قطاع التنظيم الصحي

Health Regulation Sector

Document Type: Health Information Policy	**Ref No:** DHA/HRS/HISHD/HIACP/1/2021		**Version Number:** 1
Document Title: Policy for Health Information Assets Classification		**Effective Date:** 29/12/2021	**Revision Date:** 29/12/2024
Ownership: Health Regulation Sector			
Applicability: All Healthcare Entities under the Jurisdiction of Dubai Health Authority			

1. Purpose

1.1. To set out Dubai Health Authority (DHA) `s requirements for Classifying Health Information Assets (HIA) in the Emirate of Dubai; in line with the UAE and Emirate of Dubai legislative, regulatory frameworks, and necessities.

1.2. To outline the requirements and responsibilities of healthcare Entities working under jurisdiction of DHA on HIA classification.

1.3. To ensure that the applicable and relevant security controls are set in place for HIA in line with relevant UAE and Emirate of Dubai legislative and regulatory requirements.

2. Scope

2.1. All HIA within the Emirate of Dubai handled by healthcare Entities under jurisdiction of DHA.

2.2. These 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 below information assets in health Entity :

2.2.1. Medical and non-Medical information (e.g. Administrative, HR, etc.).

2.2.2. Identifiable and De-identifiable data.

2.2.3. Data Accessed for primary or secondary use.

2.2.4. Physical or digital forms of data.

2.3. All users accessing and using information in healthcare sector in the Emirate of Dubai; including all employees, contractors, consultants, suppliers, vendors, partners, customers and wider stakeholders where appropriate.

3. Definitions/Abbreviations:

Audit: Systematic and independent examination of HIA classification to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).

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

Classification: means assigning categories to assets on pre-set criteria. In information security classification is used to categorize information assets in terms of sensitivity to protect it from unauthorized access, use, disclosure, disruption, modification or destruction.

Classified information assets: information assets/material or data that an Entity claims as sensitive, secret, or confidential that requires protection of its confidentiality, integrity, or availability. Access to these information is restricted to people, process or other parties.

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 nondisclosure of certain information assets expect to an authorized individual as per the classification level of the asset.

Custodian: is defined as an individual or Entity that has approved responsibility for maintaining an information asset.

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

External parties: an individual or organization that deals with the Entity through a business relationship and has access to Entity`s health information.

Data: All that can be stored, processed, generated and transferred by Information and Communications Technology (ICT) such as numbers, letters, symbols, images and the like.

Data Collection: A systematic gathering or organized collection of data, in any format, for a particular purpose, including manual entry into an application system, questionnaires, interviews, observations, existing records, and electronic records.

Declaration of Maturity: is a comprehensive assessment of Entity’s capability to classify, handle, store, archive and dispose HIA as per existing Laws and regulations.

De-identified Health data: De-identified health data is patient data that has been scrubbed of important identifiers such as birth date, gender, address, and age. De-identified patient data is often used for research.

Electronic Medical Records: Subject of care Administration System used across the Entity to record subject of care activity in real time. Management of the system is in conjunction with the Health regulation electronic records requirements.

Electronic Platform: An electronic system composed of hardware; software; networks; storage systems; and a connectivity and communication site, via which Dubai Data are disseminated and exchanged.

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 and medical centre, telemedicine provider, laboratory and diagnostic centre, and pharmacy, etc.

Exchange of Health Information: Access, exchange, copying, photocopying, transfer, storage, publication, disclosure or transmission of health data and information.

Health Information: Health data 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.

Identifiable Health Data: Data are considered “individually identifiable” if they include any of the 18 types of identifiers specified by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code)
- All elements (except years) of dates 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
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual.

Incidents: an incident can be thought of as violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practice.

Information and Communication Technology: Technical or electronic tools or systems or other means that enable the processing of information and data of all types, including the possibility of storage, retrieval, dissemination and exchange.

Information assets: 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. The following are considered HIA:

(a) Information (in physical and digital forms)

(b) Medical device and equipment

(c) Applications and Software

(d) Information System

(e) Physical Infrastructure (Data center, access barriers, electrical facilities, HVAC systems, etc.)

(f) Human resources (in support of care delivery)

Information Asset Owner: A senior member of Entity who is the nominated owner for one or more identified HIA of the Entity.

Information Assets classification: is the process of categorizing all HIA, based on its sensitivity, business value and context, and determines the level of safeguards that are applied to the information.

Information Governance (IG) Office/Section: is the point of contact for all enquiries related to:

(a) Data protection

(b) Freedom of information

(c) Records management

(d) Information risk management

(e) Information security

(f) Business continuity

Internet Protocol (IP) address: is a unique address that identifies a device on the internet or a local network.

