Records & Information Management Policy

Version 5.1 | 02 March 2018

Document Title:	*Records & Information Management Policy*
Summary:	*This document establishes a framework for managing information assets that are records. It outlines the principles and accountabilities to ensure that records are created, maintained, used and disposed of by the Cancer Institute NSW (the Institute).*
Date of Issue:	*02 March 2018*
Status:	*Active*
Contact Officer:	*Chief Information Officer (CIO)*
Applies To:	*All staff, including contract staff, outsourced providers of services, and volunteers.*
References:	***Legislative, Government Policies Directives and Standards on Records Management:*** • *Health Administration Act, 2002* • *State Archives and Records Act 1998 - including standards and retention and disposal authorities issued under the Act (replaced Archives Act 1960)* • *Government Information (Public Access) Act 2009 (GIPA) – (replaced the Freedom of Information Act 1989)* • *Privacy and Personal Information Protection (PPIA) Act 1998* • *Health Records and Information Privacy Act 2002* • *Electronic Transaction Act 2000* • *Evidence Act 1995* • *Standards issued by the NSW State Archives and Records Authority* • *Recordkeeping Policy Directives issued by the Ministry of Health* • *AS ISO 15489 Australian Standard on Records Management (2002)* • *NSW Premier's Memo 2012-15: Digital Information Security Policy* • *Records Management – Department of Health* • *Records Disposal Authority (DA 25) (Use of Functional) by NSW Department of Health* • *State Archives and Records - Checklist for the Senior Responsible Officer for records and information management* • *State Archives and Records Authority of NSW – Records and Information Management Policy Checklist* • *State Archives and Records Authority of NSW – Disposal Authority (DA57)*

- *State Archives and Records Authority of NSW – Cancer Institute NSW Functional Retention and Disposal Authority (DA 204)*
- *State Archives and Records Regulation 2015 – Normal Administrative Practice Guidelines*
- *Cancer Institute (NSW) Act 2003*
- *NSW ICT Strategy, Information Management Framework, A Common Approach to Information Management and Standards, June 2013*
- *Communications - Use & Management of Misuse of NSW Health Communications Systems*
- *NSW Health – Records Retention and Disposal on the Closure of Health Organisations*

Institute Policies and Procedures:

- *Records and Information Management Procedure (E15/13547)*
- *Data Governance Policy (E10/13359)*
- *Information Security Policy – for end users (E07/26801)*
- *Information Classification and Labelling Guidelines (E14/02843)*
- *Risk Management Policy (E07/27229)*
- *ISMS Policy (E09/02164)*
- *Business Continuity Management Policy (E12/28428)*
- *ICT Recovery Plan (E15/21826)*

Version and Change History	**Version**	**Who**	**Date**	**What**
	1.2	*Not Stated*	Sept 2007	*Not Stated*
	2.0	*Not Stated*	Dec 2009	*Not Stated*
	3.0	*J Bosanquet*	Dec 2011	*Not Stated*
	3.1	*C Ashton / S Mai*	30/04/2015	*Re-draft of policy to include statutory changes & incorporate SRO responsibilities.*
	4.0	*P Siddens*	2/09/2015	*Content changes to align with: State Records Authority of NSW Records & Information Management Policy Checklist, State Records NSW - Records Management Policy & State Records NSW – Senior Responsible Officer for Records & Information Management Checklist.*
	5.0	*P Siddens*	21/10/2016	*Annual review & minor amendments to numbering of*

				sections/topics and name change for State Archives and Records Authority of NSW.
	5.1	*P Siddens*	02/03/2018	*Annual review & minor edits.*
Approvals	**Version**	***Who***	**Date**	**Record**
	1.2	*Not Stated*	Sept 2007	*Not Stated*
	2.0	*Not Stated*	Dec 2009	*Not Stated*
	3.0	*Not Stated*	Dec 2011	*Not Stated*
	4.0	*B Macauley*	Oct 2015	*Email approval*
	5.0	*Jane Moxon*	30/11/2016	*Email approval*
	5.1	*Lisa Cox*	04/06/2018	*Email approval*

Contents

1 Introduction

1.1 Overview

The records and information management policy establishes the governance framework for the creation, capture, control, use, maintenance, and disposal of records and information in the Cancer Institute NSW (the Institute). The records and information management policy works in conjunction with records and information management strategies developed by the Institute. The strategies implement and deliver effective records and information management within the Institute and help to support and facilitate good business.

