

health

Department of Health
NORTHERN CAPE

Records Management Policy

Version control

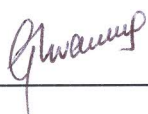
Version : V001

Publishing Date : June 2015

Review Date : After 3 years but not later than 5 years from the
Publishing Date

Responsible Manager : Director Corporate Services

Approved by the

Head of Department :  Date: 02 JUNE 2015

Ms GE Matlaopane

Table of Contents

Policy Aim	3
Policy Scope	3
Policy Statement.....	3-8
Roles and Responsibilities.....	8-11
Review and Distribution.....	11
Acknowledgements and Sources.....	12

Policy Aim

1. The purpose of this policy is to ensure that departmental records are managed in a well-structured record keeping system as well as to strengthen the security and safety of clinical records by enforcing compliance and adherence to the National Archives and Records Services of South Africa Act 43 of 1996.
- 1.2. This policy must be read in conjunction with the Security and ICT policies, the National Archives and Records Services of South Africa Act 43 of 1996 as well as the Northern Cape Provincial Archives Act no. 7 of 2013.

Policy Scope

2. This policy applies to all records of the Northern Cape Department Health excluding clinical records.

Policy Statement

3. It is the policy of the Northern Cape Department of Health that all records created and received by the department shall be managed in accordance with records management principles contained in section 13 of the National Archives and Records Service Act, 1996.
 - 3.1. The department considers its records to be valuable assets to:
 - 3.1.1. Enable department to find the right information easily and comprehensively;
 - 3.1.2. Perform its functions successfully and efficiently and in an accountable manner;
 - 3.1.3. Support the business, legal and accountability requirements of the department of Health.
 - 3.2. Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and

promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

3.3 The following broad principles apply to the records keeping and records management practices of the department:

3.3.1. The department follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.

3.3.2. Electronic records in the Department of Health are managed according to the principles promoted by the National Archives and Records Service.

3.3.3. Department has performance measures for all records management functions and reviews compliance with these measures.

4. Records Classification System and Related Storage areas

4.1. Correspondence system

4.1.1. File Plan

4.1.1.1. Only the approved file plan shall be used for the classification of correspondence records. The file plan shall be used for the classification of paper-based and electronic (including e-mail) records.

4.1.1.2. Specific procedures for the allocation of file subjects and reference numbers to electronic records are filed on file. More specific guidance regarding the classification of e-mail is contained in the e-mail management policy.

4.1.1.3. Employees shall allocate file reference numbers to all correspondence (paper, electronic, e-mail) according to the approved subjects in the file.

4.1.1.4. When correspondence is created/received for which no subject exists in the file plan, the records manager should be contacted to assist with additions to the file plan. Under no circumstances may subjects be added to the file plan if they have not been approved by the records manager.

5. Storage Areas

5.1. Paper-based correspondence files are kept in the custody of:

5.1.1. The central registry

5.1.1.1. All paper-based correspondence system records that are not HR related are housed in the central registry

5.1.1.2. All these records are under the management of the records manager who is mandated to ensure that they are managed properly.

5.1.1.3. The registry is a secure storage area and only registry staff are allowed in the records storage area.

5.1.1.4. Employees that need access to the files in the registry shall place a request for the files at the counter.

5.1.1.5. The registry shall be locked when it is not in operation.

5.1.2 The Human Resources registry

5.1.2.1 All human resources related records are housed in the HR registry.

5.1.2.2 The general HR subject files as well as HR case files are under the management of the records manager who is mandated to ensure that they are managed properly.

5.1.2.3. The department of health maintains a set of paper-based case files for each employee of the department. These files are confidential in nature and are housed in a secure storage area in the HR registry

5.1.2.4. The case files are managed as part of the list of series of separate case files that is maintain and managed by the records manager.

