



دائرة الصحة
DEPARTMENT OF HEALTH

DOH STANDARD ON PATIENT HEALTHCARE DATA PRIVACY

September 2020

PUBLIC

عام



 دائرة الصحة DEPARTMENT OF HEALTH	
Document Title:	DOH Standard on Patient Healthcare Data Privacy
Document type	Standard
Document Ref. Number:	DOH/SD/SS/PHDP/0.9
Effective Date:	16 th September 2020
Previous versions	None
Document Owner:	Support Services Division
Applies to:	<ul style="list-style-type: none"> • DOH-licensed healthcare professionals. • Healthcare providers. • Health insurers. • Third Party Administrators. • Data Storage entities. • Pharmaceutical facilities and pharmacists.
This Standard should be read in conjunction with related UAE laws, DOH Standards, Policies and Manuals including but not limited to: <ul style="list-style-type: none"> • Federal Law No.2, 2019 on the Use of Information and Communications Technology (ICT) in Healthcare. • DOH Resolution No. 36 of 2019 Disciplinary Regulations for the Health Sector of the Emirate of Abu Dhabi (General). • Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS). • DOH Regulator Manual. • DOH Healthcare Provider Manual. • DOH Health Professional Manual. • Law No. (23) Of 2005 Concerning Health Insurance in the Emirate of Abu Dhabi. • UAE Cybercrime Law No. 5 of 2012. 	



Table of Contents

Purpose.....	4
Scope and Applicability	4
Definitions	4
Prerequisite and Data Collection	6
Data Usage	9
Data Transfer and Data Security	10
Enforcement and Sanctions	11
APPENDIX A - Detailed Description of Requirements	12
APPENDIX B - References	18



1- Purpose

This Standard seeks to ensure that identifiable patient health information - also termed “Protected Health Information” (PHI) - is appropriately protected for the use and disclosure by organizations subject to Federal Law no. 2, 2019, by setting the minimum data protection requirements stakeholders must comply with including:

- 1.1. The circumstances in which the patients Protected Health Information (PHI) may be used or disclosed by the entity.
- 1.2. Secure and optimal use of patient health information.
- 1.3. Operational policies, standards and practices that are aligned with the requirements of all applicable laws and regulations.
- 1.4. Security and safety of health data and information to maintain its:
 - 1.4.1. Confidentiality: by not allowing the trade or exchange of the patient’s health data and information to other than authorized cases.
 - 1.4.2. Integrity: by maintaining the safety of the patient’s health data and information from vandalism, damage, modification, alteration or unauthorized deletion.
 - 1.4.3. Availability: to authorized individuals and to facilitate access to it when needed.
 - 1.4.4. Privacy: a patient’s right to control the access to his/her personal or healthcare data.

2- Scope and Applicability

2.1. The standard covers:

- 2.1.1. All categories of health care entities regulated by DOH in the Emirate of Abu Dhabi.
- 2.1.2. Healthcare professional(s), insurance providers, service providers, vendors, brokers and third-party administrators who have access to and are processing or storing personal sensitive health information pertaining to patients in all forms known as Protected Health Information.

2.2. Applicability of specific control mandates/requirements of the standard:

- 2.2.1. Is defined based on the maturity, operational complexity and operating environment of the entity.
- 2.2.2. Entities shall perform a privacy risk assessment to understand and implement the controls as appropriate, including for situations where the patient is receiving treatment via telemedicine, remote care and for medical tourism.

