Document Type: Health Information Policy	**Ref No:** DHA/HISHD/PP-12	**Version Number:** 1
Document Title: Policy for Health Information Assets Management	**Issue Date:** 26/12/2022 **Effective Date:** 26/03/2023 **Revision Date:** 26/12/2027	
Ownership: Dubai Health Authority		
Applicability: All Healthcare Entities under the Jurisdiction of Dubai Health Authority		

1. Definitions/Abbreviations:

Accession records: is the means by which the accessioning process is documented. Accession record is an administrative and descriptive document that summarizes standard information about the process of transferring materials to a repository, including information about the provenance, contents and legal and physical transfer of the records such as, rights and restrictions. It often precedes arrangement and description; and can be used as the basis for the creation of an archival description once the materials have been arranged.

Active Health Information Asset (HIA): The HIA that are consulted or used on a routine basis. Routine functions may include activities such as release of information requests, revenue integrity audits, or quality reviews.

Assets: are economic resources. It is anything tangible or intangible that is capable of must being owned/controlled to produce value and that is held to have positive economic value.

Adverse event includes:

- Accident: an event that results in injury or ill health.
- Incident:

  – Near miss: an event that, while not causing harm, has the potential to cause injury or ill health.

  – Undesired circumstance: a set of conditions or circumstances that have the potential to cause injury or ill health (e.g. untrained nurses handling heavy patients)

Classified Person: is someone who could be exposed to ionising radiation, through occupational exposure including reasonably foreseeable incidents, who could receive more than the following doses: 6 mSv/year whole body effective dose, 150 mSv/year equivalent dose to the extremities, and 15 mSv/year to the lens of the eye. It also specifically applies to an employee who works with a source of ionising radiation where a dose rate could deliver a whole body exposure of 20 mSv (or 500 mSv to the extremities or 20 mSv to the lens of the eye) within a few minutes from a reasonably foreseeable event.

Clinical Trial Sponsor: A person, company, institution, group, or organization that oversees or

pays for a clinical trial and collects and analyzes the data.

Compliance: is the act of adhering to, and demonstrating adherence to, a standard or regulation (international or internal).

Confidentiality: Part of the information security triad, confidentiality means the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consent: Is the fact that permission has been given. A person who consents to something is, in effect, giving permission for that thing to happen.

Controller: Any authority, agency or other body which, alone or jointly with others, determines the method, standards, and criteria for processing the Personal Health Information and the purposes and means of this processing. In this Policy, the Controller is the Entity or data owner.

Data: An organized set of information, facts, concepts, instructions, observations, or measurements in the form of numbers, letters, words, symbols, images, videos, signs, sounds, maps, or any other form, generated, processed, stored, interpreted, or exchanged, by individuals or Information and Communications Technology (ICT).

Data Protection Impact Assessment: Describes a process designed to identify risks arising out of the processing of Protected Health Information (PHI) and to minimise these risks as far

and as early as possible.

Data Subject: A person who is the subject of Protected Health Information (PHI). This can be the patient or any healthy service user.

Degaussing: Erasing hard disk and magnetic tapes though an electromagnetic field.

Destroy: Refers to the confidential and secure destruction of the HIA with proof of destruction. These will be HIA with no archival value and there is no longer an ongoing business need to retain them for longer.

Digitizing: (also known as digital imaging or scanning) is defined as the process of converting any hard- copy, or non-digital record into digital format.

Disposal: Refers to the secure destruction of a Health Information Asset (HIA) or the transfer of HIA for permanent preservation. A certificate of transfer should be provided as proof of transfer (and can act as evidence of disposal).

Electronic Medical Record: Electronic Medical Record (EMR) is a digital version of a Data Subject/patient's paper medical chart and personal information. It contains a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory test results.

Entity: Entity in Dubai that is involved in the direct delivery of healthcare and/or supportive healthcare services, or in the financing of health such as health insurer and health insurance

facilitator, healthcare claims management Entity, payer, third party administrator, hospital, medical clinic, medical Center, telemedicine provider, laboratory and diagnostic center, and pharmacy, etc.

Healthcare Professional: A person who by education, training, certification and licensure is qualified to provide health services

Health Information: Data and health information processed and made apparent and evident whether visible, audible or readable, and which are of a health nature whether related to health facilities, health or insurance facilities or beneficiaries of health services.

Health Information Assets Management: the end-to-end tracking and management of HIA to ensure that every asset is properly used, maintained, upgraded and disposed of at the end of its lifecycle. The key components of HIA management are:

- Information creation
- Information keeping and tracking
- Information maintenance (including tracking of record movements)
- Access and disclosure
- Transfer
- Appraisal
- Archiving
- Disposal.

Health Information Assets Custodian: Custodians are the people who are actually in possession of the information, and who implement and administer controls over the information according to instructions from owners.

Health Information Assets Owner: are senior members of staff who have been appointed by their Entity to be responsible for one or more identified information asset(s). This person will be responsible for ensuring that the Information Asset is handled and managed appropriately.

Inactive Health Information Assets: The HIA that involve a Data Subject/patient who has not sought treatment for a period of five (5) years. These HIA must be retained for reference, or to meet the full retention requirement.

Incidents: Violation or imminent threat of violation of information security policies, acceptable use policies, or Entity`s security standard.

Information asset: Health assets within the Entity including:

- Electronic copies of health information
- Physical/printed copies of health information
- Software / Applications
- Devices and equipment used by the Entity for information processing and storing.
- Human resource information within the Entity.

Litigation: the act, process, or practice of settling a dispute in a court of law.

Long-term Illness: are chronic diseases / conditions for which there is currently no cure, and which are managed with drugs and other treatment, for example:

- Alzheimer disease and dementia
- Arthritis
- Asthma
- Cancer
- Chronic obstructive pulmonary disease
- Crohn disease
- Cystic fibrosis
- Diabetes
- Epilepsy
- Heart disease
- Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Syndrome (AIDS)
- Mood disorders (Bipolar, Cyclothymic, and Depression)
- Multiple sclerosis
- Parkinson disease

Medical Records (also called Health Records): A record that consists of data concerning health; has been made by or on behalf of a health professional in connection with the

diagnosis, care or treatment of the individual to whom the data relates.

Medical Surveillance: is the systematic assessment of employees exposed or potentially exposed to occupational hazards. This assessment monitors individuals for adverse health effects and determines the effectiveness of exposure prevention strategies.

Metadata: is "data about data" or structured information about a resource.

Protected Health Information (PHI): also referred to as personal health information; include any of the 18 types of identifiers specified below:

- Name (Full or last name and initial)
- Address (All geographical identifiers)
- All elements of dates (other than years) related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89).
- Telephone numbers
- FAX number
- E-mail address
- Emirates Identification Number
- Medical record number
- Health insurance beneficiary numbers
- Bank Account number
- Certificate/license number

- Vehicle identifiers (including serial numbers and license plate numbers)
- Device identifiers or serial numbers
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images.

Any other unique identifying number, characteristic, or code.

Processing: Data processing covers the creating, entering, using, modifying, updating, deleting, storing, disclosing and disposing of data.