NABIDH: A health information exchange platform by the Dubai Health Authority that connects public and private healthcare facilities in Dubai to securely exchange trusted health information.

Need-to-Know: A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties.

Primary use: The information collected by the healthcare provider for the primary purposes of giving treatment and health care to the subject of care.

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

Secondary use: The secondary use is use of personal health information for purposes other than treating the individual subject of care, including but not limited to Research, Public Health, Quality Improvement, Safety Initiatives, payment and marketing. Some secondary uses directly complement the needs of primary use. Examples include medical billing, hospital administrative, and management operations.

Subject of care: An individual approaching the health services in the Emirate of Dubai.

System: A set of electronic data and health information exchange operations, involving a set of electronic parts or components that link together and work together to achieve a specific goal.

Very Important Person (VIP) Criteria:

(a) Senior visitors (leaders and heads of state)

(b) Foreign ministers during their visit to the UAE

(c) Ambassadors and Delegates in the UAE

(d) Ministers and Undersecretaries of the Ministry of the UAE

(e) Chairmen and Undersecretaries of the government departments of the UAE

(f) Royals and crown princes of the UAE and other Emirates including their immediate family members (wives, sons, daughters, brothers and sisters)

(g) Al Nahyan and Al Maktoum family members

(h) Members with prefix “Sheikh” or “Sheikha” in their official identity

(i) Members with prefix “High Excellence” or “Her Excellence” in their official identity.

DHA	:	Dubai Health Authority
EMR	:	Electronic Medical Records
HIA	:	Health Information Assets
HISHD	:	Health Informatics & Smart Health Department
HRS	:	Health Regulation Sector
ICT	:	Information and Communications Technology
IG	:	Information Governance
IP address	:	Internet Protocol address
VIP	:	Very Important Person

Term	Meaning / Application
Must	This term is used to state a **mandatory** requirement of this Policy
Should	This term is used to state a **recommended** requirement of this Policy
May	This term is used to state an **operational** requirement of this Policy

4. Policy Statement:

4.1. The Health Information Assets (HIA) classification policy is an integral part of the DHA's approach to Information Governance (IG). This policy must be read in conjunction with other related DHA_Health Regulation Sector (HRS)_Health Informatics & Smart Health Department (HISHD)_IG policies and regulations.

4.2. All HIA generated by Health Entities must be subject to classification into one of the following sets based on value and sensitivity of the information, and the consequences of Information compromise:

4.2.1. Open Data /Public

4.2.2. Confidential

4.2.3. Sensitive

4.2.4. Secret

4.3. Information compromise includes, but is not limited to:

4.3.1. Data loss.

4.3.2. Data misuse.

4.3.3. Data interference.

4.3.4. Data unauthorised access.

4.3.5. Data unauthorised modification.

4.3.6. Data unauthorised disclosure.

4.4. As per Resolution No. (2) of 2017, on Approving the Policies for Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai:

"Personal Data that reveals information about or is, directly or indirectly, related to a Person's family; racial, ethnic, or social origin; affiliations; political views; religious or philosophical beliefs; criminal record; membership in unions; health; or personal life" is considered as Sensitive data.

4.5. A limited subset of information could have more damaging consequences (for individuals, the health sector, or the UAE Government generally) if it was lost, stolen or published in the media. Where information is identified as such, it must be clearly marked as Secret.

4.6. The Sensitive and Secret data require the Entity to impose measures (generally procedural or personnel) to reinforce strict controls while accessing, storing, sharing, and disposing. Example of these controls are:

4.6.1. Subject of care/ Patient consent

4.6.2. Data sharing agreement

4.6.3. Encryption of Data

4.6.4. Anonymization of information.

4.7. Secret data are the utmost critical information, requiring the highest levels of protection from the all types of threats. Unauthorized access to Secret data might cause significant damage to the following:

4.7.1. The ability of a Federal Government or a Local Government to perform its duties.

4.7.2. The operational effectiveness of highly valuable security procedures.

4.7.3. Diplomatic relations with any country or international organisation.

4.7.4. Safety, security, or prosperity of the UAE; or any other country, by affecting its commercial, economic, or financial interests.

4.7.5. Security of critical national infrastructure.

4.7.6. The operational effectiveness of the police authorities or military forces of the UAE in a way that causes them to encounter, in the course of performing their duties.

4.7.7. Public interest or national security of the Emirate of Dubai or the UAE.

4.7.8. Domestic stability of the Emirate of Dubai or the UAE.

4.7.9. Capabilities or security of the UAE or its allied forces, leading to their inability to perform military duties.

4.7.10. Long-term damage to the economy of the Emirate of Dubai, or UAE.

4.7.11. Private Entity that has a vital and strategic role in the national economy, resulting in heavy financial losses, bankruptcy, or loss of its leading role.

