Government of **Western Australia**
Department of **Health**

Data Stewardship and Custodianship Policy

health.wa.gov.au

Effective: 01 July 2016

Title: Data Stewardship and Custodianship Policy

1. Background

In the course of its operations, WA Health collects, stores, uses and discloses a large volume of data including confidential health and business information. 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 Western Australia.

The State of Western Australia is the owner of all data collected by and within WA Health irrespective of the method of storage or size of the collection. WA Health has a legislative responsibility to protect the confidentiality of this information and to respect the privacy of those individuals to whom it relates. The allocation of Data Stewards and Data Custodians to data collections will ensure accountability for the management, security, quality and timely availability of data, while ensuring compliance with the Information Management Policy Framework. The Framework provides a coherent set of principles, policies, standards and guidelines for managing information across all stages of the information lifecycle. Having clear data governance roles and responsibilities is a fundamental principle of the Framework.

2. Scope

This policy applies to, and is binding upon, each Health Service Provider and its staff members. The policy also applies to Contracted Health Entities to the extent that the Contracted Health Entities provide health services to the State. It also includes the Department of Health. This covers any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

This policy encompasses information stored in any format, such as hard copy (paper), electronic (digital), microform, audio, video, image, graphical, physical sample or numerical form, including unit record and aggregate data.

It includes collections of business and health information for which sound and accountable data governance practices are required. Accordingly, a Data Steward and Custodian must be formally assigned to data collections 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 data
- the data collection is used for reporting at a State level, national level or external to the Health Service Provider where the data collection resides
- the data collection contains health information or personal information
- the data collection is used across multiple Health Service Providers.

The following are excluded from the scope of this policy:

- data that are exclusively owned by external organisations or agencies although held by WA Health unless a formal agreement or contract states otherwise
- data that are collected by WA Health staff for the primary purpose of research
- data that are released outside of WA Health for research whether that research is conducted by persons who are staff members of the Health Service Provider or persons employed or engaged in the Department or other persons.

Data pertaining to research are the responsibility of the researcher(s) and must be managed in accordance with the conditions of data release, as well as ethics and site approval requirements (refer to Research Policy Framework).

3. Policy Statement

This policy mandates that a Data Steward and Data Custodian must be formally assigned to all data collections within scope and sets out the responsibilities for protecting the confidentiality, integrity and availability of the data.

Implementation of this policy and adherence to its requirements will facilitate compliance with the Information Management Policy Framework, which provides a coherent set of agreed policy standards and guidelines for effective information management.

4. Delegates Authorities

The State of WA is the legal owner of all data collected by, within and for WA Health. The Director General of the Department is the delegated owner of this data and is responsible for its security, management and legitimate use and disclosure.

Where powers and responsibilities for collection of data are assigned by statute they will be held and exercised in accordance with the relevant legislation and must only be delegated in accordance with the relevant legislation.

Where stewardship responsibilities for data collections are not assigned by statute, the Director General delegates a number of these responsibilities to senior officers of the Health Service Provider, as well as the Department. Delegations must be made in writing and must not be further delegated. These delegations are documented in the Authorities, Delegations and Directions Schedule (Delegations Schedule), which specifies the positions of Tier-level officers to whom delegated powers or authorisation have been granted.

Data Stewards are delegated overall accountability and responsibility for the data collection as outlined in section 13.1. Data Stewards are categorised as Tier 2A officers within the Department and at least Tier 2B within Health Service Providers.

5. Assignment of Stewardship

Information is collected in all formats, including hardcopy (paper), although the vast majority of information is ‘born electronic’ or converted into electronic formats and managed in an electronic information systems environment. Statewide information is typically collected and stored in Enterprise Systems, while information collected by the Department or the Health Service Provider for their specific requirements is stored in Local Systems. The assignment of data stewardship for Enterprise (i.e. statewide) and Local Systems, as well as Data Warehouses, is outlined below and applies to information in any format.

