Data Governance Policy

Version 2.0| 19 October 2015

cancer institute NSW

Working together to lessen the impact of cancer

Document Title:	*Data Governance Policy*			
Summary:	This policy provides the Cancer Institute NSW with an instrument to formally manage its data assets in a collaborative, consistent and co-ordinated manner.			
Date of Issue:	*19/10/2015*			
Status:	*Final*			
Contact Officer:	*Manager, Data and Information Governance*			
Applies To:	*All staff and contractors of all Divisions of the Cancer Institute NSW.*			
References:	*CINSW Policy, Procedures and Guidelines:* • Information Security Policy (for end users) (E07/26801[v2]) • Information Classification and Labelling Procedure (E14/02843[v2]) • Records & Information Management Policy (E06/10927) • Data Custodian Guideline (E14/15305) *NSW Government:* • NSW Government – NSW Data & Information Custodianship Policy • Electronic Information Security Policy – NSW Health • NSW Health – Privacy Manual for Health Information • NSW Health Data Governance Program – Staff roles and responsibilities • Data collections – disclosure of unit record data for research or management of health services • Cancer Institute (NSW) Act 2003 *Industry:* • Data Management Association's Guide to the Data Management Body of Knowledge (DAMA-DMBOK)			
Version and Change History	**Version**	**Who**	**Date**	**What**
	0.1	*Stephen James*	03/10/2010	*Initial draft.*
	1.0	*Stephen James*	27/07/2010	*Revised final draft.*
	1.1	*Narelle Grayson*	09/09/2015	*Reviewed and updated Policy*
Approvals	**Version**	**Who**	**Date**	**Record**
	1.0	*Beth Macauley*	July 2010	*Email approval*
	2.0	*Beth Macauley*	19/10/2015	*Email approval*

Contents

1 Introduction

The Cancer Institute NSW (the Institute) was established in July 2003 through the Cancer Institute (NSW) Act 2003 to lessen the impact of cancer in NSW. The Institute is funded by the NSW State Government and governed by the Cancer Institute NSW Board. The Institute's objectives are to:

- reduce the incidence of cancer in the community
- increase the survival rate for cancer patients
- improve the quality of life of cancer patients and their carers
- provide a source of expertise on cancer control for the government, health service providers, medical researchers and the general community.

The Institute's data assets are used to support these objectives.

2 Purpose

The purpose of this policy is to provide the Institute with an instrument to govern its data assets effectively through the exercise of authority and control (planning, guiding and monitoring) over the management of these assets in order to ensure:

- strategic alignment of the Institute's data assets to the NSW Cancer Plan
- compliance with relevant legislation, policies and procedures and standards
- confidence in the data used to inform decisions
- effective assurance and control of data management processes
- formalised roles and responsibilities
- protection of the data through documented policies and procedures, and ongoing communication, education and monitoring.

3 Scope

This policy covers data governance for all of the Institute's data assests (regardless of the system in which the data are stored) and data management functions as defined by the Data Management Association's Guide to the Data Management Body of Knowledge (DAMA-DMBOK):

- Data Quality.
- Data Privacy and Security.
- Meta-data.
- Masterdata and Reference data.

- Data Warehousing and Business Intelligence.
- Document & Content.
- Data Architecture.
- Data Development.
- Data Operations.

4 Policy Statements

4.1 Data Governance Policy

A Data Governance Policy (this document) shall be maintained by the Manager, Data & Information Governance, approved by the Chief Operating Officer and published and communicated to all relevant employees and relevant external parties. This Policy shall be reviewed and updated annually, or sooner if required.

4.2 Data Management Function Policies

A Policy shall be documented for each Data Management Function. These policies must be referenced when reviewing or updating current data management procedures or when developing new data management procedures across the Institute. Each Policy shall be reviewed and updated annually, or sooner if required.

4.2.0 Data Quality

Data shall be 'fit for purpose' and each data asset shall have defined data quality requirements. Data quality shall be assured, measured, monitored and improved based on timeliness, accuracy, validity, completeness, relevance and reliability. Information about data quality shall be made available to users to ensure they are aware of the quality of the data when making decisions or interpreting findings. Where possible, data quality shall be assured at the point of creation.

4.2.1 Data Privacy and Security

Each data asset shall be classified according to the Information Classification and Labelling Procedure (E14/02843). Data must be secured and protected from unauthorised access. Data must be collected, stored, used & disclosed and archived & disposed in accordance with privacy legislation and relevant privacy and security policies and procedures. A Privacy Impact Assessment shall be conducted prior to the undertaking of any business initiative, project or act which has the potential to incur privacy risks. A formal privacy breach procedure shall be applied for all suspected and actual privacy breaches. On commencement of employment at the Institute, and every two years thereafter, all staff, including contractors must complete privacy and security training and sign an Information privacy and confidentiality agreement.