4.7.12. The safety and lives of certain personnel of the police, security, or military authorities; or of witnesses in critical court cases.

4.7.13. Security and the administration of justice, or obstructing investigations into serious crimes or prosecution of perpetrators.

4.7.14. Invading any Intellectual Property Rights.

4.7.15. Causing heavy loss of life.

4.8. The classification of HIA is wholly based on the examination of the value of the information, who will have access to the HIA, and the resulted risk impact if the information was compromised or accessed by unauthorized individuals:

Classification	**Category Description**	**Risk Impact of Information Compromise**	**Examples**
Open Data/Public	• Information intended to be used in public domain or public use, and has no legal, regulatory or organizational restrictions for its access and/or usage. • Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping	**No impact**	• Public Domains • Patient information leaflets • Press release / announcements • Regulatory filings, such as Internal Revenue Service filings • Certification labels such as The Joint Commission Certification • Research publications • General public health awareness or regulation awareness publications

	citizens, patients and other stakeholders understand better the country's/ governmental/organizational vision and values. • Encryption recommended. • The use and release of open data must comply with applicable copyright laws.		• General sales or marketing materials • Business contact information. • Etc.
Confidential	• Information that must be afforded **limited confidentiality protection** due to its use in the day-to-day operations. • Information that relates to the internal functioning of the Entity and will not have general relevance and applicability to a wider audience. • Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary, if they were to be revealed.	• Its compromise may violate UAE federal law, Emirates of Dubai local law, and/or DHA policies and regulations. • Cause **limited** damage to the public interest, Entity/ individual reputation, • Limited financial aspects damage. • Adversely affecting the Entity by limiting its competitiveness • Adversely affecting public safety or justice.	• Routine business operations and services. • Minutes of meetings, internal Policies, Standard Operating Procedures and Internal Circulars, Contract of non-critical projects, projects charters, and Entity`s performance reports. • Correspondence within the Entity or with other Entities or third parties. • Financial reports and transactions. • Confidential decision-making documents. • Internal regulations, policies, standards, procedures. • Etc.

Sensitive	• Information that requires **strong protection** due to its critical support to decision-making within the Entity, across health sector, and government. • Information that could disclose designs, configurations or vulnerabilities exploitable by those with malicious intent. • Information that the Entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody.	• The compromise of this information might violate UAE federal law, Emirates of Dubai local law, and/or DHA policies and regulations. • Lead to **significant disruption/loss** of emergency and heath care capabilities, loss of public trust in the health sector, or significant loss of reputation to the health sector with momentous coverage by the national and international press. • Adversely affecting the Entity by limiting its competitiveness. • Adversely affecting public safety or justice.	• Medical records and Personal health information. • Sensitive medical information: - Chemical dependency, - Human immunodeficiency virus infection - Mental health conditions - Behavioral health information - Psychotherapy notes, -Alcohol and substance abuse, - Reproductive health, - Genomic information, -Sexual health (including sexually transmitted diseases), - Child pregnancy data - Child abuse conditions. • Strategic/critical projects contract or RFPs • Audit reports • Risk/assets registers • Financial details in relation to projects or proposals • Information security incidents reports • Human resource files/Personal information about staff/Personally Identifiable Educational Records/Confidential information about the management of the Entity. • Court proceedings. • Adoption records.

			• Disciplinary records, complains, investigations minutes, violations. • Agreements or contracts of a secret nature between the Entity and another Entity within the UAE or internationally. • Etc.
Secret	• Information that requires **significant and multilevel protection** due to its highly sensitive nature.	• The disclosure of such information to the public or exchange within the Government on other than an authorized basis is **illegal** and may cause **very serious damage** to the Individuals, government, national security, social cohesion, economic viability and health of the country. • Information compromise could potentially threaten life; seriously prejudice public order, triggering discrimination, mistreatment, humiliation or undermining people's dignity or safety.	• Medical record of Very Important Person (VIP). • Security forces data. • Security reports, minutes, or orders. • Sensitive minutes and report of executive council and its committees. • Agreements/contracts between the Emirate of Dubai and another Emirate or between the UAE with another country. • Data relevant to witnesses of serious law suites. • Credit Card Details/Credit Card Details/Payment card information. • Controlled Technical Information ("CTI") • IP addresses. • Network & Infrastructure Diagrams. • Etc.

4.9. Assessing Risk of Potential Disclosure

As the total potential impact of information disclosure increases from Low to High, the classification of data should become more restrictive moving from Public to Secret. Below table can assist in classification of HIA within the Entity. If appropriate data classification is still unclear after considering these points, contact the DHA_HISHD for assistance (HISH@dha.gov.ae).