3- Definitions

No.	Term	Definition / Abbreviation
1	Central system	Is the digital platform for the exchange of electronic health information between health sector entities? In the Emirate of Abu Dhabi, this is represented by “Malaffi”, the Abu Dhabi Health Information Exchange Platform.
2	Controls	The administrative, technical, and physical safeguards applied within entity to satisfy privacy requirements.
3	Data	All that can be stored, processed, generated and transferred such as numbers, letters, symbols, images and the like (including digital and non-digital).
4	Entity / Entities	Entity in Abu Dhabi 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 (TPA’s), hospital, medical clinic and medical center,



		telemedicine provider, laboratory and diagnostic center, and pharmacy, etc.
5	Exchange of health information	Access, exchange, copying, photocopying, transfer, storage, publication, disclosure or transmission of health data and information.
6	Health authority	Any federal or local governmental body concerned with health affairs in the United Arab Emirates. (DOH – Department of Health).
7	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.
8	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.
9	Individually identifiable health information	<p>Is health information that is held or transmitted by an entity or its contractors / third parties in any form or media, whether electronic, paper, or verbal:</p> <ul style="list-style-type: none"> • Demographic data and general identifiers such as name, address, birth date, mobile number, Emirates ID etc. • Information that identifies the patient or for which there is a reasonable basis to believe that it can be used to identify the patient. • Protected Health Information including information on the Patient’s past, present or future physical or mental health condition and the provision of health care to the patient, or details of medical insurance. • Past, present, or future payment for the provision of health care to the patient. • Medical reports / records whether it is in electronic or paper format. • Information about any organ donation to/by patient, of any body part or any bodily substance of that patient, or derived from testing or examination of body part.
10	Least privilege	The principle of providing users and programs with only essential and needed privileges to complete a specific task, and provides adequate assurance that no excess privileges are granted for users/programs/roles to complete a specific task.
11	Marketing	Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.
12	Need to know	The principle of providing access to users and data only when there is an established need for access.
13	Personally Identifiable Information (PII)	Personally Identifiable Information - information that, when used alone or with other relevant data, can identify a patient. PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely
14	Person / Individual / Patient	A natural or arbitrary person whose protected health information is or has been captured by the entity.
15	Privacy Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (I) a person other than an authorized user accesses or potentially accesses data or (II) an authorized user accesses data for another than authorized purpose.
16	Privacy Risk	The likelihood that entities / patients will experience problems resulting from data processing, and their impact should they occur.
17	Privacy Risk Assessment	Sub-process of entity's risk management for identifying, evaluating, prioritizing, and responding to specific privacy risks.
18	Privacy Risk Management	Set of defined processes for identifying, assessing, and responding to privacy risks. Generally, part of Risk Management practices.



19	Privacy Policy Standard	Standards to protect patient's medical records and other protected health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.
20	Processing	Creating, entering, modifying, updating or deleting information (digital and non-digital).
21	Professional guidelines	A description of the methods, actions and procedures used as a guidance.
22	Programs	Set of actions developed with the aim of improving the health conditions of a patient
23	Protected health information (PHI)	Protected health information - "Relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient"
24	Site	The entity where the PHI is stored, handled and used
25	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.

4- Prerequisites and Data Collection

4.1. Required nondisclosures

- 4.1.1. Ownership of the patient health information is always with the patient.
- 4.1.2. All entities who are interacting with the patient health data lifecycle should take the patient's consent.
- 4.1.3. No entity may use the central system unless authorized to do so by the health authority or the concerned authority, as determined by the implementing regulations of the Federal Law no. 2, 2019.
- 4.1.4. No entity is permitted to store, develop, or transfer PHI outside the United Arab Emirates that is related to health services provided within Abu Dhabi, except in cases where an exception to do so is issued by the Department of Health in coordination with the Ministry of Health and Prevention.

4.2. Authorized uses

Without prejudice to any applicable legislation, anyone who exchanges and circulates patient information:

- 4.2.1. Must ensure its confidentiality.
- 4.2.2. Must not use it for non-health purposes.
- 4.2.3. Must not use it without the written consent of the patient, except in the following cases.
 - 4.2.3.1. Data or health information required by the health insurance companies or any provider of health services with respect to the health services received by the patient for purposes of auditing, approving or verifying the financial benefits related to those services.
 - 4.2.3.2. The purposes of scientific and clinical research, provided that the patient's identity is not disclosed and that the ethics and rules of scientific research are followed.
 - 4.2.3.3. The purpose of preventive and curative measures related to public health, or to maintain the health and safety of the patients or any other persons in contact with them.
 - 4.2.3.4. At the request of the judicial authorities.



