Information Storage and Disposal Policy

1. BACKGROUND

In the course of its operations, 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.

All information needs to be managed, stored and disposed regardless of value and retention period. The purpose served by the information, its physical form and value will dictate the nature of the storage and disposal method.

Appropriate storage conditions and disposal methods will ensure that information is protected, accessible, managed and destroyed when required. The appropriate disposal schedule and destruction methods must be applied to ensure WA Health’s information is adequately protected.

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 data.
- The data collection contains personal 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 scope of this policy includes both paper based (including medical records) and electronic data.

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

3. PURPOSE

The purpose of the Information Storage and Disposal Policy is to document best practice for the storage and disposal of WA Health Information. This ensures information is stored, classified, secured, accessible and disposed in a consistent and timely manner.
4. POLICY

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

4.1 Storage of Information

Storage conditions for all records must be based on the physical form, use, informational value and function of the record.

Paper Records

Storage conditions for paper records should be designed to protect 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.

The Environmental and Safety and Protection Minimum Requirements for Paper Records (Attachment A) documents the minimum requirements for paper records.

Secondary Storage Facilities

Semi-active (required infrequently e.g. 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 Government Procurement. As the CUC is not mandatory for regional areas, WA Country Health Service (WACHS) are 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 bar-coding records and storage boxes, will enable records to be easily located when required.

Out-sourcing 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 and relevant WA Health policies.

Electronic Records

WA Health must manage and retain its electronic records using the same policies as paper based records. Electronic records including databases must only be disposed in accordance with an approved Retention and Disposal Authority.

Electronic records 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.

The Long Term Management of Electronic Records Policy details the process for retaining electronic records created and maintained within WA Health. This policy ensures that electronic records of continuing value maintain their functionality and are migrated forward due to hardware and software changes in accordance with the relevant retention and disposal authorities.
For the following electronic records the Environmental and Safety and Protection Minimum Requirements for Paper Records (attachment A) can be used as a guideline for appropriate storage conditions:

- Photographic media black and white – Sheets film, xrays and microforms
- Photographic media colour – Sheet film and cine film
- Magnetic media – computer tapes and disks, video tapes and Magneto-optical disks.
- Optical Media – Compact and mini disks.

**Portable Computer and Storage Devices**

When portable computer and storage devices are used for the capture or transport of original data, such data must be transferred to the primary storage as soon as practicable. Unsecured devices must not be used to store or transport unencrypted sensitive or confidential WA Health data. Users of shared (pool) devices must ensure that they remove all data that they have stored on the device before returning the devices.

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

- Encryption – process of systematically encoding data before transmission and during storage.
- 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 the portable storage device.

For further details please refer to the [Mobile Computing Devices Policy and Guidelines](#).

### 4.2 Classification

WA Health information must be classified as public, protected or confidential and stored accordingly. The [Information Classification Policy (OD 0304/10)](#) contains guidelines that outline the storage requirements by the:

- type of information – electronic, paper and removable media; and
- classification of the information – public, protected or confidential.

### 4.3 Security

Information security management ensures the storage of information in a manner that ensures appropriate protection. Recordkeeping and information systems should include and apply physical and technical security controls to ensure the integrity of records is not compromised.

The [WA Health Recordkeeping Plan](#) documents suitable security arrangements for storage of paper and electronic records, including:

- Hard copy records are stored in a secure room accessible only to authorised staff. A barcode system is in place to enable tracking of records.
• Hard copy records stored off site are located at a storage facility approved under the CUC for the supply, storage, retrieval and destruction of intermediate record services. As the CUC is not mandatory for regional areas, WACHS are able to enter into agreements with local offsite storage providers.
• Electronic records have varying degrees of access depending on delegations assigned to staff within WA Health.
• Electronic records are backed up on a regular basis.

To ensure the appropriate security mechanisms for data, the following policies are available:
• Electronic – Information Security Policy.
• Information stored on mobile computing devices - Mobile Computing Devices Policy and Guidelines.
• Physical Environment of computers used to store information - Physical and Environmental Security Standard.
• Database security - Database Administration Standard.

4.4 WA Health Retention and Disposal Schedules
All WA Health staff must ensure records created are stored for the appropriate retention period and disposed at the appropriate time and using an appropriate method.

The following policies will assist in determining the correct time frames and methods of disposal:
• 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.

4.5 Disposal of Information
Records authorised for disposal by the relevant schedules may be destroyed after the specified minimum retention period has elapsed.

WA Health staff must ensure that the destruction of records is secure and confidential. When using external contractors, a certificate confirming the complete destruction of records must be provided by the contractor.

Paper records may be destroyed by:
• Shredding - a means of destroying paper records by mechanical cutting into strips or particles. Shredding must render all information incapable of reconstruction.
• Pulping - the process where paper records are prepared for recycling by chemical and/or mechanical methods.

Patient records must never be buried or disposed of in conventional rubbish repositories/council tips.

Destruction of data stored on digital storage media may involve data sanitisation and/or destruction of the physical storage media. Methods available for the destruction of data stored on digital media include:
• Reformatting - is a basic form of sanitisation typically used to free storage for use by other data. Reformatting does not fully destroy data. Instead, the storage area containing the data is merely marked as available and retains the old data until it is overwritten.
• Overwriting - a form of sanitisation and renders the underlying, previously stored data beyond easy recovery.
• Degaussing - is a procedure that reduces the magnetic flux density to zero by applying a reverse magnetising field to the digital storage media. Degaussing renders any previously stored data on the storage media unreadable.
• Physical methods - includes crushing, cutting, melting, scratching or shredding. Physical destruction (when performed correctly) is considered secure as the data stored on the digital storage media is rendered irretrievable. An external contractor may be used for the physical destruction of digital storage media. Melting and smelting are not recommended as an environmentally sound means of media destruction.

When considering the destruction of electronic data the following policies are relevant to ensure the correct method is used:
• Electronic Records - OP 1872/04 Long Term Management of Electronic Records Policy.
• Information & Communications Technology (ICT) equipment containing information - Disposal of ICT Equipment Policy.

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 UMRN, patient surname and given names may be collected.
• Date range – Indicates the inclusive dates of records being destroyed (eg 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.
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.

A Data Repository includes 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.

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 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.

6. ASSOCIATED POLICIES

Information Classification Policy OD 0304/10
WA Health Recordkeeping Plan
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
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

8. SUPPORTING DOCUMENTS

State Records Office – Principles and Standards
### Environmental and Safety and Protection Minimum Requirements for Paper Records

#### Environmental conditions
- **Temp/RH**
  - 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 reaction and 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; and
    - 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.