Document Type: Health Information Policy	**Code:** DHA/HRS/HISHD/PP-11	**Version Number:** 1
Document Title: Policy for Data and Health Information Protection and Confidentiality	**Issue Date:** 10/08/2022 **Effective Date:** 10/10/2022 **Revision date :** 10/08/2025	
Ownership: Health Regulation Sector		
Applicability: All Healthcare Entities under the Jurisdiction of Dubai Health Authority		

1. Definitions/Abbreviations:

A Fair Processing Notice: A notice given to individuals when the Entity gathers their PHI. The notice explains how their data will be used, how they can exercise their legal rights over their data and provides a link to the full privacy policy.

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

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 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 Protected 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 Protection Officer: Any natural or legal person appointed by the Entity (as controller) or processor, who undertakes the tasks of ascertaining the extent to which the Entity complies with the controls, requirements, procedures and rules for processing data and health information stipulated in accordance with UAE Federal Law No. 45 of 2021 regarding the protection of personal data and ensuring the integrity of Entity`s systems and procedures in order to achieve compliance by its provisions>

Data Subject: A person who is the subject of PHI.

Disclosure: The release of personally identifiable data to a third party.

Destroy: Refers to the confidential and secure destruction of the Health Information Assets (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.

Disposal: Refers to the secure destruction of an HIA OR the transfer of HIA for permanent preservation. A certificate of transfer will be provided as proof of transfer (and can act as evidence of disposal). Refer to section five of the Code for further information about

permanent preservation.

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

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 Center, telemedicine provider, laboratory and diagnostic center, and pharmacy, etc.

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

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.

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

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

Protected health information: also referred to as personal health information; include any of the 18 types of identifiers specified below:

- Name (Full name as per passport or Emirates ID)
- 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
- Driving 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: Means any operation which is performed on data such as:

- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Collection, recording, organization, structuring or storage (e.g. within a filing system).

- Adaption or alteration.
- Retrieval, consultation or use.
- Restriction, destruction or erasure.

Processor: a natural or legal person, public authority, agency or other body which Processes PHI on behalf of the Controller; as per Controller`s guidance and according to its instructions.

Pseudonymised Information: The processing of PHI in such a manner that it can no longer be attributed to a specific Data Subject without the use of additional information. The additional information is kept separately and is subject to technical and organizational measures to ensure that the PHI are not attributed to an identified or identifiable natural person.

Public Interest: Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader social interest.

Secondary use: is for purposes other than treating the individual subject of care, such as for Research, Public Health, Clinical Audit and Quality Improvement, Safety Initiatives, Facility Accreditation Purposes, Assessing, Exercising, Establishing, Prosecuting or Defending a Legal Claim or Complaint, and marketing. Some secondary uses directly complement the needs of primary use. Examples include medical billing, Entity`s 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.

DHA	:	Dubai Health Authority
DPO	:	Data Protection Officer
DPIA	:	Data Protection Impact Assessment
HIA	:	Health Information Assets
HIPAA	:	The Health Insurance Portability and Accountability Act
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
SAR	:	Subject Access Request
UAE	:	The United Arab Emirates

2. Purpose

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

2.2. To assure Entities under jurisdiction of DHA are providing a secure environment for data management; specifically identifiable health information - also termed "Protected Health Information" (PHI).

2.3. To outline the requirements and responsibilities of Entities working under jurisdiction of DHA on Data and Health Information Protection and Confidentiality.

2.4. To ensure the confidentiality of health information and protect the privacy of community members by providing proper governance for optimal data management and protection.

2.5. To define the rights and duties of all concerned parties dealing with data and health information.

3. Scope

3.1. All Entities working under jurisdiction of DHA.

3.2. All Data and health information within the Emirate of Dubai handled by Entities under jurisdiction of DHA.

3.3. Data and health information 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:

3.2.1. Medical and non-Medical information (e.g. Human resource, complaints records, corporate records - administrative records relating to all functions of the Entity etc.).

3.2.2. Identifiable and non-identifiable data.

3.2.3. Data accessed for primary or secondary use.

3.2.4. Physical or digital forms of data.

3.2.5. Structured record systems (Paper and electronic)

3.2.6. Transmission of information (Fax, email, post and telephone)

3.4. All information systems purchased, developed, managed or utilised by the Entity.

3.5. All users accessing and using health information in healthcare sector in the Emirate of Dubai; including all employees, contractors, consultants, suppliers, vendors, partners, customers and wider stakeholders where appropriate; accessing information 'owned entirely or partially' by the Entity.