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality **Preserving authorized restrictions on information access and disclosure, including means for** protecting personal privacy & proprietary information	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity **Guarding against improper** information modification or destruction**, and includes ensuring information non-repudiation and authenticity.**	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability **Ensuring** timely and reliable access **to and use of information.**	The disruption of access to or use of information or an information system	The disruption of access to or use of information or an information system could be expected to	The disruption of access to or use of information or an information system could be expected to have

	could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

4.10. Health Information Assets Labelling

4.10.1. All HIA regardless of its form (Electronic or physical) must be appropriately labelled based upon the security classification category identified and the level of confidentiality the information needs.

4.10.2. To achieve clearly identifiable protective markings for physical documents, it is recommended:

a. Using capitals, bold text, large font and a distinctive colour (red preferred), for example SENSITIVE.

b. Placing markings at the centre top and bottom of each page.

c. Separating markings by a double forward slash to help clearly differentiate each marking.

4.10.3. The labelling system needs to be clear and easy to manage.

4.11. Health Information Assets Re-classification

4.11.1. The Entity must consider reclassification of the HIA at any point of time whenever there is a need to change the classification based on a reassessment of the potential impacts of its compromise.

4.11.2. Reclassification may raise or lower the security classification of HIA.

4.11.3. Declassification is the administrative decision to reduce the security classification of HIA when it no longer requires security classification handling protections.

4.11.4. The re-classification of HIA (in terms of either degrading or upgrading its classification) must be done by the information asset owner.

4.11.5. Since re-classification involves change in access control, appropriate pre-cautions/security controls must be considered against information disclosure.

4.12. Health Information Assets Access Permissions within the Entity

4.12.1. No Individual must access Confidential/Sensitive/Secret HIA without first obtaining an Access Permission from the Entity.

4.12.2. Entity must follow the principles of ‘need to know’ and ‘minimum necessary’ while providing access to Sensitive and Secret HIA and for the minimum extent required for processing / purposes of the Entity’s operations.

4.12.3. Entity must periodically review the continuing necessity of HIA access.

4.12.4. The Entity must establish rules for protecting data, based on its classification, such as access restrictions or encryption.

4.12.5. Below table explains the HIA access control requirements:

Health Information Assets Access Control Requirements			
Open Data /Public	**Confidential**	**Sensitive**	**Secret**
• Available to the public. • Can be shared with third parties with no permission.	• Available to authorized users. • Shared by HIA owner consent.	• Available only to authorized users. • Information asset owner must consider more Stringent access control • Sharable across Government /Private Entities: - With the consent of the individual. - As required by contract, subject to appropriate non-disclosure restrictions and data sharing agreement. - Pursuant to a waiver of authorization issued by an authorized Institutional Review Board. • Access must be logged and reviewed by the information asset owner.	• Access to this information may be distributed only: • If required by law or regulation. • Pursuant to a lawfully issued order. • If necessary in the course of a legal proceeding.

4.13. Health Information Assets Sharing with Third Parties

4.13.1. Healthcare Entities must specify, in accordance with the provisions of this policy and as per the UAE ICT law, the Government and Private Entities that are authorised to access/share it`s Confidential/Sensitive Data:

d. Sharing of Sensitive Data with the UAE Ministry of Health and Prevention (MOHAP) is allowed within the framework of the UAE ICT law and through DHA_HISHD.

e. Sharing of Sensitive Data with other UAE Government Entities must be approved and facilitated by DHA_HISHD.

f. Sharing of Sensitive Data with Private third parties should be evaluated and approved by DHA_HISHD (HISH@dha.gov.ae).

4.13.2. A Data Sharing Agreement must be produced, agreed and signed by all parties prior to any health data containing Sensitive information being accessed or shared with any organisation or body external to the Entity.

4.13.3. The Data Sharing Agreement must contain relevant clauses, as denoted below:

a. Notifying subject of care and obtain their consent prior to disclosing identifiable health data to a third party.

b. Confidentiality and non-disclosure requirements.

c. A Non-Disclosure Agreement valid after end of the life of the data sharing agreement.

d. Security requirements to process (i.e. at store, at transfer, at disposal etc.) the HIA securely.

e. Providing health information timely when and as required.

f. Incident handling and reporting in case of HIA breach.

g. Retention requirements and secure information asset disposal.

h. Restriction clauses for no further subcontracting without permission of the Entity.

i. Liabilities and indemnifications.

j. Clause for periodic audits to ensure compliance.

4.13.4. Sharing of Confidential/Sensitive data for Secondary use (e.g. Research, Public Health, Quality Improvement, Safety Initiatives, Insurance, Payment, and Marketing) must be as per UAE and Emirate of Dubai legislative and regulatory requirements.