Pulverizing: Media is shattered or grounded into small non-constructible pieces.

Retention Periods: Begin when the HIA ceases to be operational. This is usually at the point of discharge from care when the HIA is no longer required for current on-going business, or the Data Subject or service user has deceased.

Scanning: Process of converting paper documents into electronic formats through document imaging process.

Secondary use: is for purposes other than treating the individual subject of care, such as for Research, Public Health, Quality Improvement, Safety Initiatives, and marketing. Some secondary uses directly complement the needs of primary use. Examples include medical

billing, hospital administrative, and management operations.

Subject Access Request (SAR): is the Right of Access allowing an individual to obtain records to their personal information, held by an organisation/Entity.

Very Important Person (VIP) Criteria:

- Senior visitors (leaders and heads of state).
- Foreign ministers during their visit to the UAE
- Ambassadors and Delegates in the UAE
- Ministers and Undersecretaries of the Ministry of the UAE
- Chairmen and Undersecretaries of the government departments of the UAE
- Royals and crown princes of the UAE and other Emirates including their immediate family members (wives, sons, daughters, brothers and sisters)
- Al Nahyan and Al Maktoum family members
- Members with prefix "Sheikh" or "Sheikha" in their official identity.
- Members with prefix "High Excellence" or "Her Excellence" in their official identity.

CSP : Cloud Service Provider

DHA : Dubai Health Authority

DPO : Data Protection Officer

EMR : Electronic Medical Record

HIA : Health Information Asset

HISHD	:	Health Informatics & Smart Health Department
HRS	:	Health Regulation Sector
IAO	:	Information Asset Owner
ICT	:	Information and Communications Technology
IG	:	Information Governance
ISO	:	Information Security office
PHI	:	Protected/Personal health information
UAE	:	The United Arab Emirates.

2. Purpose

2.1. To set out Dubai Health Authority (DHA) `s requirements for Health Information Asset (HIA) management in the Emirate of Dubai; in line with the United Arab Emirates (UAE), and Emirate of Dubai laws, legislative, and regulatory frameworks.

2.2. To assure Entities under jurisdiction of DHA are providing a secure environment for

the management of HIA.

2.3. To outline the requirements and responsibilities of Entities working under jurisdiction of DHA on HIA management.

2.4. To ensure the confidentiality of information and protect the privacy of community members by providing proper governance on HIA.

2.5. To define the rights and duties of all concerned parties dealing with HIA.

3. Scope

3.1. All Health Information Asset within the Emirate of Dubai handled by Entities under jurisdiction of DHA.

3.2. This policy also covers all information systems purchased, developed, managed or utilised by the Entity related to healthcare services.

3.3. Health Information Asset (HIA) as defined by UAE Information and Communications Technology (ICT) in Healthcare law includes information/data in all its form, as well as the underlying application, technology, and physical infrastructure to support its processing, storing, communicating and sharing. This includes but is not limited to:

3.3.1. Medical records (health and care records, registers – for example, birth, death, Accident and Emergency, theatre, minor operations, etc.)

3.3.2. Non-Medical information (e.g. Human resource, complaints records, corporate records / administrative records related to health service functions of the Entity etc.).

3.3.3. Laboratory assets (paraffin blocks, slides, digital images etc.) and patient test reports.

3.3.4. X-ray and imaging reports, output and images.

3.3.5. Identifiable and non-identifiable data.

3.3.6. Data Accessed for primary or secondary use (such as records that relate to uses beyond individual care; for example, records used for service management, planning, research, quality, etc.).

3.3.7. Microform (microfiche or microfilm)

3.3.8. Audio and video tapes, cassettes, CD-ROM etc.

3.3.9. Physical or digital forms of data/records.

3.3.10. Structured record systems (Paper and electronic)

3.3.11. Transmission of information (Fax, Email, post and telephone).

3.3.12. Metadata added to, or automatically created by, digital systems.

3.3.13. Warehouses or resources from which the Entities retrieve, store, and maintain data and information. This include, but are not limited to:

a. Application-specific databases

b. Diagnostic biomedical devices

c. Master patient indexes

d. Patient medical records and health information.

3.4. All users accessing and using HIA in healthcare sector in the Emirate of Dubai; including all employees, contractors, consultants, suppliers, vendors, partners, customers and wider stakeholders where appropriate; accessing HIA should be conscious of this policy.

4. Policy Statement:

4.1. The Health Information Asset management Policy is an integral part of the DHA's approach to Information Governance (IG) in the Emirate of Dubai. This policy must be read in conjunction with other related DHA IG policies.

4.2. Both UAE Federal Law No. (2) of 2019 concerning the Use of the Information and Communication Technology in the Area of Health ("ICT Health Law"), and DHA Health Information Assets (HIA) Classification Policy have impact on HIA

Management. Hence, this policy elaborates the intersection between all related UAE laws, Emirate of Dubai legislations, and DHA regulations. Nevertheless, the regulation that is more specialized in health and detailed will supersede.

4.3. Health Information Asset Management

4.3.1. Health Information Asset (HIA) Management should be recognised as a specific corporate responsibility within every Entity.

4.3.2. All HIA assets within the Entity must be classified as per DHA Health Information Assets Classification policy: (Health Information Assets Classification policy).

4.3.3. All HIA assets should be labelled, processed, and stored strictly in accordance with the classification levels assigned to them.

4.4. Benefits of Deploying Health Information Assets Management System within an Entity:

4.4.1. Entities has all relevant information in hand as and when required.

4.4.2. Health Information can be accessed and located easily, and the current version is identified where multiple versions exist.

4.4.3. Health Information can be interpreted to know who created or added to the record, when (during which business process), and how the record is related

to other records.

4.4.4. Health Information can be trusted; the record's integrity and authenticity can be demonstrated.

4.4.5. Health Information can be maintained through time; the record is available and accessible throughout its lifecycle; regardless of technology advancement.

4.4.6. Health Information are secure from unauthorised or inadvertent alteration or erasure. Access and disclosure are properly controlled, and audit trails track all uses and changes.

4.4.7. Records are held in a robust format, which remains readable for as long as they are required.

4.4.8. Health Information are retained and disposed of appropriately and securely using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of HIA with archival value.

4.5. Use of cloud-based solutions for Health Information Asset management

Before any cloud-based solution is implemented there are a number of measures to be considered:

4.5.1. UAE laws and DHA regulations must be adhered to in selecting any cloud-based solutions for HIA management by the Entity.

4.5.2. The cloud-based solution must provide adequate evidences that they follow UAE laws and legislations.

4.5.3. The cloud-based solution must prevent handling and storing health information with a Cloud Service Provider (CSP), outside the legal jurisdiction or geographical boundaries of the UAE, including for CSP's Backup or Disaster Recovery purposes.

4.5.4. Records in cloud storage must be managed as records in any other environment. The contractual contract for cloud storage must include a clause that:

a. The continuity of cloud storage for the duration of contract is adhered to.

b. In case of transfer of cloud storage to another vendor, the data should be returned to the Entity in a transferable format to retain the retention period.

c. The CSP has no ownership rights on the stored data regardless of the format or storage medium.

d. The CSP must have appropriate controls in place to dispose/destroy the

health information if no longer required and provide reasonable assurance that data is not recoverable.