4. Policy Statement:

4.1. The Data and Health Information Protection and Confidentiality Policy is an integral part of the DHA's approach to health Information Governance (IG) in the Emirate of Dubai. This policy must be read in conjunction with other related Health Regulation Sector (HRS)_Health Information and Smart Health Department

(HISHD)_IG and relevant policies and standards published by HRS.

4.2. Both UAE Federal Law No. (2) of 2019 concerning the Use of the Information and Communication Technology in the Area of Health and Executive Decision (51) of 2021 ("ICT Health Law"), and UAE Federal Data Protection law No. (45) of year 2021 ("UAE Data Protection Law"); have impact on Health Information. Hence, in this policy we are elaborating on the intersection between all related UAE laws, Emirate of Dubai legislations, and DHA regulations on health information mentioned below:

4.2.1. UAE Data Protection Law: https://www.dha.gov.ae/en/licensing-regulations-laws

4.2.2. UAE ICT Health Law: https://www.dha.gov.ae/uploads/112021/8af22f1c-ebe4-4e20-b157-743ac93bb20b.pdf

4.2.3. Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the UAE https://www.dha.gov.ae/en/licensing-regulations-laws

4.2.4. DHA "Health Information Assets Classification Policy": https://nabidh.ae/#/comm/policies.

Nevertheless, the regulation that is more specialized/detailed in health will supersede.

4.3. Dubai Health Authority Mandates Key Principles on Processing Protected Health Information

As per UAE ICT Health Law and UAE Data Protection law, DHA has key principles on how the Entities must process Protected Health Information (PHI) within the Emirate of Dubai. These principles apply to the use of PHI within Entities and when shared with other Entities or individuals. Compliance against these principles is a key and failure to comply may lead to regulatory action:

4.3.1. *Fairness, Lawfulness, and Transparency*:

a. Processing of PHI must be lawful, fair and in a transparent manner.

4.3.2. *Purpose limitation*:

a. Protected health Information must be collected for specified, clear, and legitimate primary use purposes and not further processed in a manner that is incompatible with those purposes.

b. Any PHI given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the Data Subject.

c. If the Entity is using the PHI for purposes other than primary use, then it must follow the articles in UAE ICT Health Law:

i. The Entity must justify the purpose(s) for using PHI for secondary use.

ii. The purpose of the secondary use of PHI must be recorded by the Entity.

iii. Secondary use (e.g. Research, Public Health, Clinical Audit and Quality Improvement, Safety Initiatives, Facility Accreditation Purposes, Prosecuting or Defending a Legal Claim or Complaint, and marketing). of PHI should require further permission/approval from DHA (HISH@dha.gov.ae).

4.3.3. *Data minimization*:

a. Protected health Information must be adequate, relevant and not excessive, and limited to what is necessary in relation to the purposes for which they are processed.

b. Protected health Information must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the health information is processed.

4.3.4. *Accuracy*:

a. Entity must take reasonable steps to ensure PHI is accurate, complete, and up to date.

b. Every sensible step must be taken to ensure that inaccurate PHI are rectified immediately.

4.3.5. *Integrity, Confidentiality, and Security:*

The Entity must guarantee the integrity and confidentiality of PHI at all circumstances.

4.3.6. *Protected health information retention:*

a. As mandated by UAE federal laws, Emirate of Dubai legislations, and DHA regulations/policies; PHI processed for any purposes shall not be kept for longer than is necessary.

b. When the grounds for retention no longer apply, the Entity must securely and permanently dispose PHI.

c. The timeline of health information retention is specified in UAE ICT Health Law and DHA policies and regulations.

4.4. Protected Health Information Confidentially

4.4.1. The confidentiality of PHI must be protected at all circumstances as per Legal obligation derived from UAE laws, Emirate of Dubai legislations, and DHA policies and regulations.

4.4.2. While managing/processing PHI, the Entity must ensure maintaining appropriate technical/organisational measures to protect integrity and confidentiality of the data and health information, including safeguard against:

a. Unauthorised access.

b. Unlawful processing.

c. Accidental information loss/destruction/damage.

4.4.3. All contracts of employment must include an information governance/data and health information protection and confidentiality clause. Contracts with third parties/agencies and temporary staffs are subject to the same rule.

4.4.4. The Entity should have a "Confidentiality Agreement" that non-Entity staff must sign before undertaking any work in or on behalf of the Entity.

4.4.5. It is essential that the Entity provide a confidential service to Data Subjects. Breaches of that confidentiality must lead to regulatory investigation and should result in disciplinary measures to those who have been negligent in causing the breach.

4.5. Data and health information Protection by Design and by Default

4.5.1. Data and health information protection must be considered at the start of any new project, service, contract, or process.