5.1.3. **Electronic correspondence records are stored on a shared drive that is maintained by the IT.**

5.1.3.1. Access to storage areas where electronic records are stored is limited to the Information Technology employees who have specific duties regarding the maintenance of the hardware, software and media.

5.1.4. **Electronic system other than the correspondence systems**

5.1.4.1. The Department of Health has a number of electronic records systems in operation which is not part of the correspondence system and that generate and store public records.

5.1.4.2. The records maintained in these systems are under the control of the records manager who is mandated to ensure that they are managed properly.

6. Disposal of records

6.1. No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the Provincial Archivist.

6.2 The Provincial Archivist issued standing disposal authority number (which will be added as soon as it is issued by the Provincial Archivist) for the disposal of records classified against the file plan. The records manager manages the disposal schedule.

6.3. The Provincial Archivist issued standing authority number (which will be added as soon as it is issued by the Provincial Archivist) on the schedule of records other than correspondence systems.

6.4. Retention periods indicated on the file plan and schedule are determined based on the departmental legal obligations and functional needs. Should an employee disagree with the allocated retention periods, the records manager should be contacted to discuss a more appropriate retention period.

6.5. All disposal actions should be authorised by the records manager prior to their execution to ensure that archival records are not destroyed inadvertently.

6.6. Disposal in terms of these disposal authorities will be executed annually.

6.7. Non – archival records that are needed for litigation, Promotion of Access to information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Manager: Legal Services has indicated that the destruction hold can be lifted.

6.8. Paper –based archival records shall be safely kept in the records storage area until they are due to transfer to the Provincial Archives Repository. Transfer procedures shall be prescribed by the Provincial Archives in the Records Management Policy Manual.

6.9. Specific guidelines regarding the procedure to dispose of electronic records are contained in the electronic records management policy.

7. Access and Security

7.1. Records shall at all times be protected against unauthorized access and tampering to protect their authenticity as evidence of the business of the Department of Health.

7.2. Security classified records shall be managed in terms of the Information Security Policy.

7.3. No staff member shall remove records that are not available in the public domain from the premises of the Department of Health without the explicit permission of the records manager in consultation with the information security manager.

7.4. No staff member shall provide information and records that are not in the public domain to the public without consulting the Chief Information Officer.

7.5 Personal Information shall be managed in terms of the Promotion of Access to Information Act until such time that specific protection of privacy legislation is enacted.

7.6. No staff member shall disclose information of any member of staff or client of the Department of Health to any member of the public without consulting the Chief Information Officer first.

7.9. An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.

7.10. Registry and other records storage areas shall be locked when not in use.

8. Legal admissibility and evidential weight

8.1. The records of the department of health shall at all times contain reliable evidence of business operations. The following shall apply:

8.1.1. Paper-based records

8.1.1.1. No records shall be removed from paper-based files without the explicit permission of the records manager.

8.1.1.2. Records that were placed on files shall not be altered in any way.

8.1.1.3. No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the records manager.

8.1.1.4. Should evidence be obtained of tampering with records, the staff member involved shall be subjected to disciplinary action.

8.1.2. **Electronic records**

8.1.2.1. The Department of Health shall use systems which ensure that its electronic records are: authentic, not altered or tampered with; auditable and produced in systems which utilize security measures to ensure their integrity.

Roles and Responsibilities:

9. This policy is having the following role players

9.1. The **Head of the Department** shall:

9.1.1. As the Information Officer approve requests for information in terms of the Promotion of Access to Information Act no.3 of 2000.

9.1.2. Enhance accountability, transparency and improvement of service delivery by ensuring that sound records management practices are implemented and maintained.

9.1.3. Support the implementation of this policy and instruct all employees of the department to support the values contained in this policy.

9.1.4. Designate the assistant manager: records management to perform the record management duties to enhance records management practises and compliance of the department to legislative and regulatory requirements.

9.1.5. Inform the records manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

9.2. The **Senior Managers** shall:

9.2.1. Ensure the implementation of this policy in their respective units and maintain good record keeping and records management practices.

