DATA GOVERNANCE FRAMEWORK

VERSION	1.0
DOCUMENT AUTHOR	Data Governance Committee
APPROVED BY	EIS Health Ltd. Board
EFFECTIVE DATE	31 March 2020

EIS Health Ltd.

Contents

1. Introduction

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

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

1.1 Purpose and scope

The purpose of this Framework is to outline how CESPHN effectively governs data. This includes:

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

The Framework applies to all data assets listed in 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.

1.2 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.

2. 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 following are key documents that are relevant to this Framework:

- Privacy Act 1988
- Health Records and Information Privacy Act 2002
- Freedom of Information Act 1982
- Australian Secure Cloud Strategy
- RACGP Computer and Security Standards
- Practice Incentives Program Eligible Data Set Data Governance Framework
- Framework to guide the secondary use of My Health Record system data.

3. Guiding principles

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

- **Data is secure and privacy is protected:** sensitive and personally identifiable data are protected by the highest security standards and personally identifiable information is managed in line with legislation
- **Data is accessible:** data is available and accessible to authorised individuals when it is needed
- **Data is discoverable and re-usable:** data is easy to find and re-used wherever possible and stored in one location to ensure there is a single version of truth
- **Data is appropriately managed:** data is managed in a way that is transparent with clear roles and responsibilities to ensure accountability
- **Data quality and integrity improvement is essential:** data is accurate and reliable.

4. Governance structure

4.1 Organisation structure

CESPHN's Data Governance Committee, chaired by the General Manager for Planning and Engagement with membership from all streams, drives the work program. The Chair of the Data Governance Committee reports to the Executive Management Team, who in turn reports through CESPHN's existing governance arrangements to the Governance Sub-Committee and Board.

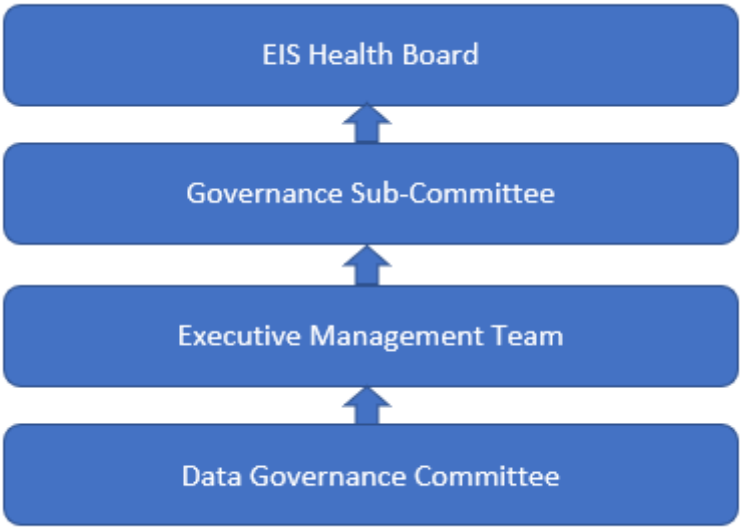

Figure 1: CESPHN's organisation structure

EIS Health Board

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

Governance Sub-Committee

The Governance Committee is a sub-committee of the EIS Health Board and is responsible for oversight of data governance and ensuring that data governance related policies, systems and procedures are maintained and regularly reviewed.

Executive Management Team

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

- Endorsing data governance policies and procedures
- Ensuring the resourcing and implementation of data governance
- Reporting data governance and data related matters to the Governance Sub-Committee and Board.

Data Governance Committee

The Data Governance Committee is responsible for making recommendations to the Executive Management Team relating to data governance and data related matters. The Committee is responsible for ensuring:

- Compliance with relevant legislation, regulations and standards
- Clear roles and responsibilities in relation to data management
- Confidence in the quality and integrity of CESPHN's data assets
- Efficient systems for collecting, storing and validating data
- Standard analytic and mapping tools

- Monitoring emerging technologies and data sharing initiatives
- Protection of data through documented policies and procedures, and ongoing communication, education and monitoring
- Risks are identified and mitigated including those associated with compliance, security, access, privacy, continuity, management and cost
- Meaningful interpretation and reporting of data.

