Government of Western Australia
Department of Health

Information Storage and Disposal Policy

Delivering a Healthy WA

TITLE: INFORMATION STORAGE AND DISPOSAL POLICY

1. BACKGROUND

WA Health creates and collects a vast amount of information, much of which is confidential personal health information. Information collected by WA Health is an important resource used for the clinical care of patients, health service planning, monitoring, improvement and medical research. This information is vital to patient safety and wellbeing and must be managed with consideration for its confidentiality and sensitivity.

All information needs to be managed, stored and disposed according to its classification, business requirements and retention period. Suitable retention periods, storage conditions and the use of recommended disposal methods will ensure that information is managed, protected and accessible across WA Health.

2. POLICY

The 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.

WA Health information must be classified as public, protected or confidential and stored accordingly. The *Information Classification Policy (OD 0537/14)* contains guidelines that outline storage requirements by the:

- classification of the information
- format of information – paper, electronic and removable media.

The security of information must be managed in a manner that ensures appropriate protection. Paper-based and electronic information systems should include and apply physical and technical security controls to ensure the integrity of information is not compromised. The *WA Health Recordkeeping Plan* documents suitable security arrangements for storage of paper-based and electronic information. The *Information & Communications Technology (ICT) Physical & Environmental Security Policy (OD 0506/14)* documents safeguards for ICT equipment and information.

At the end of the retention period written authorisation must be obtained prior to disposing of records. Disposal of records must be carried out in accordance with the relevant Retention and Disposal Schedule and by a method commensurate with the classification of

the information. Confidential information must be destroyed by a method that ensures no possibility of reconstructing the contents.

2.1 Storage of Paper-Based Information

Storage conditions for paper records should be designed to protect the data not only from unauthorised access and theft, but from damage that can be caused by vermin, fire, water, mould and natural disasters.

Paper records that are considered to have a permanent or continuing value (in accordance with Retention and Disposal Schedules) should be stored in conditions that satisfy the State Records Commission record keeping requirements for government organisations.

The *Environmental and Safety and Protection Minimum Requirements for Paper Records* (Appendix A) outlines the minimum storage requirements for paper records.

Semi-active (required infrequently, for example, once a year) or inactive hard copy records may be stored in secondary storage facilities, either in-house or in a commercial facility approved under a Common Use Contract (CUC) established by the Office of Government Procurement (refer to Department of Finance – *Buyers Guide - Storage, Retrieval and Destruction for Paper and Electronic Records (CUA 34504 & 123499)*). As the CUC is not mandatory for regional areas, the WA Country Health Service (WACHS) is able to enter into agreements with local offsite storage providers.

When transferring records to secondary storage facilities, the method of retrieving the information, if requested, must be considered. Complete documentation of all records sent off-site, including barcoding records and storage boxes, will enable records to be easily located when required.

Outsourcing storage does not lessen the obligation to ensure records are secured, managed and made accessible. The secondary storage provider must also be accountable for maintaining the required storage conditions in accordance with the applicable Memorandum of Understanding (MOU) and relevant WA Health policies, guidelines and procedures.

2.2 Storage of Electronic Information

Electronic information must remain available, accessible, retrievable and usable for as long as a business need exists or as long as legislative, policy and archival provisions and procedures require them to be kept.

Electronic information including databases must only be disposed in accordance with an approved Retention and Disposal Authority.

The *Long Term Management of Electronic Records Policy (OP 1872/04)* details the process for retaining electronic records created and maintained within WA Health. This policy ensures that electronic information of continuing value maintains its functionality and is migrated forward in accordance with the relevant retention and disposal authorities when hardware and software changes.

The *Information & Communications Technology (ICT) Physical & Environmental Security Policy (OD 0506/14)* should be applied to ICT facilities to safeguard equipment and information from unauthorised intrusion and damage.

2.3 Storage of Information in Other Formats

The *Environmental and Safety and Protection Minimum Requirements for Paper Records* (Appendix A) can be used as a guideline for appropriate storage conditions for information stored using the following formats:

- photographic media black and white (e.g. sheet film, x-rays and microforms)
- photographic media colour (e.g. sheet film and cine film)
- magnetic media (e.g. computer tapes and disks, video tapes and magneto-optical disks)
- optical media (e.g. compact and mini disks).

2.4 Portable Computer and Storage Devices

When portable computer and storage devices are used for the capture or transport of data, the data must be transferred to primary storage as soon as practicable. Only WA Health registered portable devices should be used for storing or transporting sensitive or confidential WA Health data and this data must be encrypted. Users of shared (pool) devices must ensure that they remove all data that they have stored on the device before returning the devices.