Information is a key asset of the Institute. All information resources need to be managed and handled in a consistent manner from their creation/acquisition to disposal in order to:

- maximise their utility to the Institute;
- Demonstrate the Institute's compliance with legislation and regulations, provide a mechanism for consistent, accountable and informed decision-making based on access to reliable information.

This policy creates a framework for managing information assets that are records. It outlines:

- the principles adopted by the Institute to manage records;
- Roles and responsibilities applicable to all staff who create and manage Institute records.

1.2 Objectives

The objectives of the records and information management policy are to:

- ensure that full and accurate records of all activities and decisions of the Institute are created, managed and retained or disposed of appropriately;
- demonstrate the Institute's compliance with legislation and regulations which may affect records and information management;
- Meet the Institute's obligations for accountability while ensuring that it protects the rights and interests of the organisation, its staff, clients and the community.

1.3 Scope

This policy applies to records, in all formats (including electronic records), received, used or created by the Institute.

This policy applies to all staff, contractors and temporary employees of the Institute.

2 Policy

The Institute will manage its records in accordance with legislation, government directives, best practice standards and related policies (see the references within this document for more information).

2.1 Records as a Resource

The Institute values records and information as a strategic resource that is integral to good business. Recordkeeping responsibilities are assigned to all staff (and contractors), including the requirement to create and retain records.

2.2 Records & Information Management Program

In accordance with Section 12 (2) of the *State Archives and Records Act 1998*, the Institute will establish and maintain a Records & Information Management Program that includes a planned, co-ordinated set of policies, procedures, people, systems and activities that are required to manage records.

The Records & Information Management Program will consider the following records and information management strategies:

- integrating records and information management into work processes, systems and services;
- implementing records and information management to ensure that it is accountable and meets business needs;
- managing email;
- managing risk assessments and use of cloud or similar service arrangements;
- managing the use of removable storage;
- managing and maintaining the corporate records & information management system (HPRM);
- integrating records and information management into business systems and managing and preserving records and information of long term value in these systems;
- managing records and information held in social media applications;
- Managing records and information used with mobile devices or BYOD.

Effective records and information management strategies ensure that:

- information assets are managed responsibly and in accordance with best practice;
- accurate, reliable and relevant information can be provided to the business and clients;
- the Institute's investment in its information assets is not wasted (i.e. information can be reused and repackaged to enhance opportunities and stimulate innovation);
- records and information are more accessible and useable and available for those with appropriate authority;

- costs are reduced as the Institute does not retain records and information unnecessarily;
- the Institute can provide stakeholders with transparency around, and accountability for, government operations; and
- the Institute is compliant with legislative and audit requirements.

2.3 Creation, Capture and Storage of Records

All staff in the Institute will create and capture full and accurate records of any significant business transaction, proportionate to business need, undertaken in the course of their official duties. This includes, but is not limited to:

- evidence of decisions, approvals, financial records, agreements and contracts;
- providing advice, instructions or recommendations;
- drafts of documents for the Institute containing significant annotations or submitted for comment or approval by others;
- correspondence received and sent relating to their work undertaken for the Institute.

Records are created, captured and managed digitally (digitised records), unless authorised by the Chief Operating Officer (COO) to be retained in paper format. This will ensure information is more readily available and accessible.

Institute paper records will be stored in designated storage areas with access restrictions in accordance with the Institute's Records and Information Management Procedure (E15/13547).

These records will be created, captured and assigned the appropriate Institute business classification in a recordkeeping system approved by the Chief Information Officer (CIO), who is appointed as the Senior Responsible Officer for records and information management. HP Records Manager (HPRM) and departmental files are the Institute's official recordkeeping system.

Rarely used records or records that are no longer in use for official purposes that are still required are to be retained in accordance with the relevant General and Functional Retention & Disposal Authority.