5.1. Enterprise Systems

Enterprise Systems are large-scale, integrated information systems comprising statewide data which support processes, information flows, reporting and data analytics across WA Health. Typically Enterprise Systems are transaction-based systems and are classified as Class 1 applications requiring 24 hour, 7 day per week availability and technical support. The Health Support Services (HSS) usually provide technical support and manage the hardware, maintenance and system development of Enterprise Systems. Business User Groups may provide business advice and direction to HSS.

Examples of Enterprise Systems include, but are not limited to, Emergency Department Information System (EDIS), iPharmacy, Medical Records Information Tracking System (MeRITS), Patient Administration System (webPAS), Theatre Management System (TMS) and Oracle – Financials, Alesco and Objective.

The Assistant Director General of the Purchasing and System Performance Division within the Department of Health is the Data Steward of data held within Enterprise Systems.

5.2. Local Systems

Local data collections are often held in small to medium scale information systems which support processes, information flows, reporting and data analytics within a local area, such as the Department of Health, Health Service Provider or hospitals within a Health Service Provider. Typically Local Systems are classified as Class 2 and 3 applications, requiring availability and technical support during business hours only.

Examples of Local Systems for Health Service Providers include, but are not limited to, Freedom of Information Register, Occupational Safety and Health at Work (OSH at work) and Vehicle Booking Systems.

The Department of Health Local Systems are used to meet business requirements, as well as mandatory reporting requirements typically associated with legislation or funding agreements. Examples include the Department's National Minimum Data Sets, such as the Elective Surgery Wait List, Emergency Department Data Collection and Hospital Morbidity Data Collection.

The Data Stewards for Local Systems are:

- Assistant Director Generals (Tier 2A) for the Department
- Chief Executives (Tier 1B), or an Executive Director (Tier 2B) that is nominated by their respective Chief Executive, for Health Service Providers.

5.3. Data Warehouses

A Data Warehouse integrates data, from many heterogeneous sources (i.e. various Enterprise and Local Systems) and stores them in an easily accessible central repository. A Data Warehouse is designed to support business decisions by facilitating the consolidation of data to support analysis and reporting at different aggregate levels. The integration of query, reporting and analysis tools provides users with the opportunity to efficiently extract critical data, as well as drill down and through the data for clinical and operational analytics. This capability provides a coherent picture of activity at a point in time and supports strategic and tactical decision making, while driving quality improvement and cost reductions.

The use or disclosure of data from any Enterprise or Local System for data warehousing purposes is subject to approval from the Data Steward, and may be dependent upon the applicant complying with a set of predefined conditions pertaining to access, use and disclosure of the data.

5.3.1. Statewide Data Warehouse

A Statewide Data Warehouse contains data extracted from multiple Enterprise and/or Local System(s) for more than one Health Service Provider.

The Assistant Director General of the Purchasing and System Performance Division within the Department of Health is the Data Steward of all Data Warehouses that comprise statewide data.