4.5.5. Necessary measures must be taken to avoid any breach of protected health information stored in the cloud as per all UAE laws and DHA Data and Health Information Protection and Confidentiality Policy (Health Information Protection and Confidentiality Policy).

4.5.6. Entities must make sure the health information stored in cloud-based solutions are available based on Subject Access process. If information not found or left unfound, it would be a breach of the Data Subject`s rights.

4.6. Retention of Health Information Assets

4.6.1. In general and as per ICT Health Law, HIA must be stored for at least Twenty five (25) years from the date of the last health Procedure/Encounter of the Data Subject/ Patient. However, some HIA need more timeline for retention based on business/operational/legal requirements. This decision must be taken by the Entity`s Executive leader/Medical Director with a designated function to appraise HIA.

4.6.2. All Paper medical records must be digitized after maximum two (2) years of the release of this policy, and must be retained as same. The physical HIA can be destroyed after it is digitized according to the technical requirements

outlined in this document and Quality control was conducted.

4.6.3. Retention times for HIA outlined in this policy must be maintained regardless of closure / or merging of the Entity.

4.6.4. In most cases, it will be appropriate to dispose HIA once retention period has expired and appraisal performed by the Entity, unless the records have been selected for permanent / or longer preservation.

4.6.5. The retention periods given in below table are the minimum periods for which HIA must be retained.

Type/Subtype of Health Information Assets	**Minimum Retention Period**
Medical	
• Electronic Medical Records (EMR) • All Prescriptions (including Controlled drug) • Digitized Laboratory / radiology Imaging Assets • Digital images or graphical output used in diagnosis and	• Twenty five (25) years after last encounter with the Data Subject/Patient.

analysis. • Dental records • Neonatal screening records • Dental, ophthalmic and auditory screening records. • Angiography tapes and disks • Electrocardiogram Records • Endoscopy Records • Audiology records • Ambulance records	
VIP Data Subject/Patients' EMR/ Physical Records	• Indefinitely: Do not destroy/ Do not archive
Medico-Legal Cases EMR	• Indefinitely
Medico-legal cases Paper based	• Should be retained by the Entity up to Twenty five (25) years; after records have been digitized. • Decision to maintain original records beyond this period is subject to the Entity`s decision and legal advice
Video records/voice recordings relating to patient care/ /video-conferencing records	• Kept as active record for one (1) year and then archive for two (2) years. • All relevant clinical information must be implemented to

related to patient care/ Telemedicine Audio/Video calls	the appropriate health record.
Human fertilization records, including embryology records *	• Thirty (30) years*
• Cancer/Oncology and Radiotherapy records • Record of long term illness or an illness that may reoccur • Records connected to National registries	• Thirty (30) years after last encounter with the Data Subject/patient.
Registers, logs, and census reports (Electronic): • All registries • Blood bank register • Surgical procedure and theatre records register • Vaccination Registers • Daily Census Reports • Delivery Room Log • Operation Theatre Log	• Indefinitely

• Records of reactions to transfusions • Admission and Discharge Lists/ registers • Operating Room Schedule • Patients Index • Disease Index • Operating Index	
Dental diagnostic or study models	• Digital Models: Twenty five (25) years after completion of treatment. • Physical Models: o Adults: Retaining original pre- and post-operative models for Ten (10) years after completion of treatment. o Children: Ten (10) years after completion of treatment or up to their 25th birthday whichever is the longer. o Discarding intermediate models after five (5) years. o If digitized: the physical model can be discarded sixty (60) days after records have been digitized.
Records of destruction of HIA (in	• Indefinitely

manual or computer format)	
Births, Deaths, and Adoption Records	
• Birth / Death Registry • Birth /Death/ Still-births certificate • Mortuary registers • Local authority adoption record	• Indefinitely.
Body release forms	• Two (2) years
Pathology†	
Electrophoretic strips and immunofixation plates	• Five (5) years unless digital images taken, in which case Two (2) years and stored as a photographic record
Foetal serum	• Thirty (30) years
Frozen tissue for immediate histological assessment (frozen section)	• Stained microscope slides – Ten (10) years • Residual tissue – kept as fixed specimen once frozen section complete.
Microbiological cultures	• Two (2) days after final report of a positive culture issued.
Museum specimens (teaching collections)	• Indefinitely. • Consent of the relative is required if it is tissue obtained

	through post mortem.
Stained slides	• As per The College of American Pathologists (CAP) Minimum Period of Retention of Laboratory Records and Materials
Equipment/instruments maintenance logs, records of service inspections	• Lifetime of equipment
• Day books/other records of specimens received by a laboratory • External quality control records • Accession records • Specimen requests (including the patient chart or medical record if used as the requisition) • Chain-of-custody collection, receipt, accessioning, and handling records. • Proficiency testing records	• Ten (10) years

• Internal quality control records (relating to products) • All quality control, quality assurance and quality management records, Certificates of analysis.	
Policies and procedures	• Two (2) years following discontinuance
Test method validation/ verification records (method performance specifications)	• Length of time the test is in use, plus two (2) additional years
Individualized Quality Control Plan (IQCP), including risk assessment and supporting data, and approval of quality control plan.	• Length of time the test is in use, plus two (2) additional years following discontinuation of the IQCP.
Ongoing IQCP quality assessment data	• Two (2) years
Surgical Pathology (including bone marrows) †	
Cervical screening slides	• Ten (10) years
• Human tissue • Slides	• Thirty (30) years.

• Storage of material following analyses of nucleic acids	
Paraffin blocks	• Thirty (30) years and then appraise for archival value.
Genetics (including Biochemical Genetics, Cytogenetics, Molecular Genetics and Newborn Screening)†	
Genetic samples and records	• Thirty (30) years after last encounter with the Data Subject/ Patient.
Frozen tissue or cells for histochemical or molecular genetic analysis	• Ten (10) years
Neonatal screening (dried blood spot): • Specimen (Guthrie) cards • Records	• Ten (10) years • Thirty (30) years after last encounter with the Data Subject/ Patient.
Copy of original report, or ability to reprint the information content of an original report • Legal genetic testing • Somatic genetic testing	• Indefinitely • Twenty five (25) years after last encounter with the Data Subject/patient.