2.4 Access to Records & Information

Records will be accessible to all authorised staff that requires access to them for business purposes. Reasons for restricting access are outlined in the Institute's Records and Information Management Procedure (E15/13547) and appropriate security controls are to be applied to records of a sensitive or confidential nature.

Access to records and information will be managed appropriately in accordance with legal and business requirements.

Access to the Institute's records by members of the public, may be obtained under the:

- *Government Information (Public Access) Act (GIPA)*,

- *Privacy and Personal Information Protection Act (PPIPA)*,
- *Health Records and Information Privacy Act (HRIPA)*, or
- *State Archives and Records Act 1998*.

Regardless of the format, records must be accessible over time.

2.5 Security & Protection of Records & Information

The Institute's records must be securely protected from unauthorised or unlawful:

- access,
- destruction,
- loss, deletion, or
- alteration.

The Institute is required to identify systems which hold high risk and/or high value records and information. Any risks to information must be identified, managed or mitigated. For more information, refer to Risk Management Policy (E07/27229).

The Institute has implemented a number of security measures, including information security policies, as part of its Information Security Management System (ISMS), for safeguarding its information assets in accordance with the Information Classification and Labelling Guidelines (E14/02843).

Staff must abide by these measures at all times.

2.6 Ownership of Records

Records created, received, managed or stored by, or on behalf of the Institute, are owned by the Institute, not by individuals or specific divisions.

All records created by contractors performing work on behalf of the Institute belong to the Institute and are records under the State Archives and Records Act 1998. This includes the records of contract staff working on the premises as well as external service providers.

Contracts should clearly state that ownership of records resides with the Institute Records, where relevant, and instructions included regarding creation, management, and access to the records created.

2.7 Transfer & Archiving of Records

The Institute will transfer all records required as State archives to State Archives and Records NSW when they are no longer in use for official purposes.

Confidential records must be transported securely and stored in secure locations with access limited to authorised users.

All records being transferred to any other agency must be coordinated through the Chief Information Officer (CIO) and the Information Management Specialist (Records Management Program Lead), who are responsible for transfer procedures for records.

2.8 Maintenance, Monitoring & Management of Records

2.8.1 Maintenance of Records

Records must be appropriately maintained, stored and preserved for as long as the record is required.

The Institute will test or audit systems to ensure that:

- they are operating routinely, and
- there are no issues affecting information integrity, useability or accessibility.

2.8.2 Monitoring of Records

The Institute will:

- cooperate and liaise with State Archives and Records NSW in relation to monitoring compliance; and
- monitor and review records and information management to ensure that it is:
  - implemented,
  - accountable,
  - meets business needs, and
  - complies with the State Archives and Records Act and associated standards and codes of best practice.

2.8.3 Management of Records

The Institute will:

- recognise and address the importance of managing all records and information across all operating environments, including:
  - diverse system environments, and
  - physical locations.
- safeguard, manage and preserve records and information with long term value (digital and physical records), ensuring they are stored in a hazard-free and secure environment;
- assess and address records and information management in all outsourced, cloud and similar service arrangements;
- address the migration of records and information through system and service transitions; and
- take retention and disposal requirements for records and information into account when decommissioning any system containing records.

2.9 Retention & Disposal of Records

The Institute must retain records and information for as long as they are required to meet business, accountability and community expectations. Records and information are also kept (sentenced) and disposed of in accordance with the Retention and Disposal

Authority of the State Archives and Records Act 1998 and requirements under the State Archives and Records Regulations 2015 - Normal Administrative Practice (NAP) Guidelines.

The Institute has an authorised functional retention and disposal authority – State Archives and Records Authority of NSW – Cancer Institute NSW Functional Retention and Disposal Authority (DA 204) and State Archives and Records General Disposal Authorities including, but not limited to:

- GA28 – Administrative Records.
- GA31 – Royal Commissions, Special Commissions of Inquiry, Commissions of Inquiry.
- GA33 – Source Records that have been migrated.
- GA35 – Transferring records out of NSW for storage with and maintenance by service providers based outside of NSW.
- GA44 – Statewide health services, quality assurance, reporting, education and training.
- GA45 – Original or source records that have been copied.
- GDA11 – Audio visual programs and recordings.
- GDA17 – Patient/Client Records.

