Retention and Destruction of Medical Records Policy

March 2021

Version 1

Table of Contents

Introduction: 3

Purpose: 3

Scope: 3

Definitions: 4

1. Storage of Medical Records: 4

2. Inactive Medical Records: 5

3. Archiving of Medical Records: 5

3.3 Archiving within the facility: 5

3.4 Remote Archiving: 6

3.5 Electronic Medical Records: 6

4 Timelines for retention: 7

4.1 Exceptions to retention: 7

5 Destruction of Records: 8

5.1 Paper Medical Records: 8

5.2 Electronic records: 9

5.3 Other storage media of medical records 10

6 Responsibilities of Healthcare Facilities: 10

Reference: 11

Introduction:

The retention of medical records by healthcare facilities is essential to the assurance of patient care. Health information management includes both retention and destruction functions using all media, including paper, images, optical disk, microfilm, DVD, and CD-ROM. The warehouses or resources from which to retrieve, store, and maintain data and information include, but are not limited to, application-specific databases, diagnostic biomedical devices, master patient indexes, and patient medical records and health information. To ensure the availability of timely, relevant data and information for patient care purposes; to meet national legal requirements; and to reduce the risk of legal discovery, organizations must establish appropriate retention and destruction schedules. However, with the passage of time and accumulation of medical records, facilities may find it difficult to retain medical records for long periods of times especially for patients who cease to follow up their care within that facility. This document is issued by NHRA based on Decree number (46) 2002 regarding Criminal Law procedures and Decree (15) 1976 regarding Penal law in order to standardize medical records retention and disposal in the Kingdom which specify a period of three years for the retention of medical records.

Purpose:

To define and describe medical records retention and disposal in the Kingdom.

Scope:

All licensed healthcare facilities within the Kingdom.

The life cycle of records management begins when information is created and ends when the information is destroyed. The goal for organizations is to manage each step in the record life cycle to ensure record availability.

At a minimum, record retention schedules must:

- Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses of the organization
- Include guidelines that specify what information is kept, the time period for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, optical disk, magnetic tape)
- Include clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained

Definitions:

Active: means that the records are consulted or used on a routine basis. Routine functions may include activities such as clinic visits, laboratory tests, radiology etc.

Archiving: The storage of inactive records either in the healthcare facility or at an authorized archiving company/area.

Destruction: The irreversible act of deletion of the medical record

Inactive: means that the records are used rarely but must be retained for reference or to meet the full retention requirement. Inactive records usually involve a patient who has not sought treatment for a period of time (three years) or one who completed his or her course of treatment.

Kingdom: Kingdom of Bahrain

Medical Record: A record held for each healthcare recipient visiting the healthcare facility. The records may be paper or electronic medical records.

NHRA: National Health Regulatory Authority

Retention: The length of time for which medical records are kept

1. Storage of Medical Records:

1.1. Medical records must be stored in a secure location with limited access

1.2. The storage area should comply with health and safety requirements and have proper environmental controls (such as temperature and humidity) and protection against fire and thief.

1.3. Electronic records should be stored on a server in addition to remote backup being performed regularly.

2. Inactive Medical Records:

2.1. Medical records may be deemed inactive if the healthcare recipient fails to attend the facility for three consecutive years.

2.2. All records (whether paper or electronic) must be retained within the healthcare facility as inactive records for a minimum of **three years** (as per statute of limitation of the Kingdom) from the date of the last visit of the healthcare recipient.

3. Archiving of Medical Records:

3.1 Records may be archived after being inactive for three consecutive years.

3.2 Archived records must be retained for 7 years, after being inactive for three years (total of 10 years).

3.3 Archiving within the facility:

3.3.1 The facility may either hold these records with the active records or separately.

3.3.2 The same security level of active records must be implemented with archived records.

3.3.3 A log of all archived records must be maintained

3.3.4 When an archived record is accessed, the following information must be recorded:

3.3.4.1 Date of access

3.3.4.2 Name, National ID number, and designation of person gaining access

3.3.4.3 Reason for access

3.3.4.4 When the record is removed from the archive, the following information must be recorded:

3.3.4.5 Date of removal of record

3.3.4.6 Name, National ID number, and designation of person removing the record

3.3.4.7 Signature of the person removing the record

3.3.4.8 Reason for removal of record

3.3.4.9 The date of return of record

3.3.5 If a healthcare recipient revisits the facility within the specified period, the record should be reactivated and shifted with the active records. The file should not be archived again except if the healthcare recipient fails to attend to the facility for a minimum of three years.