4.5.2. The Entity must integrate data and health information protection into every aspect of PHI processing activity. This includes implementation of the data and health information protection principles and safeguarding individual rights, such as data minimization, pseudonymisation and purpose limitation as set in this

policy.

4.6. Data Subject Rights on Protected Health Information

As per UAE Federal Data Protection law No. (45) of year 2021; there are rights for Data Subjects in respect of their PHI being processed that must be respected by all Entities:

4.6.1. The right to Consent before processing Data Subject PHI.

a. Without prejudice to any applicable legislation; anyone who exchanges and circulates Data Subject information must ensure its confidentiality and not use it for non-health purposes, and without the written consent of the Data Subject.

4.6.2. The right to receive information on type of PHI being processed:

a. The purpose of processing.

b. The source and recipient Entities (within UAE and abroad) that will process Data Subject`s PHI.

4.6.3. The right to restrict/discontinue PHI processing by the Controller in situations being defined on articles (16, 17 & 18) of UAE Data Protection Law of year 2021.

4.6.4. The right to be informed of security measures being considered while

transferring the PHI between Entities (within UAE and abroad).

4.6.5. The right to be informed on the process and timeline of storing/archiving the PHI.

4.6.6. The right to be informed whether any automated decision-making, including profiling has/will been undertaken on their PHI.

4.6.7. The right for selective disclosure of PHI to Entities as deemed necessary. Exercising this right shall not impede the Data Subject's existing rights to availing health care services.

4.6.8. The right to request the transfer of their PHI whenever it is possible from technical aspects.

4.6.9. The right to request correcting any inaccuracies in their PHI, and have incomplete PHI fully completed. These requests must be assessed and responded by the Entity within 5 working days.

4.6.10. The right to be informed on Entity`s breach process; and how the Data Subject will be informed about PHI breach.

4.6.11. Without prejudice to the applicable laws and legislations, and necessities of the public interest, the Data Subject has the right to request "opt-out" from the data and health information processing in conditions being defined on article (15) of UAE Data Protection Law of year 2021.

4.6.12. The right to access their PHI via "Subject Access Request" (SAR) and to review and obtain a copy of their PHI / records such as provider's medical and billing records or a health plan's enrolment, payment, claims adjudication, and medical management records maintained by the concerned Entity. The Entity must:

a. Document the verbal or written SARs with the signature of the Data Subject.

b. Respond to the SAR within one month (e.g. calendar 30 days) of its receipt.

c. Ensure to update the Electronic Medical Record systems when accommodating these requests as and when needed.

d. Retain communications and documentations associated with these requests for a period mandated by UAE ICT Health Law of year 2019 and DHA policies.

4.6.13. The right to lodge a complaint to the supervisory authority (e.g. DHA).

4.7. Information Technology (IT) systems

4.7.1. It is essential that IT systems within the Entity have adequate controls in place to prevent loss, unlawful processing, or inappropriate access.

4.7.2. The Entity`s Information Security Policy must provide detailed guidance on the security of Health IT systems including minimum standards of access controls.

4.8. Access to Protected Health Information / Data Usage

4.8.1. Entities must develop and implement policies and procedures that restrict access and usages of PHI based on the specific roles of their staff, trainees, vendors and third party contractors.

4.8.2. The policies and procedures must identify:

a. The persons, or classes of persons, within the Entity who need access to PHI to carry out their duties

b. The categories of PHI to which access is needed.

c. Any conditions under which they requisite the PHI to do their jobs.

4.8.3. Users must only access PHI for those Data Subjects that they have authorisation to access for specific purposes.

4.8.4. Any access to records, which is not legitimate / authorised, is prohibited and unlawful.

4.8.5. Staff have no right to access PHI held in records about their relatives/friends/ or co-workers; where they do not form part of the care team.

4.8.6. Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access.

4.8.7. Existing system users should not allow others to access systems using their

login credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach.

4.8.8. The Entity must carry out audits of access to PHI; and any member of staff who is found to be in breach of this guidance by inappropriately accessing PHI must face disciplinary action.

4.8.9. The unauthorised access to the Entity's computer systems including hacking and the subsequent use of that PHI is considered a criminal action.

4.9. Business Continuity /Disaster Recovery Plans

4.9.1. The Entity must ensure that it has both business continuity and disaster recovery plans in place for all its information assets.

4.9.2. The Entity should ensure that these plans are tested regularly in order to maintain the integrity and availability of the information held.

4.10. Processing Protected Health Information within the Entity

4.10.1. Processing of PHI within the Entity must be lawful and safe and as per related UAE federal laws, Emirate of Dubai legislations, and DHA regulations.