4.2 Roles and responsibilities

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

Figure 2: CESPHN's data governance roles and responsibilities

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 Corporate Services General Manager.

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 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 after an appropriate assessment has been undertaken.

Data Sponsor

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

- Establishing the rationale for CESPHN holding a data asset
- Enabling the strategic management, governance and operation of data assets
- Providing direction and guidance, and authorising appropriate resources for management of a data asset
- Ensuring adherence with all relevant legislation, policies, standards and procedures

- Appointing Data Custodians and ensuring the Data Custodian's duties are fulfilled.

Data Custodian

The Data Custodian is responsible for the day to day oversight of a data asset including the location of data and metadata, approval of access to data and the overall quality and security of the 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 data protection to ensure privacy, security and confidentiality of information
- Ensuring the data asset has metadata, including a data dictionary, business rules and guide to use
- Ensuring any use of the data aligns with the purpose for which is was collected
- Controlling access to data in compliance with all relevant legislation, policies and standards, and any conditions specified by the Data Sponsor
- Ensuring processes are in place to provide feedback to data suppliers about data quality including issues requiring rectification
- Escalating material risks and issues to the Data Sponsor
- Notifying the Data Governance Committee secretariat of any new data assets that need to be added to the asset registry or changes to existing data assets
- Appointing Data Stewards and ensuring the Data Steward's duties are fulfilled.
- Regularly reviewing users with access to data and the ongoing need and appropriateness of access

Data Steward

The Data Steward is responsible for the day to day management and operation of a data asset, its completeness and quality. Key accountabilities include:

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

Data User

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

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

5. Policies and procedures

CESPHN's internal 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 include:

- Data governance
  - Data Roles and Responsibilities Manual
  - Data Systems and Asset Registry
- Data privacy and data security
  - Privacy Policy and Procedure
  - IT Infrastructure Policy and Procedure
  - Cyber Security Policy and Procedure
  - Privacy Impact Assessments
- Data breach
  - Data Breach Response Plan
- Data sharing and data release
  - Data Sharing and Release Procedure
  - Data Sharing Agreements Registry
  - Research Policy
- Data use
  - Internet and Computer Usage Policy and Agreement
  - Access Management Procedure
  - Online Survey Procedure
  - Information Management Guidelines
- Data quality
  - Data Quality Metrics

Induction procedures for CESPHN staff include an overview of the Data Governance Framework, related policies and procedures, and user responsibilities and accountabilities. This is in addition to all staff signing confidentiality agreements at the time of employment that clearly spell out their information security responsibilities and the consequences of breaching confidentiality.

6. Data management

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

6.1 Data acquisition

CESPHN collects data to better understand and improve the health system. Data is only collected and held if it is necessary for, or directly related to one or more of CESPHN's functions or activities. Data is stored alongside metadata and data dictionaries to accurately define and describe it.

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

data. Privacy Impact Assessments are completed for each data asset to assess data risks and identify appropriate controls.

6.2 Data storage and security

CESPHN stores data on-site and using secured cloud-based storage solutions. CESPHN's IT Infrastructure Policy and Procedure and Cyber Security Policy and Procedure provides a detailed description of:

- Security requirements for internally and externally hosted systems
- Hosting requirements for cloud-based solution data centres
- Data centre backup and restoration requirements
- Administrative access levels to servers
- Proper use of IT systems.

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

- Authorising access to data according to permissions determined by the Data Custodian
- Regularly updating security protection on all devices
- Providing online safety awareness training to staff.

6.3 Data quality

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

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

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

6.4 Data access, use and analysis

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

The core principles of data access and use include:

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

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

6.5 Data sharing and release

Sharing and release of data to third parties must comply with state and federal privacy legislation. An appropriate assessment must be undertaken to determine the purpose of releasing data, ensure Ethics Committee approval has been granted where applicable, and assess privacy and security risks, such as accidental loss or damage, unauthorised access, malicious misuse, and inadvertent alteration or disclosure.

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

7. Compliance

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

7.1 Data breaches

In the event that a data breach occurs, 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.