3.4 Remote Archiving:

3.4.1 These storage areas may be owned by the facility or an authorized archiving company

3.4.2 Storage conditions must comply with earlier mentioned requirements about safety and protection (1.2.)

3.4.3 If an authorized archiving company is utilized, a contract must be signed with the archiving company clearly stating the roles and responsibilities of each party.

3.4.4 The contract should specify actions to be taken in case of inadvertent destruction of the records (either natural or man-made disasters) and the liability of each party.

3.4.5 A log of all archived records must be maintained

3.4.6 When an archived record is accessed, the following information must be recorded:

3.4.6.1 Date of access

3.4.6.2 Name, National ID number, and designation of person gaining access

3.4.6.2.1 Reason for access

3.4.7 When the record is removed from the archive, the following information must be recorded:

3.4.7.1 Date of removal of record

3.4.7.2 Name, National ID number, and designation of person removing the record

3.4.7.3 Signature of the person removing the record

3.4.7.4 Reason for removal of record

3.4.7.5 The date of return of record

3.5 Electronic Medical Records:

3.5.1 Electronic medical records may be deemed inactive after three years from the date of the last visit of the healthcare recipient to the healthcare facility.

3.5.2 The records may be archived after three years of being inactive for seven years.

3.5.3 Archived electronic records should be secured and may not be altered or deleted at any time (please refer to the Good Documentation Practice Policy available on our website)

3.5.4 Records may be saved on the hospital server (as well as a remote backup) or on a remote backup device or cloud.

4 Timelines for retention:

Type of record	Retention of records	Archiving	Total years of retention:
1. Adults medical records	All records must be retained within the facility for a minimum of three years from the date of last visit of the healthcare recipient	7 years	10 years
2. Minors medical records		Until child reaches the age of 21 (plus 3 years statute of limitation)	Until child reaches the age of 21 (plus 3 years statute of limitation)

4.1 Exceptions to retention:

4.1.1 As an exception to the above-mentioned timelines, records which are involved in lawsuits, complaints, investigations, possible litigation, or any form of dispute must be retained until the dispute has been resolved with no possibility of an appeal.

4.1.2 These records must be retained in a secure area with very limited access.

4.1.3 For these records the following steps should be taken:

4.1.3.1 For paper records: A stamp stating “DO NOT DESTROY” should be placed on the inside cover of the record

4.1.3.2 For electronic records: These records should show an alert and the records permanently saved to prevent any further changes.

5 Destruction of Records:

Destruction of medical records must be done in a method which prevents reconstruction and possibility of reading of the information contained within the record.

5.1 Paper Medical Records:

5.1.1 Medical records may be destroyed by shredding (cross shredding) or incineration after the retention timeline has been reached.

5.1.2 The destruction of records must be done in a secure location.

5.1.3 If the destruction will be performed by an independent company, a contract is signed between the facility and the concerned company to ensure:

5.1.3.1 Safeguards against security breaches;

5.1.3.2 No destruction is made without the per-approval of the facility and the presence of its representative during the process;

5.1.3.3 Responsibilities of each party;

5.1.4 All destructions must be witnessed by a representative from the healthcare facility.

5.1.5 A log should be kept with the following information:

5.1.5.1 Date of destruction

5.1.5.2 Method of destruction

5.1.5.3 Number of medical records destroyed

5.1.5.4 Details of medical records destroyed including but not limited to:

5.1.5.4.1 Medical record number

5.1.5.4.2 Name of patient

5.1.5.4.3 National ID number of patient

5.1.5.5 Name of person in charge of destruction, National ID number, and designation

5.1.5.6 Signature of the person in charge of destruction

5.1.5.7 Name of representative from the facility, National ID number, and designation

5.1.5.8 Signature of facility representative

5.1.6 Exemptions to retention must always be ensured

5.1.7 Facilities will be held legally liable if destructions are made in violation with the exemptions mentioned earlier in this policy.