4.10.2. Data and health information processing for the purposes of Data Subject care must be within the framework of confidentiality and privacy.

4.10.3. The Entity must inform Data Subjects and service users about how their PHI is used and to whom it may be disclosed.

4.10.4. Secondary use (e.g. Research, Public Health, Clinical Audit and Quality Improvement, Safety Initiatives, Facility Accreditation Purposes, Prosecuting or Defending a Legal Claim or Complaint, and marketing) of identifiable data and health information needs consent from Subject Data.

4.10.5. Where processing is to be carried out on behalf of the Entity (as the controller), the Entity should use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this policy and ensure the protection of the PHI.

4.10.6. The processor shall not engage another processor without getting prior clear specific or general written authorisation from the Entity (as the Health Information Controller), clarifying the obligations and responsibilities.

4.10.7. In the case of general written authorisation, the processor should inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Entity (as the health information Controller) the opportunity to object to such changes.

4.11. Processing Protected Health Information through Nabidh Health Information Exchange (HIE)

4.11.1. Entity must get consent from Data Subject for accessing his/her PHI through Nabidh HIE:

a. The consent needs to be clear, simple, unambiguous and easy to understand.

b. The consent can be in paper or electronic form.

c. The consent should contain part for "opt-out"; and the "opt-out" process should be easy.

d. The consent is valid for lifelong, unless the Data Subject opts out from HIE.

4.11.2. The Data Subject should have the liberty of "opting-out" of the Nabidh HIE at any time; however, this will not affect the data and health information processed beforehand.

4.12. Obligations of Protected Health Information Processor

4.12.1. The PHI Processor must abide by all UAE laws and DHA regulations on data and health information protection and confidentiality.

4.12.2. The Processor must make sure all IT security and regulatory precautionary measures are considered while dealing with PHI.

4.12.3. The Processor must use the PHI solely for the purpose it is meant to, and for the duration, it is required. In case the timeline for PHI processing is crossed, the Processor must inform the Entity (as the health information Controller) for

further extending the timeline.

4.12.4. All PHI must be demolished or handed over to the Entity after the deadline of data and health information processing contract.

4.12.5. The Processor must not disclose the PHI or the outcome of PHI processing to any party; except in legally authorized conditions.

4.12.6. The Processor must maintain a record of processing activities under its responsibility as per article (8) of UAE Data Protection Law No. (45) for year 2021.

4.13. Processing Protected Health Information without Data Subject Consent

As per UAE ICT Health law, anyone dealing with PHI must ensure its confidentiality. If PHI is utilised for secondary use purposes, then written consent of the Data Subject is required. However, the Entity is legitimate to process the PHI without Data Subject consent, as per article (16) of UAE ICT Health law and article (4) of UAE Data Protection Law, in following settings:

4.13.1. Protected health information is required by the health insurance companies or other health service providers for purposes of auditing, approving or verifying the financial benefits related to services.

4.13.2. For the purposes of scientific and clinical research, provided that the Data Subject's identity is not disclosed and that the ethics and rules of scientific

research are followed.

4.13.3. For protecting public health, such as protecting against communicable diseases / epidemics and serious cross-border threats to health; or to maintain the health and safety of the Data Subjects or any other persons in contact with them.

4.13.4. At the request of the competent judicial authorities.

4.13.5. At the request of DHA for the purposes of inspection, supervision and protection of public health.

4.13.6. For the Processing of PHI that are manifestly made public by the Data Subject.

4.13.7. Processing is necessary for the investigation, establishment, exercise or defence of legal claims or potential legal claims including complaints to the Regulator against the Entity or its employees; or whenever courts are acting in their judicial capacity.

4.13.8. For compliance with a legal obligation to which the Entity is subject.

4.13.9. For the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

4.13.10. To ensure high standards of quality and safety of health care and of medicinal products or medical devices based on UAE laws and DHA regulations.

4.13.11. For the purposes of carrying out the obligations and exercising specific rights of the Entity (as Controller) or of the Data Subject in the field of employment, social security and social protection law.

4.13.12. For pursuant to a contract the Data Subject is part of it; or to take actions based on Data Subject request for pursuant/ modification/ or termination of a contract.

4.14. Sharing Protected Health Information Sharing with Third Parties within UAE

4.14.1. If the Entity instructs a third party, within the UAE, to process PHI on their behalf, Data Sharing Agreements/Contract must be signed.