9.1.2. Ensure that records management including e-mail are one of the key performance areas of their sub-ordinates.

9.1.3. Inform employees of their records keeping and records management responsibilities and obligations.

9.3. The **Record Manager** shall:

9.3.1. Manage all records according to the records management principles contained in the National Archives and Records Service Act, 1996.

9.3.2. Ensure compliance with the provisions of the National Health Act and manuals which apply to health records.

9.3.3. Be responsible for the determination of retention periods in consultation with users and taking into account the functional, legal and historical need of the body to maintain records of transactions.

9.3.4. Ensure that all records created and received by the department are classified according to the approved file plan and that a written disposal authority is obtained for them from the National Archives and Records Services.

9.3.5. Develop an adequate record training system, tailored to local needs, is essential to facilitate prompt record location and ensure that client/ patient care does not suffer and that privacy is not breached.

9.3.6. Conduct training and other intervention as are necessary to ensure that the that the departmental record keeping and records management practices

comply with the records management principle outlined in the National Archives and Records Services Act.

9.3.6. Identify training courses that are relevant to the duties of the registry staff and shall ensure that the employees are trained on records management.

9.4. The IT Manager shall:

9.4.1. Be responsible for the day-to-day maintenance of electronic systems that stores records.

9.4.2. Work in conjunction with the records manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.

9.4.3. Ensure that appropriate systems technical manuals and system procedure manuals are designed for each electronic system that manages and stores records.

9.4.4. Ensure that electronic records in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.

9.4.5. Ensure that all data, metadata, audit trail data, operating system and application software are backed up on daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

9.4.6. Ensure that back-ups are stored in a secure offsite environment and are virus free.

9.5 The Security Manager shall:

9.5.1. Be responsible for the physical security of all records.

9.6. The Legal Services Manager shall:

9.6.1. Keep the Records Manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of the Department of Health.

9.7. The **Registry Staff** shall:

9.7.1. Be responsible for the physical management of the records in their care as outlined in the registry procedure manual.

9.8. The **Employees** shall:

9.8.1. Create records of transactions while conducting official business.

9.8.2. Manage records efficiently and effectively by:

9.8.2.1. Allocating reference numbers and subjects to paper-based and records according to the file plan.

9.8.2.2. Sending paper-based records to the registry for filing.

9.8.2.3. Ensuring that records are destroyed/ deleted only in accordance with the written disposal authority issued by the Provincial Archivist.

Review and Distribution

10. The Provincial Records Manager is the responsible manager for this policy and for ensuring it is reviewed and updated.

11. This policy will be reviewed after 3 years but no later than 5 years from the publishing date. If necessary an updated version will be issued, if not a formal cover letter will be issued to supplement the cover of this Policy (identifying a revised publication date).

12. The Director for Policy & Planning will distribute updated versions to:

- Member of the Executive Council for Health
- Head of Department of Health

- All Chief Directors, Directors and Deputy Directors (who will in turn distribute to their staff as appropriate.)

Acknowledgements and Sources

13. This policy is based on the following legislative requirements:

- 13.1. The Constitution of the Republic of South Africa Act 108 of 1996
- 13.2. National Archives and Records Service of South Africa Act no. 43 of 1996
- 13.3. The Northern Cape Provincial Archives Act no. 7 of 2013
- 13.4. Public Finance Management Act no. 1 of 1996
- 13.5. The National Archives and Records Services of South Africa Regulations
- 13.6. The Promotion of Access of Information Act no. 3 of 2000
- 13.7. The Promotion of Administrative Justice Act no. 75 of 1997
- 13.8. Electronic Communication and Transactions Act no. 25 of 2005
- 13.9. Protection to Information Act no. 84 of 1984
- 13.10. Occupational Health and Safety Act no. 85 of 1993
- 13.11. Hazardous Substance Act no. 15 of 1973