Government of Western Australia
Department of Health

Information Lifecycle Management Policy

Delivering a **Healthy WA**

TITLE: INFORMATION LIFECYCLE MANAGEMENT POLICY

1. BACKGROUND

WA Health collects, stores, uses and discloses large volumes of information. The information is an important resource used for the clinical care of patients, for funding, management, planning, monitoring, improvement, research and evaluation of health and health services in the State.

The information lifecycle depicts the sequence of operational activities for managing information from creation until disposal. The activities within the information lifecycle are collection, storage, access/disclosure, use and disposal. Managing information through each phase provides WA Health the ability to monitor and effectively manage patient care, strategic and operational resources and meet legislative requirements.

The term 'data' generally refers to unprocessed information, whilst the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. For the purpose of this policy, the terms data and information have been used interchangeably and should be taken to mean both data and information.

2. POLICY

This policy applies to all data collections, including those provided for by statute, held by or within WA Health. For the purpose of this policy, data collections include both operational data collections and data repositories that are stored in electronic or non-electronic (i.e. paper based) formats. It includes collections of patient information, corporate, financial and workforce information where one or more of the following conditions are met:

- the data collection is used to meet business, operational and legislative requirements
- the State of Western Australia has a strategic need for the data
- the data collection contains personal health information
- the data collection is used for reporting at a state level, national level or external to the health service where the data collection resides
- the data collection is used across multiple health services.

The purpose of the *Information Lifecycle Management Policy* is to outline the phases information goes through and to document best practice to ensure information held within WA Health is managed efficiently and effectively over time to meet its legal, professional and ethical responsibilities.

The following practices must be applied to all information within scope.

2.1 Collection

Collection is the creation, acquisition or capture of the information needed to support business, operational and legislative requirements.

The collection phase of information lifecycle management is probably the most important phase. If the design and creation of data is poorly planned this can result in information

being inadequate, excessive and not fit for the purpose intended. Data collections should be created and managed in accordance with the *Data Collection Policy (OD 0381/12)*.

Prior to collecting information it is important to ensure that:

- information is only collected where there is a legitimate business purpose that is aligned with WA Health's strategic intent
- the importance and benefits of the information outweigh the costs of the collection in terms of resources expended by WA Health
- the availability of existing data sources have been explored and used where possible
- a governance process is in place, including the allocation of a Data Steward and Data Custodian (refer to *Data Stewardship and Custodianship Policy OD 0487/14*)
- relevant approvals have been sought to commence data collection (refer to *Data Collection Policy OD 0381/12*)
- a contract has been developed and approved when a third party is collecting information on behalf of WA Health.

When collecting information it is important to ensure that:

- data requirements within the collection are clearly documented to ensure the information is relevant for the required use
- information is classified in terms of sensitivity and risk to WA Health (refer to *Information Classification Policy OD 0537/14*)
- information is collected in an ethical manner, taking into consideration the rights and privacy of individuals
- appropriate metadata is documented about the purpose, processes and methods involved in data collection (refer to *Metadata Documentation Policy OD 0464/13*)
- accountability and responsibility for data quality is managed in accordance with the *Data Quality Policy (OD 0380/12)*.

2.2 Storage

Storage relates to the retention and ongoing management of information to ensure its continuing value, security and timely availability.

Once the information is created and collected, it must be stored in a manner that best supports business processes, whilst protecting the confidentiality and integrity of the information. The *Information Storage and Disposal Policy (OD 0407/12)* contains detailed information about the storage and ongoing retention of WA Health information and must be read in conjunction with this policy.

To determine the appropriate storage media and format, factors such as retention period, security and classification of the information must be considered. In determining the correct retention period, the following policies will assist staff:

- Administration, Human Resources and Financial and Accounting Records – *General Disposal Authority for State Government Information GDA 2013-017*
- Patient Records - *Patient Information Retention and Disposal Schedule version 3, 2008 (OD 0133/08)*.

Security measures for confidential and protected information must be implemented to ensure data is not lost or accessed by unauthorised personnel. To ensure the appropriate protection and security mechanisms for information, the following policies are available:

- *Acceptable Use Policy – Information and Communication Technology (OD 0468/13)*

- *Information & Communications Technology (ICT) Physical & Environmental Security Policy (OD 0506/14)*
- *Information Security Policy (OD 0389/12)*
- *IT Service Continuity as Related to the Management of Electronic Records Policy (OP 1877/04)*
- *Long Term Management of Electronic Records Policy (OP 1872/04)*
- *Mobile Computing Devices Policy and Guidelines (OD 0336/11)*.

Data should be classified in terms of its sensitivity and risk to WA Health. The classification assigned determines how the information must be stored and protected. For further information refer to the *Information Classification Policy (OD 0537/14).*

2.3 Access and Disclosure

Information access and disclosure ensures that information is readily available to authorised users in a secure, consistent and controlled manner.