In addition to encryption, all portable storage devices should have additional forms of security attached to safeguard further against unauthorised access, such as:

- access controls – screen savers, account passwords (ideally with a combination of letters and numbers) that are changed on a regular basis
- digital wipe software – this ensures the portable storage device is wiped when information is transferred to the network
- tracking function – allows the ability to track all data that is transferred onto a portable storage device.

For further details please refer to the following documentation:

- *Enterprise Architecture Standards SS03 Media Handling*
- *Information and Communications Technology (ICT) Physical and Environmental Security Policy (OD 0506/14)*
- *Information Security Policy (OD 0389/12)*
- *Mobile Computing Devices Policy and Guidelines (OD 0336/11)*

2.5 Cloud Computing

Cloud computing is a term used to describe a method of storing data on a server located externally, made accessible via the internet.

WA Health information must not be stored on external cloud computing services without agreements for the management of the information in accordance with government policy and legislative requirements such as the *Freedom of Information Act 1992* and *State Records Act 2000*.

In accordance with the WA Health *Information Security Policy (OD 0389/12)*, any agreements with Cloud service providers would need to ensure that:

- WA Health has ownership of WA Health information – Section 33 under the *State Records Act 2000* states that a department is entitled to enter into a contract with a third party to perform any aspect of record keeping provided that the Director of the State Records Commission is notified and the records remains under the control of the department.
- WA Health is informed of the storage site(s) – cloud storage providers may have their own third party storage providers. WA Health must be aware of the storage location of the information.
- Retention and disposal of information is in accordance with the appropriate WA Health Retention and Disposal Schedule.
- If personal information is also stored, security arrangements are in place to protect misuse of the information.

Current WA Health Recordkeeping Plans do not allow for the use of an external data storage provider. Legal advice must be sought before entering into a contract for cloud computing, or any external storage of WA Health information.

2.6 WA Health Retention and Disposal Schedules

WA Health information must be stored for the assigned retention period and disposed at the appropriate time using a prescribed method consistent with the classification of the information.

The WA Health Recordkeeping Plan documents the current Retention and Disposal Schedules to be used for determining retention period for all types of records (patient, administrative, financial, human resource management).

Information authorised for disposal by the relevant schedules may be destroyed after the specified minimum retention period has elapsed. The destruction of information that is classified as protected or confidential must be carried out in a secure manner. When using external contractors, a certificate confirming the complete destruction of records must be provided by the contractor.

2.7 Disposal of Information

Information must be stored for a minimum retention period before destruction takes place. For further information about the correct timeframes and methods for disposal refer to:

- 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)*.

When considering the destruction of electronic data the following policies are relevant to ensure the correct method is used:

- Electronic Records - *Long Term Management of Electronic Records Policy (OP 1872/04).*
- Information & Communications Technology (ICT) equipment containing information - *Disposal of ICT Equipment and Data Storage Media Policy* and the *Enterprise Architecture Standards SS03 Media Handling.*

2.8 Destruction Register

A register of records destroyed must be maintained for future reference and accountability. The register must be consistently and accurately maintained whenever any records are destroyed.

The destruction register must capture details of each individual record destroyed, rather than a description of a group of records, as well as reference to the relevant Retention and Disposal Authority.

A destruction register must contain the following information as a minimum:

- Disposal Authority Number – Indicates the Retention and Disposal Schedule that authorises the destruction of records.
- Index Number – Refers to the type or class of record.
- Description – Provides a description of the individual record item being destroyed. For individual patient records, the Unique Medical Record Number (UMRN), patient surname and given names may be recorded.
- Date Range – Indicates the inclusive dates of records being destroyed (e.g. 1950 - 1955).
- Company – Refers to the name of the contractor providing destruction services, and the location of the service (if applicable).
- Method of Destruction – Specifies how the records are destroyed. For example, shredding.
- Certification – Indicates the records have been destroyed in accordance with methods outlined in WA Health Retention and Disposal Schedules. An officer delegated the authority to destroy records, or who witnesses the destruction of records by a contractor, may sign this part of the register as certification or cross-reference to other certification documentation.

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	is 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 an 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 Repository	is 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.
Information	refer to Data.
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 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.
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

All persons employed (employees) in WA Health, including contractors, sub-contractors and agency personnel must familiarise themselves with the relevant legislation, policies, guidelines, standards and procedures pertaining to the storage, retention and disposal of information. The extent of these responsibilities will vary according to individual roles.

Data Custodians are responsible for ensuring the retention, storage and disposal of information is in accordance with relevant legislation and WA Health documentation.