4.13.5. Access/sharing of Secret Health information with any governmental / private Entities must be granted only on below conditions:

a. If required by law or regulation.

b. Pursuant to a lawfully issued order.

c. If necessary in the course of a legal proceeding.

4.14. Health Information Assets Physical Security and Access Control Requirements

4.14.1. The Entity must establish policies and procedures for information security, access control of HIA and HIA handling, within the Entity.

4.14.2. Information should be made available for all authorised purposes and protected from unauthorised access.

4.15. Health Information Assets Storage, Archival, Retention, and Reuse Requirements

4.15.1. All HIA must be stored/reused/archived in a secure manner as per their classification.

4.15.2. All information servers must be located in a secure data centre within the UAE.

4.15.3. The Entity must ensure that health data is not transferred/stored out of the country as per UAE laws and regulations.

4.15.4. If data has to be transferred/stored out of the country; then it should be as per UAE ICT law exemptions and after getting approval from DHA_HISHD.

4.15.5. The information asset owner must ensure data is retained for the periods set out by UAE ICT law and related DHA_HISHD policies and regulations.

4.15.6. The information asset owner must ensure that appropriate security controls are considered while storing/reusing/archiving the HIA.

4.15.7. The UAE ICT Health Law requires that Health Data must be kept for a minimum of 25 years from the date on which the last health procedure was performed on the patient.

4.15.8. The Entity must:

a. Identify and enforce archival criteria (what and when to archive, how long to archive) and methods (physical/electronic archiving).

b. Preserve data during archive.

c. Maintain adequate record on archival.

4.15.9. The Entity must ensure that appropriate backup are maintained securely while storing/archiving the HIA.

4.15.10. Suggested HIA storage requirements are provided Below:

Health Information Assets Storage Requirements				
Category	**Open Data /Public**	**Confidential**	**Sensitive**	**Secret**
Printed Material	No special handling	• Store in a secure area. • Maintain a clear desk. Workforce members should "clear their desks" at the end of each workday. • Documentation must be labelled accordingly as Confidential/Sensitive/Secret. • Physical and environmental security measures (e.g. backups, storing in a fireproof cabinets …etc.) must be maintained to enable secure HIA processing, storage, communication/sharing, hosting and disposal.		
Electronic Documents	No special handling	• Storage on Entity`s-approved devices is required. • Control access and print capability. • Store on secure network drives only (not on hard drives or desktops). • Documentation owned and/or created by Entity must be labelled accordingly as Confidential/ Sensitive/ Secret.		
Medical devices and equipment	-	Specific attention to access control, authentication, authorization, handling procedures, risk log and disposal of medical equipment and devices is required.		
Electronic media (memory sticks, hard drives, CDs)	No special handling	• Storage on Entity`s-approved devices is required. • Control access and print capability. • Store on secure place. •Use Entity`s-approved encryption. • Backup media must be physically secured. • Backup media stored offsite must be encrypted. • Backup media must be made unreadable before		

		disposal.
Mobile Devices	No special handling	• Mobile devices must be configured to prevent unauthorized use. • All mobile devices must employ encryption. • Connections between authorized mobile devices and EMRs must be encrypted. • Mobiles should be stored on secure place.
E-mail	No special handling	• Secret data must not be shared through email. • for Sensitive data: • Use of corporate email system is required. • Limit the amount of personal health information being sent to only what is necessary. • Ensure that no personal health information is in the subject line of the email. • Personal health information should be sent as: - A secure, locked (e.g. .pdf) attachment which requires a password to open. or - As a link to the health information portal. • Read/received/delivery receipts should be used where possible. • Add a disclaimer to your signature that indicates that the email is confidential and intended only for the intended recipient. It should also instruct anyone who receives the email in error to delete or shred the misdirected mail and notify the sender. • Copies of the email and attachments should be maintained in the client file. The date, time, addressee of the email should be apparent.

4.16. Physical and Environmental Security

4.16.1. Physical environment and its security measures must be maintained to enable secure HIA processing, storage, communication/sharing, hosting and disposal.

4.16.2. The Entity must consider various measures or controls that protect HIA from loss of connectivity, ensure availability of information processing, enable storage (backup and archival) equipment(s), protecting medical equipment's/devices from theft, fire, flood, intentional destruction, unintentional damage, mechanical failure, power failure, etc.

4.16.3. Physical security measures should be adequate to deal with foreseeable threats and should be tested periodically for their effectiveness.

4.16.4. The following aspects of physical and environmental security should be considered by the Entity:

a. Physical protection of data centre and information processing equipment(s)/facilities.

b. Physical entry control for secure areas.

c. Medical devices/equipment(s) protection.

d. Heating, ventilation, and air conditioning of critical areas and work places.

e. Supporting mechanical and electrical equipment.

f. Surveillance of critical areas and work places.

g. Security and protection of physical archives.

h. Fire and environmental protection.

i. Visitor management.