WA Health is committed to ensuring information that supports the provision of health care is readily available to authorised users when and where it is needed; however confidential information must also be protected from unauthorised access and disclosure.

The *Information Access and Disclosure Policy (OD 0539/14)* documents the requirements for sharing WA Health information. The policy outlines two provisional models for controlling the access and disclosure of information to authorised users (both internal and external to WA Health). The models outlined in the policy must be applied to all data collections within scope. The policy also addresses the roles and responsibilities of the Data Steward and Custodian(s) with respect to the sharing of WA Health information.

Other policies and guidelines that address the access to and disclosure of information include:

- *Guidelines for the Release of Data (IC 0125/12)*
- *Patient Confidentiality (IC 0164/13).*

2.4 Use

Use refers to the responsible, ethical and lawful utilisation of information to meet business, operational and legislative requirements.

As outlined in the *Information Use Policy (OD 0390/12)*, the following principles must be adhered to when using WA Health information:

- Information must only be used for the purpose specified. The purpose of the information requested must be outlined within the initial request.
- Information provided must be limited to the minimum required to meet the purpose specified.
- Before using any information, the context of the information must be understood by the user. For example: currency, completeness, format, limitations, values and quality.
- Information must not be used by a person other than the person(s) authorised. This is to ensure that WA Health's information is only used by the person(s) outlined in the original request.

- Information must not be used to identify or contact any individual unless this is for an approved purpose.
- Information must not be merged with any other information without prior approval from the Data Custodian.
- The information must be protected by appropriate and approved security measures.
- All personnel using the information must take reasonable steps in ensuring protection against theft, loss, unauthorised access, use, disclosure and unauthorised copying or modification.
- The information must not be kept for longer than approved without prior consent from the Data Custodian.
- The information must be appropriately disposed of in accordance with relevant disposal authorities (refer to *Information Storage and Disposal Policy OD 0407/12)*.

For third parties using WA Health information, a contract must be developed outlining their obligations. The following elements must be addressed within the contract:

- ownership of data
- access arrangements by the third party to WA Health's information
- disclosure arrangements of WA Health's data by the third party
- retention, storage and security of the information
- WA Health's audit requirements
- process for contract expiry or termination
- disposal of information after the contract expires.

2.5 Disposal

Disposal involves the appropriate removal or archiving of data in accordance with recordkeeping requirements.

Data collections must be stored for a minimum retention period before they may be disposed. The *Information Storage and Disposal Policy (OD 0407/12)* outlines the relevant legislation, policies and procedures concerning the retention and destruction of WA Health information.

For further information about the correct timeframes and methods for disposal refer to:

- Administration, Human Resources and Financial and Accounting Records –
- Electronic Records - *Long Term Management of Electronic Records Policy (OP 1872/04)*
- ICT equipment containing information - *Disposal of ICT Equipment Policy* and *Information Security Policy (OD 0389/12)*
- Patient Records - *Patient Information Retention and Disposal Schedule version 3, 2008 (OD 0133/08)*.

In all instances where data or ICT equipment containing information, considered to be original under a recordkeeping plan, is destroyed, an information register or log should be made to capture details of each individual record destroyed (refer to *Information Storage and Disposal Policy OD 0407/12*).

3. DEFINITIONS

Authorised User	individuals (internal and external to WA Health) authorised by the relevant Data Custodian to access information within a specific WA Health data collection.
Confidentiality	the ethical principle or legal right that a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure.
Data	is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning WA Health general business, information systems, employees, business partners, patients or customers, including information and entity types.
Data Collection	refers to the systematic gathering of data for a specific purpose from various sources, including manual entry into an application system, questionnaires, interviews, observation, existing records and electronic devices. It includes collections of patient, corporate, financial and workforce information. This includes both operational data collections and data repositories.
Data Custodian	the person(s) responsible for the day-to-day management of data from a business perspective. The Data Custodian aims to improve the accuracy, usability and accessibility of data within the data collection.
Data Repository	refers to data that is collected from various sources, including operational data collections for the primary purpose of monitoring, evaluation, reporting and research. Examples of data repositories include data held within the Hospital Morbidity Data Collection, Finance Data Warehouse and the Emergency Department Data Collection.
Data Steward	is a delegated person responsible for setting the overall strategic direction of a specific data collection. They ensure the collection is developed, maintained and utilised in accordance with the strategic goals of WA Health. Data Stewards are also responsible for authorising access, use and disclosure of data from the data collection for clearly defined purposes that comply with WA Health's statutory obligations.
Duty of Confidentiality	is an element of common law that prevents the disclosure of information to individuals and organisations not involved in the particular health care process.
Information	refer to Data.
Information Access	in the context of this policy refers to the direct access by authorised users (both internal and external to WA Health) to information within WA Health's data collections. Typically, direct access is gained via a network and/or system login and password to a front-end information system or to a back-end database.
Information Disclosure	in the context of this policy refers to the release of information from WA Health's data collections to authorised users (both internal and external to WA Health). Information is generally