- 4.2.3.5. At the written request of the patient (UAE national or non-national) not residing in the Emirate of Abu Dhabi and getting non-emergency medical services as a medical tourist in a healthcare facility licenced by Abu Dhabi Department of Health.
 - 4.2.3.6. At the request of the health authority for the purposes of inspection, supervision and protection of public health.
 - 4.2.3.7. Health information exchange between healthcare facilities on Abu Dhabi Health Information Exchange platform, Malaffi.
- 4.3. Data Privacy Policy and Other Patient Rights
- 4.3.1. Entities are required to have a privacy policy and procedures that describe the way they collect, use and disclose personal information for reasons such as:
 - 4.3.1.1. Provision of access to the site.
 - 4.3.1.2. Provision of health information regarding activities and healthcare services, referrals, or administrative services.
 - 4.3.1.3. Provision of services necessary to, or used in, the delivery of treatment and programs.
 - 4.3.1.4. Protection of the entity's rights or property or of customers or other third parties from fraudulent, abusive, or unlawful use of, or subscription to, campaigns and services.
 - 4.3.1.5. Enforcing and applying the terms and conditions agreed to by patient and entity.
 - 4.3.1.6. Compliance with the laws, regulations and orders and to cooperate with governmental investigations.
 - 4.3.2. The policy must:
 - 4.3.2.1. Describe the patients' right to complain to DOH and to the concerned entity if they believe their data privacy rights have been violated;
 - 4.3.2.2. Include a point of contact for further information and for making complaints to the concerned entity.
 - 4.3.3. The policy and procedures must:
 - 4.3.3.1. Be reasonably designed, taking into account the amount of PHI data, scope of operations, facility type, operating model (multiple sites), etc., and the type of activities related to protected health information and must comply with applicable laws and regulations.
 - 4.3.3.2. Include guidelines on:
 - 4.3.3.2.1. Data Collection.
 - 4.3.3.2.2. Data Processing.
 - 4.3.3.2.3. Data Security.
 - 4.3.3.2.4. Data Localization.
 - 4.3.3.2.5. Data Retention.
 - 4.3.4. Concerned entities must act in accordance with their policy.
 - 4.3.5. Entities must have in place appropriate administrative, technical and physical safeguards to monitor, detect and protect the privacy of protected health information.
 - 4.3.6. Entities shall have a periodic privacy compliance program and perform compliance audit to evaluate the effectiveness of the implemented privacy program.
 - 4.3.7. Entities must have and apply appropriate sanctions against staff, trainees, vendors and third party contractors who violate its privacy policies and procedures or the



privacy requirements.

- 4.3.8. The development and enforcement of information security policies and procedures, additional or as required by this standard, is the responsibility of the participating/ implementing entity.

4.4. Access to Patients' Data

- 4.4.1. Patients shall have the authority for selective disclosure of their health information to entities (e.g. hospitals, health care providers etc.) as deemed necessary. Exercising this right shall not impede the patient's existing rights to availing health care services.
- 4.4.2. Except in certain circumstances, patients have the right to review and obtain a copy of their protected health information / records such as provider's medical and billing records or a health plan's enrolment, payment, claims adjudication, and case or medical management records maintained from the concerned entity.
- 4.4.3. Entities may seek recommendations from regulators in cases of ambiguity.