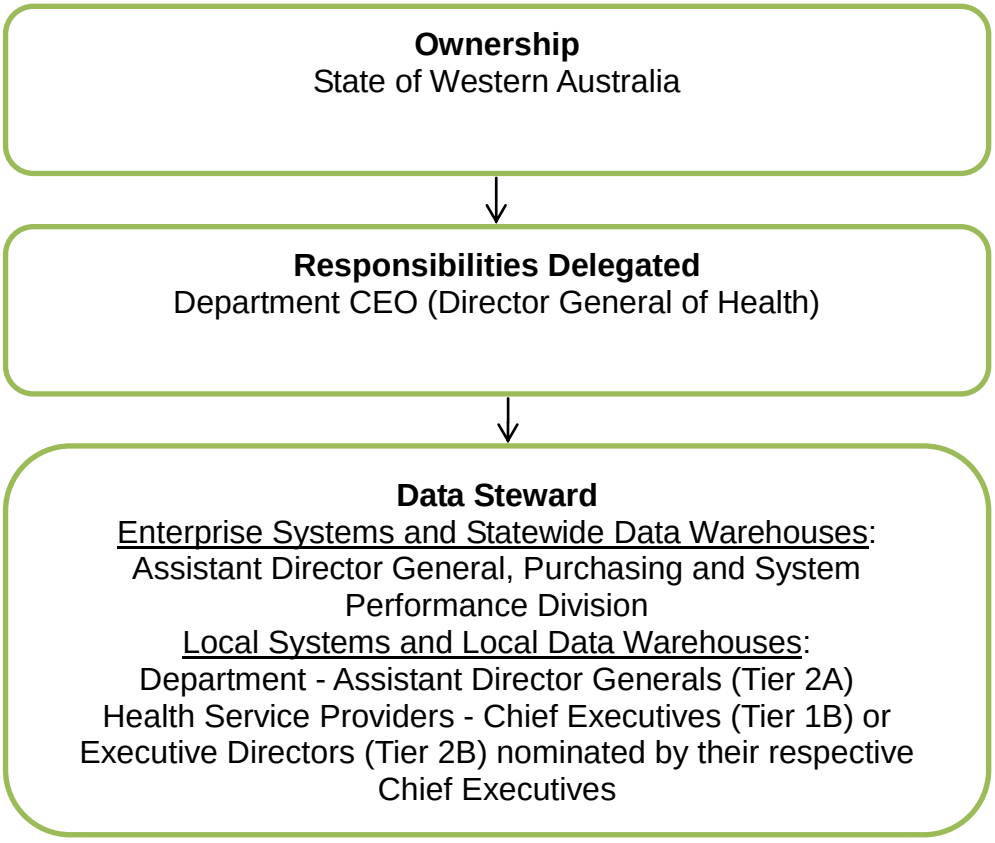
5.3.2. Local Data Warehouse

A Local Data Warehouse contains data extracted from multiple Enterprise and/or Local System(s) about a single Health Service Provider.

The Data Stewards for Local Data Warehouses are:

- Assistant Director Generals (Tier 2A) for the Department
- Chief Executives (Tier 1B), or Executive Directors (Tier 2B) nominated by their respective Chief Executives, for Local Data Warehouses.

Figure 1. Delegated Authority for WA Health Information



6. Criteria for Selecting Data Custodians

Data custodianship responsibilities for data collections must be assigned to a position rather than an occupant of a position (i.e. named person). Ensuring data custodianship is assigned to a position means that any occupant of the position, whether acting or substantive, is automatically entitled to exercise the responsibilities associated with the position.

The criteria for selecting the appropriate position for assigning custodianship include:

- competence, skills and authority to discharge the custodianship responsibilities
- understanding of the relevant legislative requirements and policy frameworks
- understanding of business needs of data users.

6.1. Assignment of Data Custodianship

Data Custodians are responsible for the day-to-day, as well as ongoing management, operation and support of the data collection (refer to section 13.2).

For Enterprise Systems, the Data Steward must nominate one Data Custodian for each Health Service Provider to ensure consistency in business processes and decisions. In this instance, all Data Custodians are expected to provide input and contribute to decisions about the data collection and are collectively responsible to the Data Steward.

For Local Systems, and Data Warehouses, the Data Steward must nominate at least one Data Custodian to manage the data collection. Data Stewards may prefer to nominate more than one Data Custodian. This may be preferable, for example, where a Local System is used across multiple sites of a Health Service Provider or to manage the disparate responsibilities of the Data Custodian's role. In these instances, Data Custodians are collectively responsible to the Data Steward and a Principal Data Custodian must be nominated by the Data Steward as the primary point of contact regarding the data collection.

Data Custodians may assign day-to-day tasks associated with their position to suitably qualified staff, but they remain responsible to the Data Steward.

6.2. Assignment of Data Custodianship Form

The assignment of custodianship must be in writing specifying details of the relevant data collection and the responsibilities allocated. The Data Custodian is responsible for completing the *Assignment of Data Custodianship Form* (Custodianship Form) (Attachment A) for the data collection. The Custodianship Form must be approved by the Data Steward, noting that the approval process varies for Enterprise Systems (Attachment B) and Local Systems (Attachment C).