4.14.2. Data and health information Sharing Agreement/Contract must include appropriate clauses setting out responsibilities for data and health information protection and confidentiality, consistent with UAE Data Protection Law, ICT Health Law, and DHA policies requirements. If no such clause exists within the data and health information sharing agreement/contract, the supplier must complete and sign a separate Confidentiality Agreement.

4.14.3. The Entity must ensure the Processor provides “sufficient guarantees” that they have the appropriate technical and organisational security measures in place to protect PHI confidentiality.

4.14.4. The third party (e.g. data and health information processor) must abide with

the data and health information protection and confidentiality terms even after the contract expires.

4.14.5. The Entity must guarantee that PHI received from or exchanged with third parties are protected in accordance with relevant UAE and DHA legislative and regulatory requirements, including this policy. Detailed guidance can be found in:

a. DHA "Health Information Assets Classification policy" (https://nabidh.ae/#/comm/policies).

b. DHA digital platform licencing requirements (Online Licencing (Sheryan) – DHA).

c. DHA Telehealth standards (https://www.dha.gov.ae/Documents/HRD/RegulationsandStandards/standards/Standards%20for%20Telehealth%20Services%20Final.pdf)

4.14.6. Any PHI transferred by the Entity outside the facility, but within the UAE, for processing, must be securely encrypted during transit.

4.14.7. Where PHI data and health information/records need to be transported in any media, this process must be carried out to maintain strict security and confidentiality of this information. All portable electronic media must be encrypted.

4.14.8. When the PHI is transferred electronically, it should be abiding access control measures on privacy, security and confidentiality (e.g. password-protected portals, encrypted Secure Sockets Layer (SSL), HIPAA compliant document transfer).

4.14.9. Protected Health Information should 'not be kept for longer than necessary' for which it is required for processing by third party.

4.15. Transfer of Protected Health Information to Outside of the UAE

4.15.1. Protected health information should not be transferred to a country or territory outside the UAE; except for transfer of PHI within the category of UAE ICT Health Law exemptions:

a. Cabinet Decision No. (51) of year 2021 on exemption for storage and transfer of health records and information must be abide to: https://www.dha.gov.ae/uploads/112021/fd2757c0-7f87-4f1d-b6c3-4c8eb9045393.pdf

b. DHA approval must be granted as per DHA Health Information Assets Classification Policy: https://nabidh.ae/#/comm/policies.

c. The approval can be granted by sending request to : HISH@dha.gov.ae

4.15.2. Any transfer or sharing of PHI to outside of UAE must be carried out securely and safely to prevent the risk of accidental disclosure or loss in transit.

4.15.3. Protected Health Information must be securely encrypted during transit; and the security measures mentioned on this policy must be abide to.

4.16. Disposal of Health Information Assets containing Protected Health Information

4.16.1. The UAE ICT Health Law and DHA policies provide detailed guidance on the minimum retention periods applicable to HIA and disposal procedures.

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

4.16.3. The disposal of electronic equipment that may hold PHI (PCs, laptops, and any other devices with information storage capabilities) should be carried in a way ensuring all data and health information is effectively removed before destruction.

4.17. Breach of Data and health information Protection and Confidentiality

4.17.1. A breach of security leads to the accidental or unlawful destruction, loss, alteration, use, copying, deface, block, erase, conceal, unauthorized disclosure, or access to PHI transmitted, stored or otherwise processed. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) are:

a. Unlawful disclosure of PHI.

b. Inappropriate access to PHI, where there is no defined clinical reason.

c. Inappropriate use/misuse of PHI.

d. Loss of availability of PHI.

e. Unauthorized disclosure or copying of PHI.

f. Access to PHI by an unauthorized third party.

g. Deliberate or accidental action (or inaction) by a Controller or Processor.

h. Sending PHI to an incorrect recipient.

i. Computing devices containing PHI being lost or stolen.

j. Alteration of PHI without permission.

k. Re-identification of de-identified PHI without the consent of the Data Subject.

4.17.2. Breaches of confidentiality or unauthorised disclosure of any information constitutes a serious disciplinary offence and gross misconduct.

4.17.3. Any breach or suspected breach of data and health information protection and confidentiality can have severe implications for the health sector, Data Subjects, and employees. Hence, both the Entity (as the health information Controller) and the data and health information Processor must abide to all UAE laws and DHA legislations in this regards.

4.18. Reporting Breach of Data and health information Protection and Confidentiality

4.18.1. Entities must establish breach/incidence response management (Incident Response and Business Continuity) and recovery (Incident Recovery and Disaster Recovery) plans that comprise of:

a. Identification of the breach.

b. Root cause of the Breach.

c. Incident patterns (whether its repetitive or new)

d. Services affected.

e. Procedures for containing /eradicating/eliminating the incident.

f. Recovery and repair of PHI.

g. Corrective / Preventive action taken.

h. Documenting the lessons learnt.