4.17. Health Information Assets Disposal Requirements

4.17.1. The retention demands of UAE federal, Emirate of Dubai, and DHA_HISHD laws, regulations, and policies must be followed before physical or digital data is disposed.

4.17.2. All HIA must be disposed-off in a secure manner as per their classification at the end of their intended life cycle with proper authorization from the HIA owner.

4.17.3. The Entity must ensure that appropriate security controls are considered while disposing the HIA so that the information contained in it is irrecoverable.

4.17.4. Formal procedures for the secure disposal of HIA should be established to minimize the risk of confidential information leakage to unauthorized persons.

4.17.5. The Entity must maintain appropriate log for all HIA Reused/Destructed.

4.17.6. All media for disposal should be treated as confidential.

4.17.7. The Entity should maintain records, on media disposal. The records should be available for audit purposes for a period defined by the retention policy. The records should have, but not be limited to, the following fields:

a. Information asset owner.

b. Type of HIA.

c. Classification.

d. Disposal type.

e. Reason for disposal.

f. Retention expiry date (if data).

g. Data removal confirmation and evidence.

h. Disposal authorized by.

4.17.8. Destruction of media by a third party should be supervised and the third party should issue a certificate of destruction.

4.17.9. Suggested HIA disposal requirements are presented below:

Health Information Assets Reuse/Destruction Requirements				
Category	**Open Data /Public**	**Confidential**	**Sensitive**	**Secret**
Printed Materials	No special handling. Consider recycling.	• Must be discarded in appropriately identified document container for shredding or destruction (except if subject to a legal hold).		
Electronic media (memory sticks, hard drives, CDs)	No special handling.	• Media subject to a legal hold may not be reused. If other media are to be reused, all data must first be removed by Information Services. • Disposal of electronic media should be in a secure manner. • All discarded media must be destroyed following the requirements of ISO 27001:2013 and Information Security Regulation (ISR) standards from Dubai Smart Government.		

4.18. All Health Entities must

4.18.1. Adopt well-crafted Information governance policies with the relevant provision(s) of this policy and other related DHA_HISHD IG policies.

4.18.2. Maintain appropriate plans and procedures to ensure HIA within their facilities are classified in line with the data classification categories specified in this Policy.

4.18.3. Implement a classification scheme to indicate the need and priority for the secure protection of HIA in order to ensure that:

a. The appropriate level of sensitivity of information is recognised.

b. The appropriate protective measures are taken while collecting, using, handling, storing, transferring, archiving and disposing the HIA as per this policy.

c. All Employees are aware of different HIA sensitivity levels and can apply appropriate controls.

4.18.4. Ensure data designated as Confidential, Sensitive, and Secret is handled in accordance with the relevant provision(s) of this policy.

4.18.5. Must set the appropriate HIA classification and access as well as retention details, in accordance with relevant UAE laws, Emirate of Dubai Laws and regulations, and DHA_HISHD data governance applicable policies.

4.18.6. Apply an appropriate degree of protection to all HIA that needs to be collected, stored, processed, generated or shared to deliver services and conduct Entity`s business.

4.18.7. Comply with all international, UAE federal, and Emirate of Dubai new and existing related regulatory requirements governing E-Health, Telehealth, Electronic Health Information Exchange (HIE), Data Protection, Data Quality, Privacy, Transparency, Cybersecurity, and Information security.

4.18.8. Comply with all Articles detailed within 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 its exemptions.

4.18.9. Comply with Resolution No. (2) Of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai.

4.18.10. Comply with The Telecommunications and Digital Government Regulatory Authority (TDRA) of the UAE rules and regulations.

4.18.11. Comply with Dubai Government Information Security Regulation (ISR) rules and regulations.

4.18.12. Comply with UAE National Electronic Security Authority (NESA) rules and regulations.

4.18.13. Comply with requirements for Information Security Management System (ISMS), ISO 27001.

4.18.14. Comply with Cabinet resolution No. (40) Of 2019 and Federal Decree-Law No. (4) Of 2016, Concerning the Executive Regulation of on Medical Liability and Addendum Regulations and Conditions for Providing Telehealth Services.

4.18.15. Comply with UAE federal, and Emirate of Dubai Electronic Security Authority standards and guidelines for cyber security.

4.18.16. Comply with all DHA IG policies (e.g. Nabidh policies and standards, Health Data Protection & Confidentiality policy, Health Data Quality policy, and Health Data Security Policy).

