access information/data for research purposes must follow the protocol detailed in CESPHN's Research Policy and Procedure and Data Sharing and Release Procedure.

Information and Data sharing and release

Sharing and release of data to third parties must comply with state and federal privacy legislation. An appropriate assessment must be undertaken to determine the purpose of releasing data, ensure HREC approval has been granted where applicable, and assess privacy and security risks, such as accidental loss or damage, unauthorised access, malicious misuse, and inadvertent alteration or disclosure. For further information, please refer to the Information Classification Policy and Procedure and Data Sharing and Release Procedure.

Data archiving and destruction

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

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

Refer to the Back Up Policy and Procedure for more information.

Information/Data Linkage

CESPHN may use data linked from multiple sources (eg LUMOS initiative) to understand the health needs of the population. If requested to contribute data to a data linkage project CESPHN will ensure:

- Ethics approval is obtained
- Protection of patient confidentiality
- Data sharing agreements are in place
- Measures are in place to ensure safe and secure data use and storage
- Completion of privacy impact assessments

Compliance

CESPHN regularly monitors compliance with its information and data management security requirements. The Information Security and Data Governance Committee reviews the information and data assets and assesses the information security risk register on a regular basis. The Information Security and Data Governance Committee also regularly reports progress against its workplan and the compliance against the ISO 27001 standard and Data Strategy to the Finance, Audit and Risk Board Committee and the Board.

Data breaches

In the event an information and or data breach occurs either by internal staff, service providers, hackers or cyber criminals, CESPHN has a procedure in place to ensure it can act swiftly to mitigate risk and prevent recurrence. The procedure includes the notification of a data breach if it is likely to result in serious harm to an individual as required under the Notifiable Data Breaches scheme. Please refer to the CESPHN Information Security Incident Assessment and Response Plan for more information. If an information or data breach has occurred, please report this via the Folio Information Security Incident Notification Form.

Framework document control

Documents related to this policy
Privacy Act 1988 (Cth)
Health Records and Information Privacy Act 2002 (NSW)
Freedom of Information Act 1982 (Cth)
CESPHN Privacy Policy
CESPHN Evaluation Framework
CESPHN Research Policy and Procedure
CESPHN Information Security Policy and Procedure
CESPHN Access Management Procedure
CESPHN Information Security Incident Assessment and Response Procedure
CESPHN Information and Data Sharing and Release Procedure
CESPHN Back Up Policy and Procedure
CESPHN Information Classification and Labelling Procedure
CESPHN Data Sharing Agreements Registry
CESPHN Acceptable Use Policy
CESPHN Access Management Procedure

ISO 27001 and ISO 9001 Controls

Controls	Name
27001 5.9	Inventory of information and other associated assets
27001 5.10	Acceptable use of information and other associated assets
9001 4.4	Quality management system and its processes
9001 5.3	Organisational roles, responsibilities and authorities

Framework review and version tracking

Version	Date Approved	Approved By	Next Review Date
1.0	March 2020	Board	March 2023
2.0	23 September 2023	EIS Health Board	23 September 2025
3.0	02 December 2025	EIS Health Board	02 December 2025