Cytogenetics: • Analysis records/ karyotypes /digital images including FISH images • Stained microscope slides in permanent mounting medium • Fixed chromosome cell suspension or FISH slides • Original specimens and containers	 • Twenty five (25) years after last encounter with the Data Subject/patient. • 4 years • 6 months • 1 month from date of issue of report
Cytology †	
Reports and digital images	• Twenty five (25) years after last encounter with the Data Subject/ Patient.
• Slides (suspicious-positive) • Fine-needle aspiration slides • Cytology paraffin blocks	• Twenty (20) years
Non- Forensic Autopsy †	
• Paraffin blocks • Slides	• Twenty (20) years
Autopsy consent	• Indefinitely

Hospital Autopsy Records	• Indefinitely
Forensic Autopsy †	
Forensic records: • Records of tissue and organ disposal. • Autopsy consent • Pathology • Toxicology • Hematology • Dentistry • DNA testing • Human tissue kept as part of the forensic record • Paraffin blocks • Slides • Hospital Autopsy Records • Gross photographs/images • Accession records • Representative sample suitable for DNA Analysis	• Indefinitely

Forensic material – criminal cases • Unblocked tissue from histological samples retained at autopsy. • Organs retained at autopsy with consent • Body fluids and tissues for toxicology • Representative tissue suitable for DNA analysis	• Indefinitely

Forensic Medicine materials including, but not limited to: • Biological samples for toxicology • Body swabs • Slides • Foreign material and trace evidence • Biological evidence • Fingernails • Representative/reference • DNA samples • Clothing • Photographs.	
Electron microscopy (EM) Material †	
• Blocks • Slides • Grids • Photos (print/electronically digital image files)	• Thirty (30) years

• Specimens and preparations Blocks for electron microscopy	
Organ Donation/Transplantation, Flow Cytometry, Transfusion Medicine ¥, Donor records †	
• Records relating to investigation or storage of specimens relevant to Organ Donation/ Transplantation • Blood component audit trail and fates.	• Thirty (30) years
Bone marrow slides	• 10 years
Radiology	
• Radiology reports • Digital image	• To be considered as a permanent part of the Data Subject/patient record and should be retained for Twenty five (25) years after last encounter with the Data Subject/ Patient.
Physical image that has been digitized for the sake of archive	• Three (3) years
Physical image that is archived without digitizing	• Twenty five (25) years
Clinical Trials/ Research Cases	• Fifteen (15) years after completion of trial.

imaging	
• Transplantation imaging • Continuity of care purpose (in some long-term diseases; for example slow growing tumour, where chance of recurrence is there)	• Thirty (30) years after last encounter with the Data Subject/ Patient.
Mammograms (if not digitized)	• Normal Packet – Ten (10) years • Screen detected cancers – Indefinitely • Interval Cancers – Indefinitely • Interesting Cases – Indefinitely
Adverse event /Untoward Events	
Adverse event Reports/ Register	• Indefinitely
Health records for classified persons under medical surveillance	• Fifty (50) years from the date of the last entry or age 75, whichever is the longer.
Research	
Advanced Clinical Trial master files of Investigational Medicinal/ Clinical Devices Products; and Trial Subject's Medical Files.	• Thirty (30) years after the conclusion of the trial. • Documents can be retained for a longer period, however, if required by the applicable regulatory requirements or by agreement with the Clinical Trial Sponsor.

	• There should be a flag or divider in health records for documents pertaining to research indicating that the Data Subject/ Patient has been recruited to a clinical trial or other research. • It is the responsibility of Clinical Trial Sponsor & Chief Investigator to ensure that documents are retained.
Research Ethics Committee Records and minutes of meeting relating to a clinical trial	• Where the trial proceeds, at least five (5) years from the conclusion of the trial. • Where the trial does not proceed, at least five (5) years from the date of the opinion.
Research Ethics Committee Records and minutes of meeting relating to a non-clinical investigation	• Three (3) years from date of decision.
Corporate records ‡ (documents not considered part of the patient's medical record)	
Clinical audit records (e.g. Entity Audits, Records Audits, and Systems Audits) – Internal & External in any format (paper, electronic etc.)	• Five (5) years from the date of completion of the audit

Accreditation documents and records of inspections	• Ten (10) years or until superseded
Operating theatre registers	• Indefinitely
• Staff Records	
Personnel health records under occupational surveillance	• Forty (40) years from last entry on the record
Radiation dose records for classified persons under medical surveillance	• Fifty (50) years from the date of the last entry or age 75, whichever is the longer
• Personnel/Human resources records • Disciplinary records	- For UAE national: until the individual's 75th birthday - For non-UAE national: Six (6) years after individual leaves service, at which time a summary of the file must be kept.
Performance reports	• Ten (10) years
• Legal, Complaints and Information Rights	
Complaints – case files	• Ten (10) years from date of file closure. • The complaint is not closed until all processes (including potential and actual litigation) have ended. • Litigation cases of significant or major issues/outcomes should be considered for 30 years retention. • Specific legal advice should be sought from the Entity's

	legal advisors to determine whether the records should be retained further. • Complaints files must always be separately from the patient file (if the complaint is raised by a patient or in relation to).
Complaints correspondence, investigation and outcomes	• Ten (10) years from completion of action/ following closure.
Fraud – case files	• Ten (10) years from date of closure of the case. • This includes cases that are both proven and unproven.
Subject access request (SAR) – where there has been an appeal	• Six (6) years from date of appeal closure
Subject Access Requests (SAR), response, and subsequent correspondence	• Three (3) years from date of SAR closure
* If it is not mentioned "after last encounter"; then the HIA should be retained for the duration it has been mentioned only (regardless of last encounter).	
† If not mentioned, then as per The College of American Pathologists (CAP) Minimum Period of Retention of Laboratory Records and Materials	
‡ If not mentioned, then as per The Joint Commission International accreditation (JCIA) Record Management.	
¥ If not mentioned, then as per The American Association of Blood Banks (AABB) Record Management	
Retention periods should be calculated from the end of the calendar year following the conclusion of treatment or the last entry in the record.	

4.7. Retention Requirements of Digitized Health Information Assets

4.7.1. All HIA should be maintained as per retention periods specified in this policy.

4.7.2. The physical HIA can be destroyed after it is digitized according to the technical requirements outlined in this document and Quality control was conducted. The retention period which would have been applied to the physical HIA must instead be applied to the digitized HIA.

4.7.3. When it is not possible to create a readable digitized image, the original physical HIA must be retained for the full retention period.

4.7.4. Digitized HIA Storage and Backup must be maintained by the Entity. Network storage containing these digitized HIA should be included in the Entity's backup schedule for business-critical data.

4.8. Active and Inactive Health Information Assets

4.8.1. All HIA should be active for at least a period of five (5) years from the discharge date / last encounter date of Data Subject/Patient. After five (5) years, the HIA can be moved to off-site storage and considered inactive.

4.8.2. In all instances, inactive does not mean that the HIA can be destroyed, because it has not yet met its full retention requirement.

4.9. Continued retention of Health Information Assets

4.9.1. There will be occasions where Entities might create longer retention periods for HIA due to the nature of that particular case; and based on business/operational/legal requirements.

4.9.2. The following are examples of when HIA cannot be destroyed or disposed of:

a. The information will possibly be required for the exercising or defending of a legal right or claim:

i. If it is required for notified legal proceedings (e.g. a court order).

ii. Where there is reasonable prospect of legal proceedings commencing (an impending court case).

b. If it is of interest to a public health or research inquiry.

c. If it is subject to a form of access request (e.g. Subject Access Request).

4.9.3. In these situations, Entities can apply longer retention times and this should be decided at the appraisal/review stage once retention time is close to be expired. These decisions must be recorded, made in accordance with formal policies and procedures by the Entity`s Executive leader/Medical Director and set a specific period for further review/appraisal.