5- Data Usage

- 5.1. Entities must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of their staff, trainees, vendors and third party contractors.
- 5.2. Entities shall adopt the principles of 'need to know' and 'least privilege'.
- 5.3. The policies and procedures must identify:
- 5.3.1. The persons, or classes of persons, within the entity who need access to protected health information to carry out their duties;
- 5.3.2. The categories of protected health information to which access is needed;
- 5.3.3. Any conditions under which they need the information to do their jobs;
- 5.4. These minimum necessary policies and procedures must also reasonably limit who within the entities has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business.
- 5.5. Training and management:
- 5.5.1. 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.
- 5.5.2. The trainings must be periodically performed within a reasonable time after employees are on boarded, and within a reasonable time of material changes in applicable policies and procedures.
- 5.5.3. Entities' training requirements shall also consider that different roles may need different training according to the roles and responsibilities.
- 5.5.4. Entities may also consider including topics such as:
- 5.5.4.1. Types of privacy breaches and notifications e.g. secured PHI, unsecured PHI, etc.
- 5.5.4.2. Where to locate policies and procedures related to privacy management.
- 5.5.4.3. Who to contact in case assistance is needed regarding privacy.



6- Data Transfer and Data Security

- 6.1. Entities shall observe patients legal right to seek information and shall document patients' verbal or written requests for information with the signature of the requestor.
- 6.2. Entities shall ensure to update the electronic EMR systems when accommodating these requests as and when needed.
- 6.3. Entities shall retain communications and documentations associated with these requests for a minimum period of 25 years as mandated by "the use of information technology and telecommunication in healthcare field" (Federal Law no. 2, 2019).
- 6.4. Entities shall exchange information on Abu Dhabi Health Information Exchange, Malaffi, in accordance with DOH's Chairman Resolution no. 90, 2018, the rules, circulars, policies and agreements in implementation thereof.
- 6.5. Protected Health Information Disclosure-Related Incident Response & Mitigation
 - 6.5.1. Entities must mitigate, to the extent practicable, any harmful effect they learn was caused by the use or disclosure of protected health information (PHI) by their staff, trainees, vendors, third party contractors or business associates in violation of their privacy policies and procedures and communicate with relevant health authorities within 24hrs of initial knowledge of the breach.
 - 6.5.2. Entities shall establish incident response management plans that comprise of identification of the incident, containing the incident, eradicating/ eliminating the incident, recovery and recover/repair and documenting the lessons learnt.
 - 6.5.3. Entities must thoroughly investigate the incidents starting from the point of discovery until closure:
 - 6.5.3.1. Determine if the incident is related to a violation of PHI.
 - 6.5.3.2. Determine if further investigation is warranted, and if not, then document the incident and retain.
 - 6.5.3.3. List and perform mitigation, remediation and sanctions.
 - 6.5.3.4. The investigation and documentation shall be systematic / organized and can be reported to respective authorities as needed.
 - 6.5.3.5. Maintain all records of the incident as per local legal / regulations.
 - 6.5.3.6. Use appropriate investigative procedures and preserve the chain of custody.
 - 6.5.3.7. Involve resources trained in incident handling when needed.
 - 6.5.3.8. Educate and document why and how to prevent recurrence of the incident.
 - 6.5.4. Entities' incident management plan shall have the provisions to timely communicate to the relevant authorities the incident response and mitigation.
- 6.6. Data Safeguards
 - 6.6.1. Entities must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in line with Abu Dhabi Health Information Cyber Security Standard (ADHICS) as well as the applicable laws and regulations. Such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, having a secured application, segregation of duties, least privilege, and limiting access on a "need to know" basis.



6.7. Data retention and monitoring

- 6.7.1. Entities shall maintain health data and information as per the data retention period of 25 years mandated by “the use of information technology and telecommunication in healthcare field” (Federal Law no. 2, 2019).
- 6.7.2. Entities resolution of complaints, and other actions, activities, and designations shall also be documented and retained.
- 6.7.3. Entities are required to undergo periodic internal and external audits and independent reviews to monitor compliance with the data privacy requirements as specific in this standard.
- 6.7.4. Entities shall retain and furnish the outcomes of the audit / compliance to DOH on a need basis.

7- Enforcement and Sanctions

- 7.1. Any deviation from the data privacy standard should be approved by DOH.
- 7.2. DOH may impose sanctions in relation to any breach of requirements under this standard in accordance with the Complaints, Investigations, Regulatory Action and Sanctions Chapter, Healthcare Regulator Manual.