	released in a form of hard copy documents, data extracts or electronic medium.
Information Management	is the discipline that directs and supports effective and efficient management of information in an organisation. Holistic, effective management of information requires mobilisation of three enterprise capabilities: people, processes (policies and procedures) and technology.
Operational Data Collection	includes data that is collected as part of the day-to-day activities of an area for the primary purpose of tracking and managing the operational aspects of the area. The operational data collection is typically a transaction-based system which contains detailed data elements to represent the activities of the area. Examples of operational data collections include data held within Patient Administration Systems, TRIM, Financial Systems and Human Resource Management Systems.
Personal Health Information	pertains to all health information where the identity of a person is apparent or can reasonably be ascertained from the information itself. Information is also personal information if it is reasonably possible for the person receiving the information to identify the individual by using other information that they already hold.
Security	is the preservation of confidentiality, integrity and availability of information.
WA Health	incorporates the legal entities of the Metropolitan Health Service, WA Country Health Service, Department of Health and the administrative entities of Child and Adolescent Health Service, North Metropolitan Health Service and the South Metropolitan Health Service.

4. ROLES AND RESPONSIBILITIES

4.1 Data Steward

Data Stewards are responsible for setting the overall strategic direction of a specific data collection. They ensure the collection is developed, maintained and utilised in accordance with the strategic goals of WA Health. Data Stewards are also responsible for authorising access, use and disclosure of data.

4.2 Data Custodian

Data Custodians are responsible for managing information through its lifecycle, from creation until disposal, in a manner that complies with relevant legislation, policies, guidelines and procedures governing the information lifecycle.

4.3 Authorised User

Authorised users of WA Health information are responsible for protecting the security and integrity of data within their possession. They must ensure that all information (in electronic or non-electronic format) is collected, stored, accessed, disclosed, used and disposed of appropriately and in accordance with the relevant policies, procedures and contractual obligations pertaining to the lifecycle sequence.

5. COMPLIANCE

Compliance with the Operational Directive is mandatory for all employees of WA Health. Authorised users who breach confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the *Public Sector Management Act 1994* and the *Criminal Code Act 1913*. Unauthorised access, use and disclosure of confidential information is misconduct pursuant to the *WA Health Code of Conduct* and suspected cases may be reported to the Corruption and Crime Commission in accordance with the *WA Health Misconduct and Discipline Policy (OD 0323/11).*

6. EVALUATION

In order to ensure currency and ongoing relevance to WA Health, this policy will be reviewed every 3 years by the Information Development and Management Branch (IDM) within the Resourcing and Performance Division.

7. RELATED DOCUMENTS

Acceptable Use Policy – Information and Communications Technology (OD 0468/13)
Data Collection Policy (OD 0381/12)
Data Quality Policy (OD 0380/12)
Data Stewardship and Custodianship Policy (OD 0487/14)
Disposal of ICT Equipment Policy
General Disposal Authority for State Government Information GDA 2013-017
Guidelines for the Release of Data (IC 0125/12)
Information Access and Disclosure Policy (OD 0539/14)
Information and Communication Technology (ICT) Physical and Environmental Security Policy (OD 0506/14)
Information Classification Policy (OD 0537/14)
Information Security Policy (OD 0389/12)
Information Storage and Disposal Policy (OD 0407/12)
Information Use Policy (OD 0390/12)
IT Service Continuity as Related to the Management of Electronic Records Policy (OP 1877/04)
Long Term Management of Electronic Records Policy (OP 1872/04)
Metadata Documentation Policy (OD 0464/13)
Mobile Computing Devices Policy and Guidelines (OD 0336/11)
Patient Confidentiality (IC 0164/13)
Patient Information Retention and Disposal Schedule Version 3, 2008
WA Health Misconduct and Discipline Policy (OD 0323/11)

8. RELEVANT LEGISLATION

Children and Community Services Act 2004
Commonwealth Privacy Act 1988 (Australian Privacy Principles)
Coroners Act 1996
Corruption and Crime Commission Act 2003
Criminal Code Act 1913
Electronic Transactions Act 2011
Evidence Act 1906, Acts Amendment (Evidence) Act 2000
Financial Management Act 2006
Freedom of Information Act 1992

Freedom of Information Regulations 1993
Health Act 1911
Health and Disability Services (Complaints) Act 1995
Health Legislation Administration Act 1984
Hospital and Health Services Act 1927
Human Reproductive Technology Act 1991
Mental Health Act 1996
National Health and Medical Research Council Act 1992
Public Sector Management Act 1994
State Records Act 2000

This page is intentionally left blank

This document is available in different formats, upon request from a person with disability.