After the Custodianship Form is approved by the Data Steward, details about the data collection (e.g. name, description, position of Data Steward and Data Custodian) are added to the WA Health Information Register (Information Register) by staff within the Purchasing and System Performance Division.

The Information Register is the official listing of all information assets, and is available on the Purchasing and System Performance Division intranet site for all staff to access. The Information Register is also available to researchers and the public via the Department's Human Research Ethics Committee internet site.

7. Establishing New Data Collections

Prior to establishing a new data collection, a Data Steward and Custodian must be appointed for the data collection. The Custodianship Form must be completed by the Data Custodian and approved by the Data Steward.

Approval to establish a new information system for data collection must also comply with WA Health's Information and Communications Technology (ICT) governance arrangements as outlined in the WA Health ICT Strategy 2015 – 2018 and requirements of the Information and Communications Technology Policy Framework.

8. Existing Data Collections

Data Stewards must coordinate the assignment of data custodianship to existing data collections when a vacancy is identified.

This process includes:

- identifying data collections for which they have delegated responsibility
- identifying the appropriate Data Custodian for each data collection by applying the criteria for selection specified in this policy in consultation with stakeholders
- notifying the Data Custodian of their responsibilities.

9. Reassignment of Data Custodianship

Data custodianship may change when a **person** leaves the position (temporarily or permanently) or due to a change in the designated **position**, which typically occurs during periods of organisational restructure.

Where a Data Steward or Custodian are absent and their position has not been filled (temporarily or permanently), then the responsibilities of the data collection resides with the next most senior delegate until the position is filled (i.e. Director General and Data Steward, respectively).

When the Data Custodian position is filled (temporarily or permanently) the Custodianship Form must be updated (Attachment A, Section C) for administrative purposes and submitted to staff within the Purchasing and System Performance Division for processing. The Data Steward is only required to sign the Custodianship Form (Attachment A, Section D) when the change in custodianship is due to a change in the allocated position to ensure the position aligns with the criteria for selection specified in this policy.

Once the relevant sections of the form are completed, the staff member appointed to fill the position (temporarily or permanently) is empowered to exercise all responsibilities associated with the role of Data Custodian.

10. Education and Training

Upon appointment, the Data Steward and Custodian need to ensure they fully understand the responsibilities of their roles by referring to:

- the Information Management Policy Framework, as well as other policy frameworks, legislation and regulations relevant to the data collection

- public sector governance standards and good practice (e.g. Aboriginal Cultural eLearning, Accountable and Ethical Decision Making, WA Health Code of Conduct, Managing Conflict of Interest, Recordkeeping Awareness Training)
- strategic/corporate plans and policies of relevance to the operating environment and related issues (e.g. WA Health ICT Strategy 2015-2018, WA Health Strategic Intent 2015-2020).

As part of continuing education, it is the responsibility of the Data Steward and Custodian to keep up-to-date with respect to the above resources and seek relevant training and professional development as required.

11. Conflicts of Interest

Conflicts of interest arise in situations where a public officer is placed in a position where their duty to act independently, ethically and without prejudice may be, or appear to be, compromised by self-interest or a relationship with a third party.

Data Stewards and Custodians must declare any conflict of interest in accordance with the WA Health Managing Conflict of Interest Policy and Guidelines (OD 0264/10). All identified conflicts of interest are to be recorded and managed in accordance with the Guidelines attached to the Managing Conflict of Interest Policy.

Where a conflict of interest involves the Data Steward, they must complete the Assessment Guide and Record Form within the Guidelines. This documentation must be submitted for consideration to the Director General or senior delegate in accordance with the relevant Delegations Schedule. In such instances, the issue or decision is to be exercised by the Director General or appropriate senior delegate.

Where a conflict of interest situation involves the Data Custodian of a particular collection, they must complete the Assessment Guide and Record Form within the Guidelines and submit for consideration to the Data Steward. In such instances, the issue or decision is to be exercised by the Data Steward.