8- Appendix A - Detailed Description of the Requirements

1. Data Privacy Policy and Procedure

The entity shall establish and communicate a policy and related procedure that states its objectives and responsibilities regarding data privacy and is in line with accepted privacy principles and applicable local laws and regulations.

DP-PP-01	Entity shall have a documented data privacy policy and related procedures, which are communicated to internal and external stakeholders as appropriate, and are reviewed / approved periodically.
DP-PP-02	The data privacy policy explains the purpose of the entity regarding the protection of privacy and personal data.
DP-PP-03	Policy shall cover obligations to legal, regulatory, and contractual requirements regarding data privacy
DP-PP-04	Privacy policy and procedures shall cover human resources practices (e.g., provisioning, de-provisioning and personnel screening) etc.

2. Inventory of Systems

The entity shall identify any inherent potential privacy risk in the data processing systems and products and inform the management.

DP-IS-01	Entity shall ensure systems/products/services that process data are inventoried.
DP-IS-02	The entity shall identify and document owners or operators (i.e. the entity or third parties such as service providers, partners, customers, and developers) and their roles / responsibilities with respect to the systems/products/services and components (e.g., internal or external).
DP-IS-03	The entity shall evaluate its role in the data processing ecosystem is identified and documented.

3. Roles and Responsibilities

The entity shall establish and implement clear roles and responsibilities regarding the attainment and safeguarding of personal data.

DP-RR-01	The entity shall assign coordination, oversight and monitoring of privacy to a designated person as required. The responsibility, authority, and accountability of the designated person are clearly documented and regularly reviewed.
DP-RR-02	The roles and responsibilities of users, including Senior Executives, in the protection of personal data and compliance with privacy policies and procedures have been established and communicated to all.

4. Identification of Personal Data and Classification (PHI, EPHI)

The entity shall document what personal data is stored, classification of data, compliance with laws and regulations while processing.

DP-PDC-01	The entity shall develop and implement a process to identify and document the processing of personal data and classifying that data as needed, that includes processes, systems and third parties that handle personal data.
DP-PDC-02	The entity shall maintain and manage a systematic record of personal data processing activities including the characteristics of these activities (legitimate basis, purpose, categories of data etc.).



5. Risk Management to Identify and Mitigate Privacy Risks

The entity shall methodically and periodically identify, assess, and mitigate risk factors that affects the attainment of data privacy objectives.

DP-RM-01	The entity shall have a process to periodically identify and assess the risks that affects data privacy objectives including their impact and the probability to implement adequate risk responses and control measures. Data Privacy risk assessment is part of the process of identifying, evaluating, prioritizing, and responding to specific data privacy risks.
DP-RM-02	Entity shall re-evaluate data privacy risk on an ongoing basis, including the entity's business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
DP-RM-03	The entity shall plan and implement the controls that are necessary to mitigate the identified privacy risks. Entity's risk tolerance is determined and clearly expressed. Progress of execution is monitored and measured.

6. Assessment of Data Protection Requirements

The entity shall systematically identify, assess and address the data privacy-related impact of new products and services.

DP-DP-01	The entity shall implement a managed and documented process to carry out an assessment of the impact on data privacy of new or significantly changed processes, products and services.
DP-DP-02	The assessment shall take into account the purposes of processing in relation to the necessity and proportionality of processing personal data.
DP-DP-03	The entity shall plan and implement the controls that are necessary to mitigate the identified data privacy risks. Progress of execution shall be monitored and measured.
DP-DP-04	Any change management process in the entity shall ensure that data privacy requirements from the assessment are implemented before the change is executed.

7. Data Privacy Incident Management

The entity shall effectively detect and handle data privacy-related incidents to appropriately limit their consequences and to take measures to prevent future breaches. The entity shall perform root cause analysis and document lessons learned from the incidents.