4.18.2. Entities must thoroughly investigate the breaches/incidents starting from the point of discovery until closure:

a. Determine if the breach is related to a violation of PHI.

b. Determine if further investigation is warranted, and if not, then document the incident and retain.

c. List and perform mitigation, remediation and sanctions.

4.18.3. The breach investigation and documentation must:

a. Be systematic/organized and the records maintained as per regulations.

b. Use appropriate investigative procedures and preserve the chain of custody.

c. Involve resources trained in incident handling when needed.

d. Educate and document why and how to prevent recurrence of the incident.

4.18.4. The Entity is required to report breaches/incidents within the designated period defined by Executive Regulations of UAE Data Protection Law.

4.18.5. Breach notifications must be reported to both the UAE Information Office and DHA (HISH@dha.gov.ae).

4.18.6. The report should include the following:

a. Nature and type of breach.

b. Date of breach.

c. How the breach was discovered.

d. Reasons of breach.

e. Categories and approximate number of Data Subject concerned.

f. Extent/severity of the breach and likely consequences of it.

g. Formal measures being taken by the Entity and/or Data and health information Processor for reporting, investigating and recording breaches.

h. Correcting procedures being taken by the Entity and/or data and health information Processor.

i. Information on data and health information protection officer (DPO) within the Entity.

4.18.7. If the data and health information Processor identified any breach on PHI; then the Entity (as data and health information Controller) must be informed immediately.

4.18.8. Entity`s employee who wish to report incidents relating to data and health information protection and confidentiality should follow the incident reporting procedures contained in the Entity`s Incident Management Policy.

4.18.9. Staff found in breach of this policy should be subject to disciplinary action up to termination.

4.18.10. Where the PHI breach is likely to result in a high risk to the privacy and confidentiality of the Data Subject, the Entity must communicate the breach to the Data Subject within the designated period defined by Executive Regulation of UAE Data Protection Law.

4.18.11. The breach notification to Data Subject should describe in clear and plain language:

a. The nature of the PHI breach.

b. Likely consequences of the PHI breach.

c. How the breach affected Data Subject privacy and PHI confidentiality.

d. Name and contact details of the Entity`s Data and health information Protection Officer.

e. Measures taken / or proposed to be taken to address the breach.

4.18.12. The Data and health information Protection Officer in the Entity is the single point of contact for all breaches.

4.18.13. Advice and guidance must be sought as soon as possible by contacting DHA HISH@dha.gov.ae.

4.19. Data and health information Protection Officer Appointment

4.19.1. The UAE Data Protection Law requires all Entities and data Processors to nominate / appoint Data Protection Officer (DPO), who has the requisite professional qualities and expert knowledge of data and health information protection compliance; based on below circumstances:

a. If processing of the data and health information may cause high risk on PHI

confidentiality due to using new techniques or high data and health information volume.

b. If data and health information processing includes systematic evaluation of PHI for automated profiling and processing.

c. If data and health information processing is on large volume of PHI.

4.19.2. The DPO can be an employee within the Entity (as the health information Controller) or/and the data and health information Processor; or an external appointed party.

4.19.3. The Entity (as the health information Controller) or/and the data and health information Processor must inform the UAE Information Office and DHA the contact details of the appointed DPO.

4.20. Roles and Responsibilities of Data and health information Protection Officer

4.20.1. This role is a senior role ensuring the Entity (as the health information Controller) and data and health information Processor are abiding to UAE Data protection law, Emirate of Dubai legislations, and DHA regulations.

4.20.2. The DPO is responsible for:

a. Overseeing implementation of data and health information protection and security measures to ensure compliance with the all UAE Data protection law, and in accordance with this Policy.

b. Ensure the legitimacy and accuracy of data and health information protection process followed by the Entity and data and health information Processor.

c. Receiving and handling all complains on data and health information protection and confidentiality.

d. Providing technical advice regarding data and health information protection assessments, periodic PHI inspection procedures, and anti-breach systems used by the Entity and/or data and health information Processor.

e. Documenting all data and health information protection assessments and risk management procedures.

f. Having reporting channels directly to the Board of Directors and Chief Executive.

g. Advising colleagues, employees, contractors, consultants, suppliers, vendors, and partners on data and health information protection compliance.

h. Conducting awareness on the UAE laws and DHA regulations, including the development of policies, procedures and guidance to Entity`s employees, contractors, consultants, suppliers, vendors, and partners.

i. Being main contact point with the UAE Information Office and DHA.