4.10. Permanent Preservation of Health Information Assets

4.10.1. Some HIA may require permanent preservation. This HIA are small core with one or more of below characteristics:

a. The HIA preserve information and evidence likely to have long-term research or archival value.

b. The HIA are likely to support research into rare or long-term conditions.

c. The HIA is related to the development of new or unusual treatments or approaches to care within the Entity.

d. The HIA is related to a topic that the Entity is recognised as a national or international leader in that field of medicine / care concerned.

e. The HIA is related to population or environmental factors atypical to the locality.

f. The HIA is related to an event or issue of significant local or national importance (for example COVID-19 pandemic).

g. The HIA enable the public to understand the working scope of the Entity and its impact on the population it serves.

4.10.2. Selection of HIA permanent retention should take place at or before records retention deadline. Authorisation for permanent retention HIA should be given by an the Entity`s Executive leader/Medical Director.

4.10.3. The HIA should not be transferred for permanent storage unless they specifically meet the criteria above. If in doubt, it is recommended to seek advice from the DHA (HISH@dha.gov.ae).

4.11. Storage of Health Information Assets

4.11.1. Storage of HIA applies to medical records, physical HIA, records stored in cloud-based solutions, and other types of HIA.

4.11.2. Below are methods that can be utilized by the Entity for storing HIA:

a. Digitizing medical records

b. Migration to the new systems

c. Cloud storage that is stored within the UAE

d. Scanning to optical disk or equivalent technology.

e. Off-site storage (for physical HIA).

4.11.3. Health information residing in multiple storage media and locations must have clearly defined retention plan and registry.

4.11.4. Storage areas for inactive HIA can include:

a. An area inside the Entity that has been certified for HIA storage.

b. An off-site, private, certified HIA storage facility with which the Entity has an active contract for storage and retrieval services.

4.11.5. Storage areas certified for HIA storing must be physically secure and environmentally controlled to protect HIA from unauthorized access, theft, damage or loss due to temperature fluctuations, fire, water damage, pests and other hazards.

4.11.6. Health information assets in storage should be maintained in the custody of the Entity and must be available to the healthcare provider or Data Subject or his/her designated representative within 3 working days.

4.11.7. Information security, data protection, and confidentiality must be assured when handling, transferring, and storing HIA.

4.11.8. Any HIA involved in litigation/investigation/court cases are considered active HIA and must be stored on site (within Entity) in a secured place designated as such.

4.11.9. While managing off-site HIA, Entities must ensure that:

a. There is a full inventory of what is held offsite.

b. Retention periods are applied to each HIA.

c. A disposal log is kept.

d. There is evidence of secure disposal of HIA.

e. Clear instructions relating to all processing of offsite HIA including destruction plans are present.

f. Access to the storage site is provided in order to exercise due diligence, and conduct site visits if necessary.

g. There is an agreement on how the HIA will be retrieved and in what timeframe it will be returned; to ensure that Entity can respond to Data subject access requests; or retrieve HIA to dispose of when the minimum retention period has been reached.

4.11.10. Entity must conduct a Data Protection Impact Assessment (DPIA) if they are looking to start storing HIA offsite; whether the offsite storage is managed by the Entity or by a private certified company. The DPIA must be accomplished in below circumstances:

a. At the outset of entering an offsite storage contract.

b. If the Entity changes service provider.

c. If the Entity changes how they manage the contract or elements of it (e.g. changing from destruction by pulping to destruction by shredding).

d. If the Entity ends the service by bringing HIA in-house.

4.12. Digitizing Medical Record

4.12.1. To improve the efficiency and management of Data Subject information, Entities must digitize physical medical records into electronic format records (e-health records) after maximum Two (2) years of the release of this policy.

4.12.2. Assets that must be digitized include: medical records, color text and documents.

4.12.3. Assets that is preferred to be digitized include: laboratory assets and radiology images.

4.12.4. Digital preservation must ensure that digital information remains accessible and usable.

4.12.5. Quality control of digitized records must be conducted:

a. Digitized document images must be inspected visually / Scroll through to ensure scanned documents are complete, clear, and easily read.

b. Digitized records must be compared to the original paper document/physical record to ensure accuracy.

c. Digitized records must be accessible and readable for their full retention period. This includes finding the file, opening the file, and reading the file regardless of the software used in its creation.

4.12.6. The content of physical records should only be destroyed once they have been digitized to the required standard and quality assurance of the digitized images has been completed, confirming that they are a like for like copy of the original physical records. The physical record itself can be destroyed after Sixty (60) days of quality control.

4.12.7. If the condition of the original record prevents a good quality digitized image from being produced; the Entity should document the problem on the digitized record and indicate that the physical copy has been maintained and where it is located.

4.12.8. Digital information must be recovered in an accessible format; in addition to providing information about those who have accessed the record.

4.12.9. Digital continuity must be maintained in a way that digital information will continue to be available as needed despite advances in digital technology and the advent of newer digital platforms.

4.12.10. Entity must ensure that digitized records are stored in a secure folder and only available to those who need access to the records.

4.12.11. Entity must ensure the archived digitized records are having required security controls.

4.12.12. An inventory must be created providing information about who have accessed the digitized record and when.

4.12.13. All incidents of potential data protection and confidentiality should be reported immediately to the Entity`s data protection officer.

4.13. Hardware (Biomedical & non-biomedical) Management

4.13.1. Hardware must be controlled and accounted at all times through the Asset management Department or (if biomedical equipment) Clinical Engineering Department.

4.13.2. All hardware must be assigned an owner specified in the Asset register.

4.13.3. There must be a record of the movements of all hardware containing PHI, containing the owner and the designated individual(s) responsible for the movement.

4.13.4. The movement of hardware must be authorized and logged by the appointed HIA management department within the Entity prior to the

hardware and electronic media entering or leaving a facility.

4.13.5. The HIA management department within the Entity must be accountable for hardware while in transit between facilities.

4.13.6. Hardware must be properly logged and securely disposed of when no longer used.

4.13.7. Protected Health Information must be removed from hardware before it is made available for reuse or dispose; and there shall be a reasonable assurance that the disposed data is not recoverable.

4.13.8. A retrievable, exact copy of PHI, (when needed or requested) must be created before any movement of hardware.

4.13.9. Before destructing HIA media, it must be sanitized by reformatting the hard drive in a secure manner or by using a wipe out utility.

4.14. Removable Media Management

4.14.1. Removable media must be stored in secure environment and in accordance with the manufacturer`s specifications.

4.14.2. Previous contents of any re-usable media must be completely erased before handing it to next custodian and reasonable assurance must be provided that the data is not recoverable.

4.14.3. Wherever mandated, cryptographic techniques must be applied to protect data on removable media.

4.14.4. Health information assets sent outside the Entity for repair or data recovery must be protected from disclosure by mutually agreed contract.

4.14.5. Record of the HIA movement must be maintained to keep an audit trail.

4.15. Health Information Assets Business Continuity Plans

4.15.1. Entities must have documented business continuity policy and plans that can be activated in a timely manner to retain/retrieve HIA in case of service discontinuation in the event of a disaster. Service discontinuity can be due to:

a. Natural and environmental threats such as earthquakes, hurricanes, extreme weather, floods, fire, etc.

b. Human factors involvement such as technology failures, terrorism, bio-terrorism, chemical/radiological/nuclear event, etc.