4.18.17. Comply with "Dubai Electronic Security Centre" requirements as applicable.

4.18.18. Comply with "Smart Dubai Government" regulations and requirements as applicable.

4.18.19. Comply with DHA-Dubai health insurance corporation requirements for e-claims, reimbursement and documentations as applicable.

4.18.20. Ensure that assets received from or exchanged with Third Parties are protected in accordance with relevant UAE legislative or regulatory requirements, including this policy.

4.18.21. Maintain appropriate training and awareness strategies to support compliance with this Policy.

4.18.22. Ensure the employee with access to HIA have the necessary trainings to effectively perform their roles.

4.18.23. Have a process for periodically reviewing the competency of the staff and other resources including third party vendors.

4.18.24. Review the training and awareness courses periodically to reflect current health data governance regulatory, policy / procedure requirements.

4.19. Roles and Responsibilities

4.19.1. The Entity must establish and implement clear roles and responsibilities regarding the attainment and safeguarding of HIA.

4.19.2. The Information Governance (IG) Manager (or the job title assigned with responsibilities of managing IG) is responsible for enforcement and endorsement of this policy.

4.19.3. The IG Office/Section (or the function assigned with IG responsibilities) is responsible to support the relevant business Office/Section in implementation of the defined controls and ensuring compliance with this policy.

4.19.4. All HIA Users are responsible to read, understand, and adhere to this policy in their day-to-day activities.

4.19.5. The IG Office/Section (or the function assigned with IG responsibilities) is responsible to conduct awareness about the policy to Users.

4.19.6. Information asset owner (or job title assigned with responsibilities of Entity's higher management) is responsible for compliance to this policy within the Entity.

4.19.7. Data Stewards (or job title assigned with responsibilities of Entity's higher management) must endorse this policy for its effective implementation.

4.19.8. All Employees, contractors, and users with access to the Entity's data (electronic, paper and other records) are responsible to ensure the safety and security of the data is protected; and must respect and abide by the relevant obligations and protections, as per this policy.

4.19.9. All Employees who handle Confidential, Sensitive, or Secret data assets:

a. Must sign an Employee Confidentiality Agreement / Non-disclosure Agreement.

b. Must understand the impact of these legal frameworks, and how it relates to their role.

c. Should be supported by training as appropriate.

4.19.10. Table below presents brief of HIA responsibilities within the Entity:

Position	***Responsibility***	***Example***
Information asset owner	Senior Level Management in the Entity with organizational and **policy responsibility** for a broad segment of Entity data.	Chief Executive Officer
Data Stewards	- Official with direct **operational responsibility** for a broad segment of Entity data. - Responsible for assessing the impact Levels, specifying data Classification guidelines, and assign a corresponding Data Classification to Data Types or Data Sets. - Ensuring the protection and establishing appropriate use of the HIA. - Develops general procedures and guidelines for the management, security and access to data, as appropriate. - Authorize access to data for which they are responsible and use reasonable means to inform those receiving or accessing the data of their obligations in so doing. - Reviews, amends, and prepares proposed enhancements to either the Data Classification Guide for review and endorsement. - Annually reviews the Data Classification Guide with appropriate authoritative bodies.	Director of Entity / Chief Information Governance Officer
Data Custodians	- Ensure that systems handling Restricted / Internal data provide security and privacy protections according to the Data Classification, the Data Steward's policies, obligations, and authorizations, and as may be identified in the Data Classification Guide. - Use reasonable means to inform those accessing data sets in their control of their obligations in so doing. - Housing, keeping the data, and managing the resources,	Various Information Technology (IT) Staff: - Application/ Database / System & Server administrator - Banner Specialists - Operations Staff - Data Management

	which enable its collection, management and controlled access. - Has custodial responsibilities for managing the data for the day-to-day, operational-level functions. - Maintains the Data Classification Guide and the framework defined by this policy.	Specialists
Data User	Any individual or unit in possession of Entity data. Employees observe the constraints and directions of Data Stewards and Data Custodians and follow the Data Classification Guide in their handling of confidential information.	- Most Entity staffs as appropriate. - Contractors. - Consultants. - Suppliers/Vendors. Partners - Customers.
Certifying Authority	Official authorized to certify the appropriateness and accuracy of Entity data and to release data for publication or other purpose that furthers the Entity's mission.	Health Informatics & Smart Health Department, HRS, DHA

4.20. Implementation

4.20.1. Implementation of the HIA classification, handling, sharing, storage, and disposal framework described above encompasses all forms of HIA including electronic medical records (EMR), electronic platforms, as well as non-electronic information, such as paper files, and hard-copy data.

4.21. Monitoring and Compliance

4.21.1. Entities are responsible for complying with this Policy.

4.21.2. The Entity should create a compliance monitoring plan which can be used to continually assess the Entity`s overall compliance with this policy.