4.20.3. The DPO must in all circumstances maintain the confidentiality of PHI.

4.21. All Health Entities must

4.21.1. Develop a data and health information protection and confidentiality policy and procedures to ensure all PHI obtained, held, recorded, used, stored 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.

4.21.2. Have in place appropriate administrative, technical and physical safeguards to monitor, detect and protect the confidentiality of PHI; and to ensure data and health information within their facilities are protected in line with the requirements specified in this Policy.

4.21.3. Conduct Data Protection Impact Assessments (DPIAs) on yearly basis, and while initiating a new project that is 'likely to result in a high risk to PHI'. Guidance on conducting DPIA can be found on : https://gdpr.eu/data-protection-impact-assessment-template/

4.21.4. Perform compliance audit to evaluate the effectiveness of the implemented PHI protection measures; and identify/mitigate potential risks.

4.21.5. Apply appropriate sanctions against staff, trainees, vendors and third party contractors who violate the Entity`s data and health information protection policies and procedures.

4.21.6. Ensure access to PHI is confined to those with specified authority to view

and/or change the data and health information; by ensuring procedures are in place for allocating and controlling access, and passwords.

4.21.7. Ensure registering:

a. All applications and databases used to handle PHI in the Entity.

b. Purposes for holding the PHI within these applications.

c. How PHI is used and to whom it may be disclosed.

4.21.8. Adopt well-crafted "Information Security Policy" with the relevant provision(s) of UAE laws, this policy, and all DHA IG policies to protect health information assets.

4.21.9. Ensuring that relevant health information assets management policies and guidelines are adhered to by information users.

4.21.10. Providers of digital health platforms should ensure that they make the required provision of Fair Processing Notices to Data Subjects on whom it holds PHI:

a. These notices must inform Data Subject:

i. What PHI is held.

ii. Why PHI is held.

iii. How PHI is used.

iv. To whom PHI may be disclosed.

b. The notice shall be provided to Data Subject through the use of leaflets and/or the provider's website.

c. The notice must explain how the Data Subjects can exercise their legal rights over their data and health information, and must provide a link to the full data and health information protection policy.

4.21.11. Comply with all UAE, Emirate of Dubai, and DHA regulatory requirements governing E-Health, Telehealth, Electronic Health Information Exchange (HIE), Data and health information Protection, Data Quality, Data Privacy, Transparency, Cybersecurity, and Information security.

4.21.12. Comply with all UAE, Emirate of Dubai, and DHA legislation, Policies and regulations on data and health information protection and confidentiality.

4.21.13. Comply with The Dubai Electronic Security Center (DESC) and with the UAE Telecommunications and Digital Government Regulatory Authority (TDRA) rules and regulations.

4.21.14. Comply with security measures of:

a. The Executive Council of Dubai Government Resolution No. (13) Of 2012 for Information Security Regulation in Dubai Government.

b. Dubai Government "Information Security Regulation" (ISR).

c. "Dubai Electronic Security Centre".

d. " Digital Dubai Authority".

e. UAE National Electronic Security Authority (NESA).

f. Information Security Management System (ISMS), ISO 27001.

4.21.15. Comply with federal and local legislation, including but not limited to:

a. Federal Law No. (4) of 2016 on Medical Liability.

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

c. UAE federal, and Emirate of Dubai electronic security authority standards and guidelines for cyber security.

4.21.16. Comply with all DHA IG policies:

a. Nabidh policies and standards

b. Health Information Assets Classification Policy

c. Data and health information Quality policy

d. Data and health information Security Policy.

4.21.17. Establish appropriate measures to assess, determine compliance and effectiveness levels of Information Security Management System (ISMS).

4.21.18. Review Application changes and projects from information security perspective.

4.22. Roles and Responsibilities within the Entity

4.22.1. The Entity must implement appropriate information Protection Controls, based on DHA Policies and related UAE and Emirate of Dubai laws and legislatives to secure their information assets confidentiality.

4.22.2. Everyone within the Entity with access to PHI should be aware of his / her responsibilities.

4.22.3. Below Table is a brief of roles and responsibility within the Entity:

ROLES AND RESPONSIBILITIES	
Chief Executive	• The Chief Executive has ultimate responsibility for ensuring that the Entity has suitable arrangements in place for the management of Data and health information Protection and Confidentiality. • It is the role of the Chief Executive to ensure that the Entity's policies support the implementation, use and handling of PHI and that processing is done transparently, lawfully, accurately, securely and with a lawful basis. • The Chief Executive is also responsible for ensuring that sufficient resources are provided to support the requirements of the Policy and the role of Data and health information Protection Officer.