4.15.2. The business continuity plan should be tested on periodic basis.

4.15.3. Entities must identify competent trained staff responsible for HIA business continuity.

4.16. Destruction Process of Health Information Assets

4.16.1. Entity must conduct regular audit to appraise it`s HIA retention time and decide for permanent retention, or secure destruction.

4.16.2. If, as a result of appraisal, a decision is made to dispose/destroy an HIA, there must be evidence of the decision.

4.16.3. In the absence of investigation, litigation or legal hold; HIA that have satisfied their legal, financial, administrative and archival requirements may be destroyed in accordance with retention outlined in this policy.

4.16.4. Original health records may be destroyed only when they are in excess of the retention period and have satisfied the requirements as mentioned in this policy.

4.16.5. The HIA must be disposed-off in a secure manner at the end of their intended life cycle with proper authorization from the Entity`s Executive leader/Medical Director with a designated function to appraise HIA.

4.16.6. Health information asset destruction is applicable to all HIA including Devices, Softcopy and hardcopies of documents.

4.16.7. The Entity has a legal obligation to maintain confidentiality standards for all HIA archiving and disposal.

4.16.8. Medical records must be destroyed in a manner that does not allow the information to be retrievable, recognizable, reconstructed or practically read.

4.16.9. The Privacy Rule in DHA policies prohibits digital and paper records containing confidential information from being thrown away in a public dumpster or recycling bin. The records must be rendered unreadable or indecipherable by shredding, burning or other destruction.

4.16.10. Destruction of all equipment or hard drives must be in a controlled method:

a. All devices / equipment must be checked to ensure all Protected Health Information (PHI) are removed, and licensed software are erased, securely overwritten or destroyed prior to disposal.

b. Hard disks must be degaussed or physically destroyed.

c. Before destructing information asset media, it must be sanitized by reformatting the hard drive in a secure manner or by using a wipe out utility.

d. Media destruction techniques such as pulverizing, degaussing, abrasion shall be considered.

4.16.11. In case of Entity Closure or moving to new EMR, Approval for

destruction/disposal/Transfer of HIA must be taken from DHA_Health Informatics and Smart health Department (HISHD) (HISH@dha.gov.ae).

4.16.12. Destruction implies a permanent action. Entities must ensure HIA are destroyed with a method that provides no possibility of reconstruction of information. For digital records, it should meet the ISO 27001 standard, as the information should not be recovered or reversed.

4.16.13. Destruction can be conducted in-house or under contract with a certified offsite company.

4.16.14. If destruction of the HIA is outsourced to a business associate:

a. The Entity, as the controller, is responsible for ensuring the Destruction provider companies/Business associates chosen to carry out offsite destruction meets the necessary requirements and can evidence this. This evidence should be checked as part of due diligence (for example, if the business associate says they have the ISO accreditation, then it should be checked with the ISO).

b. Other diligence activities, such as a site visit to the business associate, should also be carried out by Entity`s representative.

c. The contract between the Entity and Destruction provider

companies/Business associates must provide that the business associate will establish the permitted and required uses and disclosures; including the following elements:

i. The method of destruction.

ii. The time that will elapse between acquisition and destruction.

iii. Safeguards against breaches.

iv. Indemnification for the Entity due to unauthorized disclosure.

v. Requiring the business associate to maintain liability insurance in specified amounts at all times.

d. The Entity must mandate the destruction provider companies/Business associates to provide a certification of destruction that contains the following information:

i. Date of destruction.

ii. Method of destruction.

iii. Description of the destroyed records.

iv. Inclusive dates covered

v. A statement that the records have been destroyed in the normal

course of business; and Data destroyed cannot be recoverable.

vi. The signatures of the individuals supervising and witnessing the destruction.

4.16.15. The Entity must maintain certification of destruction Indefinitely.

4.16.16. Upon request, the Entity must provide the DHA with the certificate of destruction.

4.16.17. Examples of destruction methods are provided below:

Type of Health Information Asset	Destruction method
Paper record	Burning, shredding, pulping, and pulverizing
Microfilm or microfiche	Recycling and pulverizing
Laser discs used in write once-read many document-imaging applications	Pulverizing
Computerized data	Magnetic degaussing
DVDs	Shredding or cutting
Magnetic tapes	Demagnetizing

4.17. Register of Health Information Assets Destroyed After Retention Period

4.17.1. Health Information Assets that have reached their official retention period

should be reviewed under the criteria issued within this policy to assess if they should be destroyed.

4.17.2. Before destruction, Entities must maintain a register comprising the following:

a. Name of the HIA.

b. Healthcare record number

c. Subject of care first name, surname, address, and date of birth.

d. Description of the disposed HIA

e. Former location of HIA.

f. Date of destruction

g. Method of destruction

h. Inclusive dates (e.g. the time period during which the HIA was created, maintained, or stored)

i. A statement that the records were destroyed in the normal course of business

j. The signatures of the individuals supervising and witnessing the destruction

4.17.3. The register of HIA destroyed should be maintained indefinitely as proof that the HIA no longer exists.

4.18. Closing an Entity or merging Entities

4.18.1. The obligation to make HIA available to Data Subjects/patients and other healthcare professionals continues even after closure/merging of an Entity.

4.18.2. Retention times for HIA outlined in this policy must be maintained regardless of changes in ownership, closure of the Entity, or changes in the information technology systems within the Entity.

4.18.3. Prior to closing/merging an Entity, Data Subjects/patients (e.g. those seen within 25 years) should be notified. The notice should be given at least 60 days in advance, with 90 days being the best practice.

4.18.4. The notice should be given in the local newspaper in addition to one of the below ways:

a. Individual letter to the last known Data Subject/ Patient address.

b. Electronically, if this is a normal method of clinical communication with the Data Subject/patient.

c. SMS (Short Message Service).

4.18.5. Below clarification should be contained within the notice to Data Subject/Patient:

a. Explaining that the Entity plans to transfer their care, and pass on the relevant health information about their condition and medical records to another Entity within the organization/merging Entities/Custodian Entity.

b. Ensuring the Data Subjects know who will be responsible for their future care or treatment.

c. Informing the Data Subject that in this closing/merging process their medical records will be disclosed and transferred; and that without that disclosure, referral and archiving of the HIA is not possible.

d. Informing the Data Subject that in case they DO NOT consent for medical record transfer; then they have the option of taking over their medical records within 60 days of notice release.

e. Containing name, telephone number, and mailing address of the responsible person within the Entity to contact for obtaining medical records or requesting transfer of records.

f. Explaining how the medical records can be obtained or transferred.

g. Clarifying the format of the records, whether hard copy or digitized.

h. Explaining retention period for the records before they are destroyed.

4.18.6. Where an Entity is part of a larger system/organization, transition of HIA upon closing must be managed within the organization.

4.18.7. When Entities amalgamate or merge, the HIA from both systems/organizations must be maintained with integrity, and HIA from both Entities must remain accessible.

