Information Lifecycle Management Policy

1. BACKGROUND

In the course of its operations, WA Health collects, stores, uses and discloses large volumes of data. The data 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 that all data collections go through in their existence. The activities within the information lifecycle are collection, storage, access/disclosure, use and disposal. Managing information through each phase of the lifecycle provides WA Health the ability to monitor and effectively manage patient care, strategic and operational resources and 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. SCOPE

This policy applies to all data collections, including those provided for by statute, held by or within WA Health. 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 or legislative requirements.
- The State of WA has a strategic need for the information.
- The data collection contains personal information.
- The data collection is used for reporting at a state level, national level, organisation wide or externally.
- The data collection is used across multiple health services.

The scope of this policy includes both paper based (including paper medical records) and electronic information.

For the purpose of this policy, a data collection includes both operational data collections and data repositories.
3. PURPOSE

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

4. POLICY

The following practices must be applied to all data collections within scope.

4.1 Collection

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

Prior to collecting data it is important to ensure that:

- Information is only collected when there is a legitimate business purpose that is aligned with WA Health’s Strategic intent.
- There is a governance process in place including a Data Steward and Data Custodian. Refer to OD0321/11 Data Stewardship and Custodianship Policy.
- The importance and benefits of the data collection must outweigh the cost of the collection in terms of resources expended by WA Health.
- Data requirements within the collection must be clearly documented to ensure the data is relevant for the required use.
- The data is classified in terms of sensitivity and criticality to WA Health. Refer to OD 0304/10 Information Classification Policy.
- Data is collected in an ethical manner taking into consideration the rights and privacy of individuals.
- The integrity of data within the collection is preserved and protected by ensuring that the data is stored in a secure environment.

When third parties are collecting data on WA Health’s behalf a contract between WA Health and the third party must be developed. Types of contracts include Memorandum of Understanding (MOU) and Service Agreements. These contracts ensure the confidentiality and security of the data.

The following elements must be outlined within the contract to ensure:

- ownership of data;
- storage and security of data;
- retention of data - in accordance to WA Health record keeping plan and State Legislation;
- WA Health’s audit requirements; and
- disposal of data after the contract expires.
4.2 Storage

Data storage relates to retention of data, in an appropriate manner, to support business, operational or legislative requirements.

Once the data is collected and created, it must be stored in a manner that best supports business processes. To determine the appropriate storage media and format, factors such as retention period, security and classification of the data must be addressed.

In determining the correct retention period, the following policies will assist staff:

- Aboriginal and Torres Strait Islander people records – OD0051/07 Retention of Records Relating to Aboriginal and Torres Strait Islander People.

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

- Electronic – Information Security Policy.
- Physical Environment of computers used to stored information - Physical and Environmental Security Standard.
- Database security - Database Administration Standard.

Data should be classified in terms of its sensitivity and criticality to WA Health. The classification assigned determines how the information must be stored. For further information please refer to OD0304/10 Information Classification Policy.

4.3 Access and Disclosure

Information access and disclosure ensures only authorised users have access to non-public information in order to achieve business, operational or legislative requirements.

WA Health needs to ensure the right information is available to authorised users at the right time and place to enable effective clinical and management decision making. Data Stewards and Data Custodians are the critical gatekeepers who ensure access to information is only given to authorised users.

The Data Steward is responsible for:

- Overseeing the development of a role based Information Access Control model that specifies the types of users who can access the data collection and the level of access permitted. This model may be developed by the Data Custodian with endorsement by the Data Steward.
• Overseeing the development of an Information Disclosure model which specifies the level of approval required prior to releasing information from the data collection based on the granularity and sensitivity of the information requested. This model may be developed by the Data Custodian with endorsement by the Data Steward.

Data Custodians are responsible for:
• Implementing the Information Access Control model and Information Disclosure model. Further details on developing and implementing these control models can be found in the OD0360/12 Information Access and Disclosure Policy.
• Ensuring the recipient of the data fully understands the conditions of data release and their related obligations. The Data Custodian administers this by signing a Data Release contract with the recipient of the data. This is particularly important when releasing confidential and/or sensitive data. The contract describes limitations on the usage of the data, security and storage requirements as well as restrictions on further dissemination of the data to third parties.

4.4 Use
Data use refers to the appropriate utilisation of data to achieve business, operational or legislative requirements.

When using WA Health data, the following practices must be adhered to:
• Data is used only for the purpose specified.
• Data must not be used by a person other than the person with authorised access.
• Data must not be used to identify or contact any individual unless this is an approved purpose.
• Data must not be merged with any other information without prior approval from the Data Steward and/or Data Custodian.