Data and health information Protection Officer (DPO)	The Data and health information Protection roles and responsibilities are mentioned in this policy.
Line Managers	Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of: • The Data and health information Protection and Confidentiality Policy as it relates to their work areas. • Their personal responsibilities for handling PHI. • Compliance with reporting requirements. • How and where to access advice on handling PHI. • Ensuring their staff have undertaken the Entity`s mandatory training. Line Managers will be individually responsible for maintaining data and health information protection compliance within their departments/areas of responsibility.
All Staff	All staff employed by the Entity are affected by the UAE Data Protection law: • They have rights as employees about whom Entity is holding data and health information. • They have obligations as healthcare professional who collect data and health information about Data Subjects. All staff must:

	• Understand their legal obligation to keep PHI confidential, to ensure they do not breach the data and health information protection principles and uphold Data Subject's rights. • Participate in induction, mandatory and awareness training sessions. • Be aware of the nominated Data and health information Protection leads in the Entity. • Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of the reason for requiring that information. • Report actual or suspected breaches of confidentiality to their line manager.

4.23. Training

4.23.1. The Entity must maintain appropriate training and awareness strategies to support compliance with this Policy.

4.23.2. Data and health information Security and Protection training is mandatory and must be provided to staff on induction and every 2 years to ensure they are aware of their confidentiality obligations in line with this policy.

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

out their functions.

4.23.4. The Entity should have a process to periodically review the competency of the staff and other resources including third party vendors.

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

4.24. Accountability

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

4.24.2. The Entity has a legal obligation to maintain confidentiality standards for all PHI.

4.24.3. Entities are required to undergo periodic internal and external audits and independent reviews to monitor compliance with the data and health information protection requirements as specified in this policy.

4.24.4. Entities must retain and provide the outcomes of the audit / compliance to DHA on yearly basis (hish@dha.gov.ae).

4.25. Non-Compliance

4.25.1. A failure to adhere to this policy is considered a violation that requires

investigation; and disciplinary action / dismissal will be taken in accordance with the provision of the current legislations.
In case of discrepancy, difference or inconsistency between the Arabic version and the English version, the Arabic version shall prevail.

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/uploads/112021/8af22f1c-ebe4-4e20-b157-743ac93bb20b.pdf

5.2. Cabinet Decision No. (32) of year 2020 on the Implementing Regulation of UAE Federal Law No. (2) of year 2019 on the Use of Information and Communication Technology in Health Fields. Available on: https://www.dha.gov.ae/uploads/112021/7dec6039-a735-4f01-b07e-3615d0a190b1.pdf

5.3. Cabinet Decision no. (51) of 2021 on exemption for storage and transfer of data and health information and information outside the country. Available on: https://www.dha.gov.ae/uploads/112021/fd2757c0-7f87-4f1d-b6c3-4c8eb9045393.pdf

5.4. Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data (United Arab Emirates). Available on: https://u.ae/ar-ae/about-the-uae/digital-uae/data/data-protection-laws#personal-data-protection-law

5.5. DHA Health Information Assets Classification Policy (https://nabidh.ae/#/comm/policies).

5.6. 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.

5.7. 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.

5.8. 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

5.9. Federal Law No. (5) of year 2012 on Combatting Cybercrimes and its amendment by Federal Law No. (12) of 2016. Available on: https://u.ae/ar-ae/resources/laws

5.10. 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 on: https://www.dha.gov.ae/uploads/112021/625c238e-d7ab-43c5-949f-832bdcd52821.pdf

5.11. Federal Decree Law No. (4) of year 2016 on Medical Liability. Available on: https://www.dha.gov.ae/Asset%20Library/MarketingAssets/20180611/(E)%20Feder

al%20Decree%20no.%204%20of%202016.pdf

5.12. Executive Council Resolution No. (32) of year 2012 on Regulating the Entity of health professions in the Emirate of Dubai. Available on: https://www.dha.gov.ae/en/HealthRegulation/Documents/TRANS_2012_823_Executive%20Council%20Res%20No%2032%20of%202012_Final-2-dr.layla.pdf

5.13. 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/uploads/112021/343dd9eb-4de0-46c4-88ca-1c3520349f84.pdf

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

5.15. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the Emirate of Dubai. Available on: https://nabidh.ae/#/comm/policies

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. DOH Standard-on-Patient-Healthcare-Data-Privacy. Available on :

https://www.doh.gov.ae/-/media/Feature/Aamen/DOH-Standard-on-Patient-Healthcare-Data-Privacy.ashx

5.22. 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

5.23. UK Iinformation Commissioner's Office website. Available on: www.ico.org.uk