4.18.8. If the closing Entity is stand alone health facility, then:

a. Within the notice to Data Subject/Patient, it should be clarified that the Entity plans to transfer their care, and pass on the relevant medical records along with HIA to a Custodian Entity.

b. There must be a contract between the Stand alone closing Entity and Custodian Entity containing all the details for HIA keeping.

c. The closing Entity must digitize whatever that can be digitized, and move all HIA to custodian Entity. If the condition of the original records prevents a good quality digitized image from being produced; then it must be transferred as it is to the Custodian Entity.

4.18.9. If the Data Subject did not show interest in taking over the associated

medical records, then the Entity must transfer all medical records to another Entity within the organization/merging Entities/or Custodian which is responsible for records retrieval.

4.18.10. Entity`s managements should involve financial and legal advisors to ensure all HIA management options are evaluated and decisions are made in the context of the broader closure plan.

4.18.11. It is important to work with the information technology department to perform an inventory of the systems that manage HIA.

4.18.12. If the practice closes due to the practitioner's death; the practitioner's Entity becomes the owner of the HIA and should provide this notification to Data Subjects.

4.19. All Health Entities Must

4.19.1. Develop a HIA management policy and procedures to ensure all HIA obtained, held, recorded, used, archived and disposed of, are handled within the safeguarding principles of the UAE laws, Emirate of Dubai Legislations, and DHA regulations, in a secure and confidential manner.

4.19.2. Establish appropriate storing, archiving, retention and destruction schedules/process.

4.19.3. All HIA management policies and procedures should be reviewed at regular intervals (at least once every two years) and should be amended to maintain its compliance with recent UAE and DHA laws and regulations.

4.19.4. Comply with all UAE federal, Emirate of Dubai, and DHA regulatory requirements governing E-Health, Telehealth, Electronic Health Information Exchange (HIE), Data Protection, Data Quality, Data Classification (https://www.dha.gov.ae/en/licensing-regulations-Nabidh), Data Privacy, Transparency, Cybersecurity, and Information security.

4.19.5. Recognize Health Information Assets management as a specific corporate responsibility within the Entity; by providing a managerial effort for management of HIA of all types, in all formats throughout their lifecycle, from creation to ultimate disposal.

4.19.6. A designated member of staff of appropriate seniority, ideally with suitable HIA management qualifications, should lead responsibility for HIA management within the Entity. This lead role should be formally acknowledged, included in relevant job descriptions and communicated throughout the Entity. When new IT projects or upgrades are introduced, the person responsible for HIA Management should be closely involved.

4.19.7. Ensure HIA is available to meet the needs of continued Data Subject/patient

care, legal requirements, research, education, and other legitimate uses of the Entity.

4.19.8. Maintain a HIA inventory that specifies what HIA is kept, the time-period for which it is kept, and the storage medium on which it will be maintained.

4.19.9. The HIA inventory must contain a minimum information below:

a. Health Information Asset name.

b. Health Information Asset description.

c. Health Information Asset type.

d. Health Information Asset classification.

e. Health Information Asset location.

f. Health Information Assets Custodian.

g. Health Information Asset owner.

h. Health Information Asset retention period.

4.19.10. The Entity must review /update HIA classification and retention inventory at regular basis (at least yearly); or whenever there is a significant addition/deletion/modification of the HIA.

4.19.11. Entities must have in place appropriate administrative, technical and physical safeguards to monitor HIA management and to ensure HIA within their facilities are managed in line with the requirements specified in this Policy.

4.19.12. Encompass a HIA management system within the Entity that cover all stages of the asset`s lifecycle:

a. Creation: create and log information asset.

b. Using: use or handle information asset securely.

c. Retention: keep or maintain information assets in line with DHA recommended retention schedule.

d. Appraisal: determine whether information assets should go through archival preservation.

e. Disposal: dispose information assets appropriately according to DHA policies.

4.20. Training

4.20.1. Entities must train all workforce members i.e. employees, trainees, vendors, contractors and anyone over whom the Entities exercise direct control on its HIA management policies and procedures, as necessary and appropriate for them to carry out their functions.

4.20.2. No Data Subject/Patient HIA or systems should be handled or used until training has been completed. Training should be done through generic and Entity-wide training programmes.

4.20.3. The Entity should have a process to periodically appraise the competency of the staff and other resources including third party vendors on HIA management.

4.20.4. The Entity should review the training and awareness courses periodically to reflect current UAE laws and DHA health information governance regulatory requirements.

4.21. Accountability

4.21.1. The Entity is responsible for complying with all UAE laws and DHA`s policies and regulations, and must demonstrate its compliance.

4.21.2. The Entity has a legal obligation to maintain all HIA as per this policy.

4.21.3. It is the responsibility of the Executive leader/Director to ensure the Information Governance Lead/ HIA management Officer are enforcing the required policies and procedures within their Entity and that all staff members are aware of both their corporate and individual responsibilities regarding the HIA management.

4.21.4. Entities must apply appropriate sanctions against staff, trainees, vendors and third party contractors who violates HIA management policies and procedures.

4.21.5. Entities will be asked for evidence to demonstrate their fulfilment of the required HIA management regime to the DHA.

4.22. Non-Compliance

4.22.1. A failure to adhere to this policy is considered a violation that requires investigation. Disciplinary action / dismissal will be taken in accordance with the provision of the current legislations.

5. References

5.1. Federal Law No. (2) of 2019, Concerning the Use of the Information and Communication Technology in the Area of Health ("ICT Health Law"). Available on: https://www.dha.gov.ae/en/licensing-regulations-laws

5.2. Resolution No. (2) of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai. Available on: https://www.dha.gov.ae/en/licensing-regulations-laws

5.3. Law No. (26) Of 2015 Regulating Data Dissemination and Exchange in the Emirate of

Dubai. Available on https://www.dha.gov.ae/en/licensing-regulations-laws.

5.4. Cabinet Decision No. (32) of year 2020 on the Implementing Regulation of UAE Federal Law No. 2/2019 on the Use of Information and Communication Technology in Health Fields. Available on: https://www.dha.gov.ae/en/licensing-regulations-laws

5.5. Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data (United Arab Emirates). Available on: https://www.dha.gov.ae/en/licensing-regulations-laws

5.6. Ministerial Decision no. (51) of 2021 concerning the health data and information which may be stored or transferred outside the country. Available on: https://www.dha.gov.ae/en/licensing-regulations-laws

5.7. The Telecommunications and Digital Government Regulatory Authority (TDRA) of the United Arab Emirates (UAE). Available on: https://www.tdra.gov.ae/en/about-tra/about-tra-vision-mission-and-values.aspx

5.8. Federal Law No. (5) Of year 2012 on Combatting Cybercrimes and its amendment by Federal Law No. 12 of 2016. Available at: http://ejustice.gov.ae/downloads/latest_laws2016/unionlaw12_2016_5_2012.pdf

5.9. Cabinet Resolution No. (24) Of Year 2020 On the Dissemination and Exchange of Health Information Related to Communicable Diseases and Epidemics and Misinformation Related to Human Health. Available at:

https://www.dha.gov.ae/en/licensing-regulations-laws.