The disposal of records must be endorsed by the relevant Director, documented and approved by the COO and managed by the Information Management Specialist (Records Management Program Lead).

The guidelines for the disposal of Institute records are outlined in the Institute's Records and Information Management Procedure (E15/13547).

2.10 Business Continuity Strategies & Plans for Records & Information

The Institute will develop and maintain business continuity strategies and plans for records and information.

For more information, refer to Business Continuity Management Policy (E12/28428) & ICT Recovery Plan (E15/21826).

3 Roles and Responsibilities

3.1 Chief Cancer Officer

The Chief Cancer Officer (CCO) has a duty under Section 10 of the State Archives and Records Act 1998 to ensure that the Institute complies with the requirements of the Act and its regulations.

The CCO has delegated functions to the Chief Operating Officer (COO), Chief Information Officer (CIO), and division management and staff (as detailed below).

3.2 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Approving policies relating to the records and information management program.
- Ensuring the Institute complies with requirements of the State Archives and Records Act 1998 and other statutory requirements relating to records & information management recordkeeping.
- Ensuring the Institute complies with proactive release of information contained in records.
- Imposing and lifting legal holds relating to the destruction of records.
- Approving rules relating to the disposal of records, including the transfer of management responsibility for records to new entities.
- Assigns responsibilities to the Senior Responsible Officer (SRO) for the oversight of records and information management.

3.3 Chief Information Officer

The Chief Information Officer (CIO) is the Senior Responsible Officer (SRO) in terms of the State Archives and Records Act 1998; has the strategic and managerial responsibility for records and information management, and is responsible for:

- Ensuring the development and implementation of a strategic records and Information management program.
- Approving procedures relating to the Records & Information Management Program.
- Ensuring that records and information management is in place within the Institute and operating effectively to support business operations.
- Ensuring that the policy is reviewed annually, or sooner, if required and takes into account changes in business activities and priorities.
- Assessing that business systems and applications used by the Institute to store records are capable of managing records and meet the requirements of this policy.
- Ensuring business systems and applications that manage Institute records are assigned an appropriate business owner.
- Interpreting emerging and changed regulatory requirements in relation to the records and information management program.
- Ensuring resources are adequate for the records and information management program.
- Ensuring that support and infrastructure is provided for the management of electronic records in business systems and applications.
- Assigns responsibilities to business owners and business units to ensure that records and information management are integrated into work processes, systems and services.

- Assigns responsibilities to records and information management staff, including the development and implementation of records and information management strategies.
- Assigning responsibility to perform routine and comprehensive system backups and migration of electronic records.

3.4 Directors

The Directors are responsible for:

- Providing direction and support for records and information management and ensuring compliance in accordance with Section 10 of the State Archives and Records Act 1998.
- Designating at least one staff member from each business area or unit to act as a Records Champion.
- Endorsing the disposal of records, including their destruction/deletion, transfer to secondary storage and/or State Archives.

3.5 Division (Business and Program) Managers

Division (Business and Program) Managers are responsible for:

- Supporting the creation, capture, storage and monitoring of records by staff as part of normal business practice. This includes ensuring staff are adequately trained, use approved business information systems and are aware of their responsibilities.
- Ensuring that their service providers manage and maintain information that are records in accordance with this policy.
- Ensuring that systems that capture records comply with recordkeeping requirements.

3.6 Information Management Specialist (Records Management Program Lead)

The Information Management Specialist is the Institute’s Records Management Program Lead and responsible for:

- Managing the records and information management program, including:
  - Developing a recordkeeping framework with policies, procedures and guidelines, and
  - Providing advice, support and training to enable Institute staff to meet their responsibilities under records and information management legislation.
- Managing and documenting the design and use of HPRM, the Institute’s Electronic Document and Records Management System (EDRMS), classification schema and retention disposal authority.
- Regular liaison with owners of business systems to ensure that records and information management are integrated into work processes, systems and services.