12. Escalation Process

Differences of opinion may arise between Data Custodians, or a Data Custodian and a third party (e.g. researcher, media, interstate authority), regarding any aspect of the data collection. For example, the Data Custodian may refuse to disclose data to a third party if the request is viewed as excessive with respect to the aims of the project. Alternatively, Data Custodians may disagree with respect to security requirements and perceived security risks associated with the disclosure of information.

If matters pertaining to a data collection cannot be resolved, the Data Custodian will outline the issue in writing, including any risks and proposed course of action, and escalate to the Data Steward. The Data Steward will review and adjudicate as soon as possible or escalate to the Director General if the matter cannot be resolved. The Data Steward should notify all parties of the outcome.

13. Roles and Responsibilities

The roles and responsibilities of Data Stewards and Data Custodians are to ensure that data collected by WA Health is collected for a legitimate purpose and managed in accordance with the Information Management Policy Framework. In addition to these key

roles, there are ICT and other business groups that are crucial to ensuring the integrity and security of the data.

13.1. Data Steward

Data Steward's responsibilities include, but are not limited to, the following:

- ensuring any risks regarding the identification of individuals, patients and Health Service Providers have been considered and appropriately managed prior to releasing information
- approving conditions for timely and appropriate use and disclosure of data that protect privacy, confidentiality and security of the information
- ensuring the use, disclosure and access to data meets legislative responsibilities and other arrangements entered into by the State
- setting the strategic direction for the data collection and ensuring that projects and initiatives are aligned and coordinated to deliver the best value
- nominating the Data Custodian(s) for the day-to-day management, operation and support of each data collection
- approving changes in data custodianship as required
- reporting and managing any conflict of interests in accordance with WA Health policy and guidelines
- assisting with dispute resolution matters involving Data Custodians and escalating these matters to the Director General as required.

13.2. Data Custodian

Data Custodians are responsible for the day-to-day and long term management of data on behalf of the State. This encompasses a range of responsibilities that include, but are not limited to, the following:

13.2.1. Data Collection Planning

The responsibilities include ensuring that the design, development and enhancements to information systems in which the data are stored, meets business needs. This includes:

- identifying the information requirements including determining and consulting with key stakeholders and users of the information system
- liaising with ICT support staff with respect to information requirements and updates as required
- identifying relevant data items needed to meet the requirements, as well as existing or overlapping sources of information
- identifying and adhering to the requirements of relevant policy frameworks
- identifying requirements to meet legislative responsibilities and other arrangements entered into by the State.

13.2.2. Data Collection Management and Production

Responsibilities include the day-to-day management and production of the data. This includes:

- establishing data collection procedures and maintaining data quality standards

- managing data security and any risks associated with the data
- establishing procedures to permit and review access to information as required by relevant legislation and in accordance with the requirements of the Data Steward
- ensuring data are fit-for-purpose and continue to meet business requirements
- ensuring the retention, storage and disposal of data is in accordance with relevant policy frameworks.

13.2.3. Data Access, Use and Disclosure

Data Custodians have a number of responsibilities related to the access, use and disclosure of data for operational, reporting and research purposes. This includes:

- providing advice on the proper use and interpretation of the data to authorised users
- undertaking a risk assessment to ensure the identification of individuals, patients and Health Service Providers have been considered and appropriately managed prior to releasing of information
- establishing protocols relating to access, use and disclosure of information in accordance with the Information Management Policy Framework
- ensuring the access, use and disclosure of information to authorised users is in accordance with approved protocols, contracts and agreements
- providing applicants, whose request for access have been approved, with timely access to data on a 'best endeavours' basis and communicating any delays to the applicant as soon as possible
- ensuring the safe transmission of data to authorised users
- reporting and managing data breaches in a timely manner
- reporting and managing any conflict of interests in accordance with policy and guidelines.

Data Custodians may assign day-to-day tasks associated with their position to suitably qualified staff, but they remain responsible to the Data Steward. Business User Groups and the HSS may also assist the Data Custodian with respect to ICT issues, as well as planning, maintenance and ongoing management of data collections.

13.3. Business User Group

A Business User Group for an application provides a forum for representation of key stakeholders. Membership typically comprises representatives from the major hospitals or each Health Service Provider and HSS. As a result, representatives may also be Data Custodians of the data collection.