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

Department of Finance – Buyers Guide – Storage, Retrieval and Destruction for Paper and Electronic Records (CUA 34504&123499)
Disposal of ICT Equipment and Data Storage Media Policy
Enterprise Architecture Standards SS03 Media Handling
General Disposal Authority for State Government Information GDA 2013-017
ICT Physical and Environmental Security Standard (OD 0560/14)
Information and Communications Technology (ICT) Physical and Environmental Security Policy (OD 0506/14)
Information Classification Policy (OD 0537/14)
Information Lifecycle Management Policy (OD 0371/12)
Information Security Policy (OD 0389/12)
Long Term Management of Electronic Records Policy (OP 1872/04)
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 Recordkeeping Plan
WA Health Misconduct and Discipline Policy (OD 0323/11)

8. RELEVANT LEGISLATION

Commonwealth Privacy Act 1988 (Australian Privacy Principles)
Corruption and Crime Commission Act 2003
Criminal Code Act 1913
Electronic Transaction Act 2011
Evidence Act 1906, Acts Amendment (Evidence) Act 2000
Freedom of Information Act 1992
Freedom of Information Regulations 1993
Health Act 1911
Hospital and Health Services Act 1927
Human Reproductive Technology Act 1991
Mental Health Act 1996 (WA)
Public Sector Management Act 1994
State Records Act 2000

Environmental and Safety and Protection Minimum Requirements for Paper Records		
Environmental conditions	Temp/Relative Humidity	• The storage of records in air-conditioned premises where the temperature and relative humidity are maintained within recommended ranges (refer to *State Records Commission, Standard 7: Storage of State Archives*) for the various media is the ideal. However if air-conditioning is not available or practical, then priority should be given to maintaining a consistent temperature and humidity over time through ventilation, insulation, location of storage and building design.
	Internal Environment	• Dust and dirt controls. Limiting the impact and/or remedy such as a cleaning cycle. • Pest/vermin control program. • Continuous power supply. • Occupational health and safety considerations. • Records should be stored in conditions that are clean and secure, with low risk of damage from fire, water, dampness, mould, insects and rodents. They should also be kept away from direct sunlight and other sources of light and heat. The storage area should be well ventilated.
	Lighting	• Minimise the entry of natural light, ultra-violet light and heat.
Safety and protection	Fire and Disaster Management	• Alarm and fire protection system. • Smoke detectors. • Disaster management programmes should be established and maintained. • Risk management exercises include examination of records storage areas. • Fire prevention and suppression measures include heat/smoke detection, fire alarms and extinguishing systems. • Current disaster recovery plans are in place which covers each records storage location. • Staff are assigned responsibilities in the records disaster management process and are trained to meet them.

	Security	• Records with a higher degree of sensitivity or confidentiality, such as those relating to personal privacy, commercial and personal interests, personal and national security, should be identified and access to these records controlled by –
		  ◦ levels of secure storage consistent with the levels of sensitivity
		  ◦ accountable procedures controlling personnel access to the storage areas.
		• Determine access status of records and requirements of control.
		• Control access to storage areas.
		• Unauthorised entry prevention and detection systems.

	Housing and Shelving	• Buildings chosen for records storage are weatherproof, have good drainage and areas are intruder resistant and access controlled. • Storage areas are maintained and monitored, including monitoring of temperature and humidity variation and mould, dust and pest infestation. • Shelving/cabinets/racks should be appropriate for each format of record. Consideration should be given to the horizontal storage of large format records. Shelving, cabinets and racks should support the weight of each container or item and hold them separately to reduce the risk of damage that could arise from access to nearby items or collapse of stacked items. • Shelving should be clean and meet occupational health and safety requirements. • Shelving arrangements are compatible with the sprinkler system design (if installed).
	Containers and Handling	• Packaging and containers are designed to fit the records, strong enough to withstand handling, pressure and weight of records they contain and of quality and composition commensurate with the value and use. • Handling techniques include transfer containers or satchels with security seals. • Item containers are clean, in good condition and appropriate to the format and retention period of records they hold.
	Retrieval of Records	• The ability to respond immediately to unpredictable demands for either records or their content. • Effective descriptive and location controls that enable accurate identification of the records requested and their whereabouts in storage. • The design and resourcing of the storage operation, including the type and configuration of shelving, equipment, staffing and the efficiency of retrieval, delivery procedures and control systems should be considered. • Consider the location of the storage facility, particularly if physical delivery of the record is necessary.

Note: This table has been sourced from information in the '*Standard for the Physical Storage of Commonwealth Records'*, National Archives of Australia 2002.

This page is intentionally left blank

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