- Reporting and liaising with external organisations on recordkeeping matters and providing guidance on records and information management best practices.
- Developing strategic and operational plans for the records and information management program, including key performance indicators to measure and monitor the performance of the Institute's records and information management program.
- Approving and managing storage areas and storage providers for paper records.
- Lead and manage any working groups under the records and information management governance framework.

3.7 Records Champions

Records Champions are appointed by Directors and are responsible for:

- Coordinating operational record keeping activities within their division and/or office.
- Representing the division/business area on the Institute's records and information management working group and providing division and program requirements for the records and information management program.
- Ensuring that practices and systems in their programs and units comply with this policy and any related requirements.
- Promoting and advocating best records practice collectively and within their own division/business area including recordkeeping guidance to new staff on specific division and/or program's recordkeeping procedures.

3.8 All Staff

All staff (including contractors and temporary employees) are responsible for:

- Complying with the records and information management policy and procedures.
- Creating full and accurate records of activities and business decisions.
- Using approved business systems and applications to capture and manage records.
- Ensuring all records (both received and sent) that are registered in the official recordkeeping system or approved, compliant business information systems, comply with Institute policies and procedures.
- Sharing and reusing records to support collaboration, knowledge transfer and consistent decision-making.
- Protecting sensitive and private records, and safeguarding records from unauthorised access, or accidental or deliberate loss or damage.

4 Glossary

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

Term	Definition
BYOD	Bring Your Own Device.

Term	Definition
Capture	A deliberate action which results in a record being placed on a registered file or the registration of a document into a recordkeeping system. For certain business activities, this action may be designed into digital systems so that the capture of records is concurrent with the creation of records.
CCO	Chief Cancer Officer.
CIO	Chief Information Officer.
COO	Chief Operating Officer.
Digital records	Digital information, captured at a specific point in time that is kept as evidence of business activity. The term 'digital records' covers 'born digital' records such as emails, web pages, digital photographs, digital audio files and database records as well as scanned versions of paper records that have been digitised in business processes.
Digitised records	When paper formats are digitised and action is based on viewing the digital image, the digital format is considered the record, not the paper. The paper record will be considered a convenience copy and will be destroyed after quality assurance processes are complete.
Disposal	A range of processes associated with implementing appraisal decisions that are in accord with approved retention and disposal authorities. These include the retention, deletion or destruction of records. They may also include the migration or transmission of records between recordkeeping systems, and the transfer of custody or ownership of records.
Disposal Authority	A policy for the retention and disposal of records approved by the State Archives and Records NSW Advisory Committee.
EDRMS	Electronic Document and Records Management System.
Electronic records	Refer to 'Digital records'.
GA	General Authority.
GDA	General Retention and Disposal Authority.
GIPA	Government Information Public Access Act.
HPRM	HPRM is the corporate recordkeeping system and is used to capture, maintain and provide access to Institute records.
HRIPA	Health Records & Information Privacy Act.

Term	Definition
ICT	Information Communication & Technology.
ISMS	Information Security Management System.
NAP	Normal administrative practice (NAP) is a process that allows agencies to destroy certain types of low-value and short-term information in the normal course of business.
Official record	Recorded information in any form, including data in computer systems, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.
PPIPA	Privacy and Personal Information Protection Act.
Record	A record is defined in the State Archives and Records Act of NSW as: *"Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Records are evidence of business conducted by an organisation."* A record can be: • an individual information asset (e.g. a document, an email, an image, a video, a sound recording), a piece of data (e.g. a date of birth), or • a collection of information assets (e.g. a folder of documents, a box of folders, a dataset, a registry).
Records & information management Program	A planned and coordinated set of policies, procedures, people, systems and activities that are required to manage records.
Recordkeeping system	Any compliant business information system that captures, maintains and provides access to records over time as defined by State Archives and Records NSW.
Registration	The act of giving a record a unique identifier upon entry into a system. The primary purpose of registration is to provide evidence that a record has been created or captured in a recordkeeping system, with the benefit of facilitating retrieval and access.
Staff	Includes permanent, casual, contractors or consultants, working in full-time or part-time capacity, at all levels of the Institute.
SRO	Senior Responsible Officer.
The Institute	Cancer Institute NSW.