4.2.2 Meta-data

Each data asset shall have Meta-data. Meta-data shall conform to published standards and industry guidelines. Meta-data shall be recorded and maintained on a central repository. The quality of meta-data shall be assured, measured, monitored and improved. Changes to Meta-data shall be agreed and authorised with due consideration of impacts to other data management functions and business processes.

4.2.3 Masterdata and Reference data

Masterdata and Reference data shall be agreed at the enterprise level. Definitions shall comply with state and national standards where possible. Masterdata shall be recorded and maintained on a central repository. Changes to Reference and Masterdata shall be agreed and authorised with due consideration of impacts to other data management functions and business processes.

4.2.4 Data Warehousing and Business Intelligence

The Institute Data Warehouse (IDW) shall be the data repository for analytical data and organisational reporting. Changes to the Institute Data Warehouse and Business Intelligence environments shall be agreed and authorised with due consideration of impacts to other data management functions and business processes. Consideration of impacts to the IDW and Business Intelligence environments shall be made before changes to source data assets are implemented.

4.2.5 Document and Content Management

Records shall be managed in an appropriate manner in accordance with relevant legislation, standards and policies issued by the State Records Authority, and the Institute's Record Management Policy (E06/10927)

4.2.6 Data Architecture

The Institute's data model shall be expanded in an iterative approach to include all data assets. The data model shall align to Institute business processes and shall support linkage between data assets, within and across data domains.

4.2.7 Data Development

Data requirements shall be identified and defined during development of all systems. Systems shall conform to data architecture and standards.

4.2.8 Data Operations

Plans for data availability, recovery and retention shall be established, monitored and updated. Mechanisms to monitor and improve the performance of data assets shall be implemented. Data technology shall be managed according to ITIL principles and align with data requirements and conform to data architecture and standards.

4.3 Data Management Procedures

Data Management Procedures shall define the processes and procedures to be followed in order to meet the policy statements of one or more Data Management Function Policies. Existing Procedures shall be reviewed and updated and new Procedures shall be documented and applied which meet the Data Management Function Policy statements.

4.4 Data Governance Program & Framework

A Data Governance Program & Framework shall be established, implemented, operated, monitored, reviewed, maintained and improved to ensure that appropriate authority and control (planning, guiding and monitoring) is applied to data, and that data are managed in line with legislative and other compliance obligations. The Data Governance Program shall be governed by the Data Governance Committee, the Data Governance Program Group and various Data Governance Working Groups.

4.5 Data Inventory & Data Sponsorship & Custodianship

All data assets shall be clearly identified and an inventory of all data assets shall be maintained. All new data assets must be approved by the Data sponsor and a Data custodian must be appointed to each data asset by the Data Sponsor. Data custodian appointments shall be reviewed biannually. The Data custodian must be documented in the Data Inventory.

4.6 Data Compliance

Management of data (data collection, storage, access, use & disclosure and archiving & disposal) shall remain compliant with the Institute's various obligations including those specified within relevant legislation, NSW government policies and directives, NSW Health Policy Directives, Institute policies, procedures and guidelines, as well as other obligations such as contractual requirements.

4.7 Data Management Monitoring

Data and data management functions shall be measured, monitored and refined to ensure their effectiveness and quantify their value to the Institute.

5 Roles & Responsibilities

5.1 Chief Operating Officer

The Chief Operating Officer will:

- Approve the Data Governance Policy.
- Approve the necessary resources required to establish, implement, operate, review, maintain and improve the Cancer Institute NSW's Data Governance Program.

5.2 Executive

The Executive will:

- Provide the necessary resources to establish, implement, operate, review, maintain and improve the Institute's Data Governance Program.

5.3 Chief Information Officer

The Chief Information Officer will:

- Approve the Data Governance Data Management Function Policies.
- Conduct an annual review of the Data Governance Program and ensure that actions are applied as required.

5.4 Manager, Data and Information Governance

The Manager, Data and Information Governance will:

- Review and update the Data Governance Policy and Data Managment Function Policies & Procedures.
- Manage the overall establishment, implementation, maintenance, and continual improvement of the Data Governance Program.
- Apply actions required from annual review of the Data Governance Program.

5.5 Directors

All Directors will:

- Ensure that staff and contractors who have a role to play in data governance comply with the Data Governance Policy and Data Management Function Policies and are trained and remain competent to fulfil their duties.
- Ensure that business processes and procedures are aligned with the Data Governance Policy and Data Management Function Policies.

5.6 All Staff

All personnel (including staff and contractors) will:

- Comply with the Data Governance Policy and Data Management Function Policies.
- Participate in training related to data governance.
- Remain aware of their data governance roles, responsibilities and obligations.

5.7 Data Sponsor

The data sponsor undertakes the functions of 'ownership' of the data. They have the authority to approve and fund the data collection.