The main responsibilities of a Business User Group centre on assisting HSS with prioritising and supporting enhancement and change requests based on WA Health's business priorities.

13.4. Health Support Services

The HSS contribute to the maintenance and ongoing development of data collections within WA Health by managing many of the applications that are integral to collecting the data. HSS assist with the management of WA Health's ICT networks, ICT security, hardware, infrastructure, applications and websites. They contribute to the confidentiality, integrity and

availability of information by implementing technical safeguards to protect the information and minimise the risk of unauthorised or inappropriate access or use. HSS advise with respect to ICT strategic planning to ensure the alignment of all ICT initiatives with the ICT Framework and strategic direction of WA Health.

13.5. WA Health Information Communication Technology Governance

The WA Health ICT Governance Structure provides a decision making framework for WA Health's ICT investment. The boards and groups comprising the ICT Governance Structure provide oversight and leadership with respect to the planning, delivery and management of ICT programmes and projects across WA Health.

13.6. Authorised Users

All those who contribute to or use data collections within WA Health have responsibilities including, but not limited to, the following:

- recognising that WA Health information is owned by the State, and must therefore be used in a manner that affords benefit to the people of the State
- maintaining agreed standards when collecting and submitting information to data collections
- using the data for the approved purpose only
- citing the source and currency of information used
- abide by any copyright requirements when using data
- advising Data Custodians of any changes in their information requirements
- advising the Data Custodian of any errors or omissions in the data sets or information products they receive
- maintaining confidentiality and security of the information in accordance with conditions of use, legislation and policy frameworks.

13.7. Purchasing and System Performance Division

The Purchasing and System Performance Division is responsible for:

- managing the WA Health Information Register
- providing administrative support to the Director General with respect to notification of and changes in data stewardship
- providing advice to Data Custodians about policies, standards and guidelines that are within scope of the Information Management Policy Framework
- developing and maintaining documents within scope of the Information Management Policy Framework and ensuring they align with current legislation and best practice
- assisting Data Stewards and Custodians and with the reporting of any conflict of interest with respect to Enterprise and Local Systems
- reviewing compliance with this policy through consultation and auditing processes.

14. Compliance

Staff who breach confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the Public Service Regulations 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.

Health Service Providers are encouraged to develop internal business processes to manage and monitor their data governance processes and compliance with this policy.

15. Evaluation

The Purchasing and System Performance Division will carry out compliance audits to ascertain the level of statewide compliance with this policy. It is expected that all data collections within scope will be documented in the Information Register and have a Data Steward and Data Custodian assigned.

The Purchasing and System Performance Division may provide updates to Data Stewards, Chief Executives of Health Service Providers, the Director General and other relevant persons regarding the findings of the compliance monitoring activities.

The policy will be reviewed by the Purchasing and System Performance Division at least every 3 years to take account of new legislation, policy frameworks and processes.

16. Definitions

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.
Aggregate level data	Is summed and/or categorised data that is analysed and placed in a format (for example, in tables or graphs) that prevent the chance of revealing an individual's identity (individual records cannot be reconstructed).
Authorised user	Individuals (both internal and external to WA Health) authorised to use or disclose information within a specific WA Health data collection.
Best endeavours	It places upon the Data Custodian the onus of making every reasonable effort, to achieve the desired objective.
Business information	Includes, but is not limited to, administration, corporate, workforce, human resources, financial or accounting information that may contain personal information.
Confidentiality	The obligation of people not to use or disclose information for any purpose other than which was given to them, without permission.
Contracted Health Entity	Means a non-government entity that provides health services under a contract or other agreement entered into with the Department CEO (Director General) on behalf of the State, a Health Service Provider or the Minister. Refer to section 6 of the *Health Services Act 2016*.