For third parties using WA Health data a contract must be developed outlining the obligations of the third parties in using WA Health’s data. The following elements must be outlined within the contract:
• access arrangements within the third party to WA Health’s data;
• disclosure arrangements of WA Health’s data by the third party;
• retention, storage and security of data;
• WA Health’s audit requirements; and
• disposal of data after the contract expires.

4.5 Disposal
Data disposal involves the appropriate removal or archiving of data that is no longer required to meet statutory requirements, support business or operational requirements.

Superseded by:
OD: 0557/14
September 2014
When considering the destruction of data, the following policies are relevant to ensure the timing of destruction and the correct method used:

- **Aboriginal and Torres Strait Islander people records** – OD0051/07 Retention of Records Relating to Aboriginal and Torres Strait Islander People.
- **Administrative and Functional records** – Retention and Disposal Schedule for Administrative and Functional Records.
- **Electronic Records** – OP 1872/04 Long Term Management of Electronic Records Policy.
- **Information & Communications Technology (ICT) equipment containing information** - Disposal of ICT Equipment Policy.

In all instances where data, or ICT equipment containing data, is destroyed, a log should be made that contains the following:

- the title of data;
- when it was destroyed;
- who destroyed it;
- how it was destroyed; and
- who approved the destruction.

### 4.6 National Aboriginal and Torres Strait Islander Health Data Principles

In October 2006 the Australian Health Ministers’ Advisory Council (AHMAC) endorsed the ‘National Aboriginal and Torres Strait Islander Health Data Principles’. These 11 principles set out a culturally respectful foundation for the collection, storage and use of Aboriginal health and health related information.

The National Aboriginal and Torres Strait Islander Health Data Principles should be applied, where applicable when creating, reviewing or modifying a data collection.

### 4.7 Management of Personal Information – Good Practice and Opportunities for Improvement – Western Australian Ombudsman

On 28th March 2011 the Ombudsman published a report, “The management of personal information – good practice and opportunities for improvement”, following an investigation of selected State Government agencies that deal with large amounts of personal information.

Good practice principles were developed to assist Government Agencies in managing personal information they collect and hold. These principles are based on national and state legislative requirements, agency-specific legislation and internationally accepted good practice.

These principles should be reviewed and applied (if applicable), in conjunction with all WA Health Information Management policies.
5. DEFINITIONS

A **Data Collection** is a systematic gathering of data for a particular purpose from various sources, including manual entry into an information system, questionnaires, interviews, observation, existing records and electronic devices. This includes both operational data collections and data repositories.

**Data Custodians** are 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 with the data collection.

**Data Stewards** have delegated responsibility for setting the overall strategic direction of the specific data collection to 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.

A **Data Repository** includes data that are 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.

**Information Access** in the context of this policy refers to the direct access by end users (both internal and external to WA Health) to information within an organisation. 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 to end users (both internal and external to WA Health) from data collections or paper based records within an organisation. 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.

An **Operational Data Collection** includes data that are 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.
6. ASSOCIATED POLICIES

- Data Stewardship and Custodianship Policy OD 0321/11
- Information Classification Policy OD 0304/10
- Information Access and Disclosure Policy OD 0360/12
- Patient Information Retention and Disposal Schedule Version 3, 2008 OD 0133/08
- Retention of Records relating to Aboriginal and Torres Strait Islander People OD 0051/07
- Retention and Disposal Schedule for Administrative and Functional Records
- Long Term Management of Electronic Records Policy OP 1872/04
- Information Security Policy
- Mobile Computing Devices Policy and Guidelines
- Physical and Environmental Security Standard
- Database Administration Standard
- Disposal of ICT Equipment Policy

7. RELEVANT LEGISLATION

- Health Act 1911
- Health Services (conciliation and review) Act 1995
- Hospital and Health Services Act 1927
- Human Reproductive Technology Act 1991
- Mental Health Act 1996 (WA)
- Freedom of Information Act 1992
- Public Sector Management Act 1994
- State Records Act 2000
- Privacy Act 1988 (Cth) and the National Privacy Principles (NPP)

8. SUPPORTING DOCUMENTS

Australian Health Ministers’ Advisory Council (AHMAC)
‘National Aboriginal and Torres Strait Islander Health Data Principles’

Management of Personal Information – Good Practice and Opportunities for Improvement – Western Australian Ombudsman