4.21.3. Key controls should be applied in accordance with the sensitivity of the information. Controls must be physical, procedural and technical.

4.21.4. The IG Office/Section (or the function assigned with IG responsibilities) must check the compliance of this policy on a periodic basis.

4.21.5. Any exceptions to this policy with valid business justification require approval from DHA_HISHD as a certified authority as per ICT law.

4.21.6. Entities are expected to provide a Declaration of Maturity provided by a competent third party regarding information classification and handling, to be included in their Annual Report. This should be supported or coordinated by the IG Manager (or job titles assigned with responsibilities of managing Entity's business divisions and sections).

4.21.7. If some of the IG technical roles are not available in the Entity, then it should be outsourced to competent consultancy company.

4.21.8. If users are unsure or not clear of any point in this policy, they should seek clarification or advice from DHA_HISHD (HISH@dha.gov.ae).

4.22. Enforcement

4.22.1. Any compromise of HIA must be reported to the IG office/section of Entity.

4.22.2. Accidental or deliberate compromise of HIA by employees/contractors/users must lead to disciplinary action and in some cases must constitute a criminal offence.

4.22.3. An Employee found to have violated/breached this Policy must be subject to Entity`s Human Resource disciplinary procedure in accordance with relevant HR Law, the Code of Conduct for Employees, and any other applicable UAE Laws in this regard. In certain circumstances termination of employment or engagement, as applicable, and/or legal action must be taken.

4.22.4. The Entity has the responsibility on failure of a supplier or contractor to comply with this Policy. If any violations happened, the Entity must take the necessary legal action. The DHA_HISHD must be informed instantly (HISH@dha.gov.ae).

4.22.5. Breaches of the HIA Classification Policies / related laws must be reported immediately to DHA_HISHD (HISH@dha.gov.ae) through IG office/section of the Entity.

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.mohap.gov.ae/FlipBooks/PublicHealthPolicies/PHP-LAW-AR-77/mobile/index.html

5.2. Federal Decree-Law No. 45 of 2021 regarding Personal Data Protection. Available on: https://u.ae/ar-ae/about-the-uae/digital-uae/data/data-and-privacy-protection-in-the-uae

5.3. 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.smartdubai.ae/docs/default-source/dubai-data/dubai-data-policies-en.pdf?sfvrsn=b2019ec4_6#:~:text=Article%20(1),Emirate%20of%20Dubai%2C%20is%20approved.

5.4. Law No. (26) Of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai. Available on: https://www.smartdubai.ae/docs/default-source/dubai-data/data-dissemination-and-exchange-in-the-emirate-of-dubai-law_2015.pdf?sfvrsn=46ac2296_6.

5.5. 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.mohap.gov.ae/FlipBooks/PublicHealthPolicies/PHP-

LAW-AR-95/mobile/index.html

5.6. 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

5.7. 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

5.8. 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.mohap.gov.ae/FlipBooks/PublicHealthPolicies/PHP-LAW-AR-91/mobile/index.html.

5.9. Federal Decree Law No. (4) Of Year 2016 on Medical Liability. Available at: https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/(E)%20Federal%20Decree%20no.%204%20of%202016.pdf

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

5.11. 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.wam.ae/en/details/1395302953555

5.12. Dubai Health Authority (2016). DHA Health Strategy 2016-2021 - Towards a Healthier and Happier Community. Available on : https://www.dha.gov.ae/Documents/Dubai_Health_Strategy_2016-2021_En.pdf

5.13. Dubai Health Authority Nabidh policies and standards. Available on: https://nabidh.ae/#/comm/policies

5.14. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the Emirate of Dubai. Available on: https://services.dha.gov.ae/sheryan/wps/portal/home/circular-details?circularRefNo=CIR-2021-0000141&isPublicCircular=true&fromHome=true

5.15. Dubai Health Authority Policy for Policy for Healthcare Data Quality in the Emirate of Dubai. Available on: https://services.dha.gov.ae/sheryan/wps/portal/home/circular-details?circularRefNo=CIR-2021-00000037&isPublicCircular=1&fromHome=true

5.16. 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

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

5.18. UAE National Electronic Security Authority (NESA). Available on:

https://logrhythm.com/solutions/compliance/uae-national-electronic-security-authority/

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

5.20. The General Data Protection Regulation (GDPR) (from Must 2018). Available on: https://gdpr-info.eu/art-84-gdpr/

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

5.22. Health Insurance Portability and Accountability Act (HIPAA). Available on: https://www.clinfowiki.org/wiki/index.php/Health_Insurance_Portability_and_Accountability_Act_(HIPAA)#The_Privacy_Rule