Data	The term 'data' generally refers to unprocessed information, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. In this policy the terms 'data' and 'information' have been used interchangeably and should be taken to mean both data and information.
Data breach	Refers to an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.
Data collection	A systematic gathering or organised collection of data, in any format, for a particular purpose, including manual entry into an application system, questionnaires, interviews, observation, existing records and electronic devices. This includes, but is not limited to, information stored in enterprise systems, local systems and data warehouses.
Data Custodian	The person(s) responsible for the day-to-day management of a data collection, as nominated by the Data Steward. Data Custodians assist the Data Steward to protect the privacy, security and confidentiality of information within data collections. Data Custodians also aim to improve the accuracy, usability and accessibility of data within the data collection.
Data governance[1]	Is the system of decision rights and accountabilities surrounding data and the use of data. It can involve legislation, organisational structures, legal contracts, and various agreements, policies, and guidelines.
Data Steward	A position with delegated responsibility from the Director General of the Department to manage a data collection. The Data Steward's primary responsibility is to protect the privacy, security and confidentiality of information within data collections. Data Stewards also approve the conditions for appropriate use and disclosure of information for clearly defined purposes that comply with WA Health's statutory obligations and Information Management Policy Framework.
Data Warehouse[2]	A Data Warehouse integrates data, from many heterogeneous sources (i.e. various Enterprise and Local

[1] Australian Institute of Health and Welfare. Data Governance - In Brief.
http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=60129549732

[2] Chan, J. O. 2005. Optimizing Data Warehousing Strategies.
http://www.iima.org/CIIMA/CIIMA%205.1%201%20Chan-1.pdf

	Systems) and stores them in an easily accessible central repository. A Data Warehouse is designed to support business decisions by facilitating the consolidation of data to support analysis and reporting at different aggregate levels. The integration of query, reporting and analysis tools provides users with the opportunity to efficiently extract critical data, as well as drill down and through the data for clinical and operational analytics. This capability provides a coherent picture of activity at a point in time and supports strategic and tactical decision making, while driving quality improvement and cost reductions.
Department CEO	The Chief Executive Officer (Director General) of the Department of Health. Refer to section 6 of the *Health Services Act 2016*.
Disclosure	Refers to the communication or transfer of information outside of WA Health, which is considered a single entity under this policy. A disclosure can occur by giving a copy, summary, or communicating the information in any other way to another organisation or individual outside WA Health.
Fit-for-purpose	Means appropriate, and of a necessary standard, for its intended use.
Health information	Means: (a) information, or an opinion, that is also personal information, about: (i) the health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to the individual; or (iv) a health service provided, or to be provided, to an individual; or (b) other personal information collected to provide, or in providing, a health service.(Refer to section 213 of the *Health Services Act 2016*).
Health Service Provider	Health Service Provider means a health service provider established under section 32 of the *Health Services Act 2016* and may include North Metropolitan Health Service (NMHS), South Metropolitan Health Service (SMHS), Child and Adolescent Health Service (CAHS), WA Country Health Service (WACHS), East Metropolitan Health Service (EMHS), Quadriplegic Centre and Health Support Services (HSS).
Information	Refer to 'Data'.

Interstate authority	In accordance with section 218 of the *Health Services Act 2016*, means – (a) a Department of the Public Service of the Commonwealth, another State or a Territory; or (b) an agency or instrumentality of the Commonwealth, another State or a Territory; or (c) a body (whether corporate or unincorporated), or the holder of an office, post or position, established or continued in existence for a public purpose under a law of the Commonwealth, another State or a Territory.
National Minimum Data Set (NMDS)[3]	Is a minimum set of data elements agreed by States and Territories for mandatory collection and reporting at a national level. A NMDS is contingent upon a national agreement to collect uniform data and to supply it is part of the national collection.
Personal information	Has the meaning given in the *Freedom of Information Act 1992* in the Glossary section 1. Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
Research[4]	Original investigation undertaken to gain knowledge, understanding and insight. It is a broad concept and there is no simple, single way to define research for all disciplines.
Staff member	An employee in the Health Service Provider or a person engaged under a contract for service by the Health Service provider. Refer to section 6 of the *Health Services Act 2016.*
Transaction-based system	A transaction based system is an information processing system for business transactions involving the collection, modification and retrieval of all transaction data Examples of Enterprise Systems that are transaction-based include, but are not limited to Emergency Department Information