The functions of the data sponsor are:

- identifying the need for the data collection;
- defining the purpose of the data collection;
- establishing the scope and coverage of the collection;
- appointing a custodian and defining custodianship arrangements;
- adequately resourcing the data collection;
- directing the development of the data collection; and
- authorising release of information.

The Sponsor of the data assets held by the Institute is the Chief Cancer Officer.

5.8 Data Custodian

Data custodians are appointed by the Data Sponsor and have overall responsibility for the data asset(s). They should be knowledgeable about the data asset(s) but do not need to have technical expertise.

The functions of the data custodian are:

- Data compliance.
- Data collection implementation.
- Data storage and security.
- Data standards and quality.
- Data access (use and disclosure).

Further information can be found in the Data Custodian Guideline (E14/15305).

5.9 Business Owner

Business owners are managers who oversee the data asset(s) for their particular business area. They have responsibility for:

- Ensuring data management procedures and processes within their business area are documented and are aligned to the Data Management Function policies.

- Prioritising data and data management requirements identified by data managers.
- Ensuring data management issues are resolved in a timely manner.
- Ensuring data and data management functions are monitored and improved.
- Authorising user access to data assests within their business area in consultation with the data custodian.
- Ensuring staff are trained and competent to fulfil their data management duties.

5.10 Data Manager

Data managers work with data custodians and business owners to define and control data. They have high level knowledge and expertise in the content of the data they manage. Their responsibilities are related to the data management functions, including:

- Defining data and data management requirements and specifications.
- Improving data management (e.g. improving quality).
- Identifying and resolving data management issues.
- Measuring and monitoring data management activities and initiatives.
- Maintaining data management processes (e.g. maintaining meta-data).

5.11 Data User

Every person who is an authorised user of a data asset is responsible for:

- Ensuring that their access to the data is carried out in a way which does not jeopardise data security and privacy.
- Not allowing their user names or passwords to be used by any other person or accessing data on behalf of any other person; (any person who wishes to access data should apply to the data custodian for authorisation).
- Ensuring that paper documents with personal or health information are stored securely and are not viewable by others during use.
- Reporting any breach or suspected breach of data security or privacy to the data custodian.
- Signing an acknowledgement of their obligations to protect data privacy.
- Striving to ensure that data are complete, accurate and up to date.
- Complying with relevant policies and procedures.

For more information, refer to the Information Security Policy (for end users) (E07/26801[v2]).

6 Glossary

A glossary of terms and definitions is outlined in the table (below).

Term	Definition
Business Owner	Business owners are managers who oversee the data collection for their particular business area.
DAMA-DMBOK	Data Management Association's Guide to the Data Management Body of Knowledge.
Data Architecture Management[1]	Defining the blueprint for managing data assets.
Data Asset[2]	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions. Included in the Institute's Data Inventory
Data Custodian	The position appointed by the Data Sponsor that has overall responsibility for a data asset, including: • Data compliance • Data collection implementation • Data storage and security • Data standards and quality • Data access (use and disclosure) The data custodian for a particular data asset is listed in the Data Inventory entry for that data asset.
Data Development[1]	Analysis, design, implementation, testing, deployment, maintenance.
Data Governance[1]	The exercise of authority and control (planning, guiding and monitoring) over the management of an organisation's data assets.
Data Management Function[1]	One of the business processes within data management – Data Governance, Data Architecture, Data Development, Data Operations Management, Data Privacy and Security Management, Data Quality Management, Master and Reference Data Management, Data Warehousing and Business Intelligence Management, Document and Content Management, Meta-data Management.

Term	Definition
Data Manager	The person who works with data custodians and business owners to define and control data. They have significant experience and knowledge of data and data management functions.
Data Operations Management[1]	Providing support from data acquisition to purging.
Data Privacy and Security Management[1]	Ensuring privacy, confidentiality and appropriate access.
Data Quality Management[1]	Defining, monitoring and improving data quality.
Data Sponsor	The position that "owns" the data asset. They have the authority to approve and fund the data asset. The Chief Cancer Officer is the Data Sponsor of all Institute data assets.
Data user	A person who is an authorised user of a data asset.
Data Warehousing and Business Intelligence[1]	Enabling reporting and analysis.
Document and Content Management[1]	Managing data found outside of databases.
IDW	Institute Data Warehouse.
Institute	Cancer Institute NSW.
Master and Reference Data Management[1]	Managing golden versions and replicas.
Meta-data Management[1]	Integrating, controlling and providing meta-data. Meta-data is information about the physical data, technical and business processes, data rules and constraints, and logical and physical structures of the data.

1. The Data Management Association Guide to The Data Management Body of Knowledge (DAMA-DMBOK Guide). First Edition (https://technicspub.com/dmbokanddq/). See: H:\Administration Support\DAMA-DMBoK
2. Adapted from: Qld Government Chief Information Office - *What is information architecture* – White paper 1.0.0. (https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2338-information-architecture-white-paper?lnk=QS0xLTIzMzgtMQ).