5.10. Federal Decree Law No. (4) Of Year 2016 on Medical Liability. Available at: https://www.dha.gov.ae/en/licensing-regulations-laws

5.11. Executive Council Resolution No. (32) of year 2012 on Regulating the Entity of health professions in the Emirate of Dubai. Available at: https://www.dha.gov.ae/ar/HealthRegulation/Documents.pdf

5.12. Law No. (13) of 2021 establishing the Dubai Academic Health Corporation, and Law No. (14) of 2021 amending some clauses of Law No. (6) of 2018 pertaining to the Dubai Health Authority (DHA). Available on : https://www.dha.gov.ae/en/licensing-regulations-laws

5.13. Dubai Health Authority Nabidh policies and standards. Available on: https://www.dha.gov.ae/en/licensing-regulations-Nabidh

5.14. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the Emirate of Dubai. Available on https://www.dha.gov.ae/en/licensing-regulations-Nabidh

5.15. Dubai Health Authority Policy for Health Information assets classification. Available on : https://www.dha.gov.ae/en/licensing-regulations-Nabidh

5.16. Dubai Health Authority Policy for Health Data Protection and Confidentiality.

Available on : https://www.dha.gov.ae/en/licensing-regulations-Nabidh

5.17. Dubai Health Authority Policy for Health Data Quality. Available on : https://www.dha.gov.ae/en/licensing-regulations-Nabidh

5.18. Dubai Health Authority Code of Ethics and Professional Conduct (2014). Available on: https://www.dha.gov.ae/Documents/HRD/RegulationsandStandards/guidelines/Code%20of%20Ethics%20and%20Professional%20Conduct%20-%20final.latest.pdf

5.19. Dubai Government Information Security Regulation (ISR). Available on: https://www.desc.gov.ae/regulations/standards-policies/

5.20. UAE National Electronic Security Authority (NESA). Available on: https://logrhythm.com/solutions/compliance/uae-national-electronic-security-authority/

5.21. UAE Federal Law No. (7) of 2008 on national archive. Available on: https://www.na.ae/ar/Images/NA-Law2014-E.pdf

5.22. Requirements for an Information Security Management System (ISMS), ISO 270001. Available on: https://www.iso.org/isoiec-27001-information-security.html

5.23. The General Data Protection Regulation (GDPR) (from Must 2018). Available on:

https://gdpr-info.eu/art-84-gdpr/

5.24. AHIMA Record Retention Recommendation. Available on: https://library.ahima.org/PB/RetentionDestruction#.YjHBVOpByUn

5.25. A pilot comparison of medical records sensitivity perspectives of patients with must behavioral health conditions and healthcare providers. Hiral Soni, Julia Ivanova, Adela Grando, Anita Murcko 1, Darwyn Chern, Christy Dye 2, Mary Jo Whitfield 3 Health Informatics J. Apr-Jun 2021; 27(2): 14604582211009925. Available on: https://doi.org/10.1177/14604582211009925

5.26. Amy Dickens. From Information to Valuable Asset. The Commercialization of Health Data as a Human Rights Issue. Health Hum Rights. 2020 Dec; 22(2): 67–69.

5.27. Strong, K. (2008). Enterprise Content and Records Management." Journal of AHIMA, 80, 38–42. Available on: https://library.ahima.org/doc?oid=77921#.Yt443XZByUk

5.28. Requirements for the retention of laboratory records and diagnostic material (seventh edition 2018). Available on: https://www.health.gov.au/internet/main/publishing.nsf/content/B8562E2C3D131ED8CA257BF00019153C/$File/20180612%20-%20Final%20-%20Retention.pdf

5.29. The College of American Pathologists makes the following recommendations for the

minimum requirements for the retention of laboratory records and materials. Available on: https://elss.cap.org/elss/ShowProperty?nodePath=/UCMCON/Contribution%20Folders/WebApplications/pdf/retention-laboratory-records-and-materials.pdf

5.30. AHIMA's Practice Brief on Retention and Destruction of Health Information.

5.31. Government of Canada (2015). Personal Information Protection and Electronic Documents Act. Available on : http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html

5.32. Information Governance Alliance (2016). Records Management Code of Practice for Health and Social Care 1, 1-80. Available on: https://digital.nhs.uk/article/1202/Records-ManagementCode-of-Practice-for-Health-and-Social-Care-2016

5.33. Joint Commission International Accreditation Standards for Hospital, 7th Edition, (2021) Available on : https://www.jointcommissioninternational.org/-/media/jci/jci-documents/accreditation/hospital-and-amc/jci-errata-standards-only_7th-ed-hospital.pdf

5.34. Health Insurance Portability and Accountability Act. Available on: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

5.35. Medical Encyclopedia (2017). Apgar score Medline Plus. Available on : http://www.nlm.nih.gov/medlineplus/ency/article/003402.htm

5.36. National Health Service (NHS) Digital (2017). Data security and information governance. Available on : https://digital.nhs.uk/data-security-information-governance

5.37. National Institute for Health and Care Excellence (2017). Surgical Care. Available on : https://www.nice.org.uk/guidance/service-delivery--Entity-and-staffing/surgical-care

5.38. Retention of dental record. Available on: https://www.mddus.com/resources/publications-library/soundbite/soundbite-issue-18/knowing-when-to-let-go

5.39. NHS Records Management Code of Practice 2021. Available on: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/

5.40. General Records Retention Schedules for State Agencies. Available on: : https://ctstatelibrary.org/publicrecords/general-schedules-state

5.41. Records Disposition Authorization - State Agencies. Available on: https://ctstatelibrary.org/publicrecords/state

5.42. Records Disposition Authorization of Original (Non-Permanent) Paper Records Stored As Digital Images. Available on: https://ctstatelibrary.org/publicrecords/state

5.43. NHS Records Management Code of Practice 2021. Available on: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/

5.44. Scotland records management health and social care code of practice 2020. Available on: https://www.informationgovernance.scot.nhs.uk/rmcop2020/

5.45. Good Management, Good Records - Disposal Schedule. Department of Health. Available on: https://www.health-ni.gov.uk/publications/good-management-good-records-disposal-schedule

5.46. Dental Recordkeeping Guidelines. https://www.cdsbc.org/CDSBCPublicLibrary/Dental-Recordkeeping-Guidelines.pdf

5.47. CAP Minimum Period of Retention of Laboratory Records and Materials. https://elss.cap.org/elss/ShowProperty?nodePath=/UCMCON/Contribution%20Folders/WebApplications/pdf/retention-laboratory-records-and-materials.pdf

5.48. Clinical policy on retention, storage and disposal/destruction of medical records. Available on: https://health.uconn.edu/policies/wp-content/uploads/sites/28/2021/07_/Retention-Storage-and-Disposal-Destruction-

of-Medical-Records-2014-06.pdf

5.49. The royal college of radiologists code of radiology record retention protocol. https://www.rcr.ac.uk/sites/default/files/position_statement_records_management_code_practice.pdf

5.50. Department of health Australia Information Retention and Disposal Policy. https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Storage-and-Disposal/Information-Retention-and-Disposal-Policy