[3] © Australian Institute of Health and Welfare 2016. National Minimum Data Sets and Data Set Specifications. http://www.aihw.gov.au/copyright/

[4] National Health and Medical Research Council - Australian Code for the Responsible Conduct of Research. http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/r39_australian_code_responsible_conduct_research_150107.pdf

	System (EDIS), Medical Records Information Tracking System (MeRITS) and Patient Administration System (webPAS).
Unit record data	For the purpose of this policy unit record data are electronic records of information that relate to an individual, which are held by WA Health data collections.
Use	Of information refers to the communication or handling of information within WA Health. WA Health is considered a single entity under this policy. Therefore, sharing information between Health Service Providers, the Department and Contracted Health Entities is considered use.
WA Health	For the purpose of this policy, the terms 'WA Health' and 'WA Health System' have been used interchangeably. WA Health is comprised of the Department of Health and Health Service Providers (NMHS, SMHS, CAHS, WACHS, EMHS, Quadriplegic Centre and HSS) and to the extent that Contracted Health Entities provide health services to the State, the Contracted Health Entities.

17. References

Aboriginal Cultural eLearning – A Healthier Future (OD 0599/15)

Amendment to WA Health Code of Conduct (OD 0383/12)

© Australian Institute of Health and Welfare 2016. National Minimum Data Sets and Data Set Specifications.

Authorities, Delegations and Directions Schedule - Department of Health (OD 0432/13)

Department of Health. Recordkeeping Awareness Training

Information Access and Disclosure Policy (OD 0539/14)

Information Management Policy Framework

National Health and Medical Research Council - Australian Code for the Responsible Conduct of Research

New South Wales Health. 2005. Process for Approval of New or Modified Data Collections

Privacy Manual for Health Information. Reproduced by permission, NSW Ministry of Health © 2016

Public Sector Commission. Accountable and Ethical Decision Making Program

WA Health Information and Communications Technology (ICT) Strategy 2015 – 2018: Building a Strong Foundation

WA Health Managing Conflict of Interest Policy and Guidelines (OD 0264/10)

WA Health Risk Management Policy (OD 0433/13)

WA Health Strategic Intent 2015-2020

18. Relevant Legislation

Carers Recognition Act 2004

Commonwealth Privacy Act 1988 (Australian Privacy Principles)

Corruption, Crime and Misconduct Act 2003

Criminal Code Act 1913

Financial Management Act 2006

Freedom of Information Act 1992

Health Act 1911

Health Legislation Administration Act 1984

Health Services Act 2016

Human Reproductive Technology Act 1991

Public Sector Management Act 1994

State Records Act 2000

Western Australian Mental Health Act 2014

19. Related Documents

Acceptable Use Policy – Information and Communications Technology (OD 0468/13)

Australian Standard ISO 15489- Records Management

Database Administration Standard

Data Breach Response Policy (OD 0564/14)

Data Collection Policy (OD 0558/14)

Data Quality Policy (OD 0380/12)

Department of Health Open Data Strategy (OD 0633/15)

Finance Policy Framework

Guidelines for the Release of Data (IC 0208/14)

Information Classification Policy (OD 0537/14)

Information and Communications Technology Policy Framework

Information Management Policy Framework

Information Storage and Disposal Policy (OD 0559/14)

Information Use Policy (OD 0572/14)

Intellectual Property Management in WA Health (IC 0228/15)

Metadata Documentation Policy (OD 0464/13)

Patient Confidentiality (IC 0164/13)

Patient Information Retention and Disposal Schedule Version 4, 2014 (OD 0584/15)

Research Policy Framework

20. Authority

Title:	Data Stewardship and Custodianship Policy		
Contact:	Senior Policy Officer		
Directorate:	Purchasing and System Performance		
Version:	June 2016	**Date Published:**	01/07/2016
Date of Last Review:	13/06/2016	**Date Next Review:**	01/07/2019

This document can be made available in alternative formats on request for a person with a disability.