5.2 Electronic records:

5.2.1 Electronic Medical records may be destroyed by organizationally approved and validated overwriting technologies/methods/tools or digital sanitation

5.2.2 At least a single write pass should be used with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

5.2.3 If healthcare facilities computers are to be deployed either internally or disposed of, the utility software must be run against the computer's hard drive followed by reformatting.

5.2.4 If healthcare facility computers are deemed obsolete and cannot be used due to damage, the hard drive must be removed and be physically destroyed

5.2.5 The destruction must be done in a secure location.

5.2.6 If the destruction will be performed by an independent company, a contract is signed between the facility and the concerned company to ensure:

- 5.2.6.1 Safeguards against security breaches;
- 5.2.6.2 No destruction is made without the per-approval of the facility and the presence of its representative during the process;
- 5.2.6.3 Responsibilities of each party;

5.2.7 All destructions must be witnessed by a representative from the healthcare facility.

5.2.8 A log should be kept with the following information:

- 5.2.8.1 Date of destruction
- 5.2.8.2 Method of destruction
- 5.2.8.3 Number of medical records destroyed
- 5.2.8.4 Description of the disposed records
- 5.2.8.5 Details of medical records destroyed including but not limited to:
  - 5.2.8.5.1 Medical record number
  - 5.2.8.5.2 Name of patient
  - 5.2.8.5.3 National ID number of patient
- 5.2.8.6 Name of person in charge of destruction, National ID number, and designation
- 5.2.8.7 Signature of the person in charge of destruction
- 5.2.8.8 Name of representative from the facility, National ID number, and designation
- 5.2.8.9 Signature of facility representative
- 5.2.8.10 A statement that the records were destroyed in the normal course of business

5.2.9 Exemptions to retention must always be ensured

5.2.10 Facilities will be held legally liable if destructions are made in violation with the exemptions mentioned earlier in this policy.

5.3 Other storage media of medical records

5.3.1 Patient information stored in other storage media must be destroyed appropriately. Such media may include but not limited to:

- 5.3.1.1 Microfilm or microfiche methods of destruction include recycling and pulverizing.
- 5.3.1.2 Laser discs used in write once-read many document-imaging applications are destroyed by pulverizing.
- 5.3.1.3 Computerized data are destroyed by magnetic degaussing.
- 5.3.1.4 DVDs are destroyed by shredding or cutting.
- 5.3.1.5 Magnetic tapes are destroyed by demagnetizing.

6 Responsibilities of Healthcare Facilities:

6.1 Establish a policy for retention and destruction of medical records as per this national policy.

6.2 All records must be kept in a secure location with limited access

6.3 Create an abstract of the destroyed patient information

6.4 Notify patients when destroying patient information

6.5 Specify the method of destruction used to render the information unreadable.

6.6 Organizations should reassess the method of destruction annually based on current technology, accepted practices, and availability of timely and cost-effective destruction services

6.7 Facility must audit adherence to its policy

6.8 Facility must report violations to the policy to NHRA within a maximum of 2 working days.

Reference:

1. Retention and Disposal of Records Policy and Procedures. Heart of England. NHS Foundation Trust. 2011
2. Information governance: Retention of Medical Record Policy. Royal United Hospital Bath. NHS trust. 2007
3. Medical Record Retention and Destruction: https://umia.com/wp-content/uploads/2018/11/1648U-Medical-Record-Retention-and-Destruction.pdf
4. North York General Hospital Policy Manual: Record Retention and Destruction Policy: 2009
5. Keating, Angie Singer. “Destroying Data to DoD way: Military standards Help Ensure Compliance for electronic Data Security”. Journal od AHIMA 76, no. 7 (July -Aug 2005: 54-55.62.)