DP-PI-01	A formal, comprehensive privacy incident and breach management process shall be implemented, covering the following: I) The responsibilities of users to inform the designated patient in case of a data privacy incident or possible data breach. II) The designated privacy or security officer assesses whether the incident is privacy related. In case of a personal data breach, the privacy or security officer documents the nature of the breach, the consequences, and the approximate number of data records and data subjects affected. III) The privacy or security officer initiates and coordinates required actions, and determines the required involvement of patient and stakeholders to be informed. IV) The privacy or security officer monitors the progress of remediating actions and reports to management. V) Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are developed, tested and implemented.
DP-PI-02	The privacy incident management process shall include a clear and timely escalation path, based on



	the type and severity of incident, up to relevant authorities and executive management with mitigating measures.
DP-PI-03	The incident management process shall detail the lessons learned which can then be included in the entity's data privacy awareness programs.
DP-PI-04	After a data privacy incident or data breach, a formal incident evaluation shall be conducted and shall include relevant stakeholders (internal / external) and consider the following: <ul style="list-style-type: none"> • Root cause of the incident • Corrective / Preventive action taken • Incident patterns (whether its repetitive or new) • Services impacted etc.

8. Training and Awareness

Entity shall ensure the staff with access to personal data / personal data processes have the necessary data privacy trainings to effectively perform their roles.

DP-TM-01	The entity shall identify, conduct and document the appropriate training to staff members and a process in place to bridge competency gaps.
DP-TM-02	The entity shall ensure data privacy competencies / training as part of the on boarding process.
DP-TM-03	The entity shall have a process to periodically review the competency of the staff and other resources including 3 rd party vendors.
DP-TM-04	The Entity shall review the training and awareness courses periodically to reflect current regulatory, industry, and privacy policy / procedure requirements.

9. Periodic Review of Changes in Regulatory / Business requirements

Entity shall consider the risks to data privacy whenever there are changes within the entity as well as the changes in the regulatory requirements.

DP-RB-01	The entity shall implement a process to monitor, assess, and address the impact on data privacy requirements from time to time: <ol style="list-style-type: none"> I) Legal and regulatory requirements. II) Industry requirements, best practices and guidelines. III) Contracts, including SLA and privacy requirements with third parties. IV) Business operations and processes. V) People given responsibility for privacy and security. VI) Technology (existing / new). VII) Acquisitions & external integrations.
----------	--

10. Data Minimization (Need to know / Minimum necessary)

Entity shall have adequate controls to restrict the access to personal data. Entity shall follow the principles of 'need to know' and 'minimum necessary' while providing / processing personal data.

DP-DM-01	Entity shall put in a process to: <ol style="list-style-type: none"> I) Identify the extent to which personal data is essential for the purposes of the entity's operations. II) Grant access to the personal data for the minimum extent required for processing III. Periodically review the continuing necessity of personal data in the entity's processes / operations.
----------	--



11. Privacy by Design & Privacy by Default

The entity shall enforce the principles of Privacy by Design & Privacy by Default when designing / updating / changing products, services, business systems and processes.

DP-PD-01	<p>I) The entity shall apply the data privacy principles / requirements throughout the system development life cycle (SDLC) phases of plan, design, build/buy, deploy, operate, and decommission.</p> <p>II) The entity shall consider the privacy principles and privacy risks a component of entity's development methodology.</p> <p>III) The entity shall ensure that the third parties / vendors involved in the entity's processes / services observe the same principles.</p>
DP-PD-02	The development and testing environment(s) are separate from the production environment.

12. Data Access / Safeguards

Entity shall have a process to timely respond to the patient's access requests.

DP-DA-01	The entity shall document security requirements of personal data in relevant information security policies and procedures.
DP-DA-02	The entity shall validate the identity of the requesting patient before responding.
DP-DA-03	The entity shall have a process in place to timely provide the personal data, in a commonly used electronic form or as per the request of patient. Records of data disclosures and sharing are maintained and can be accessed for review.
DP-DA-04	The entity shall have a process to timely respond to patient's correction requests / deletion requests and ensure that patients are able to determine whether their personal data is correct / up-to-date.
DP-DA-05	The entity shall perform periodic assessments to check the accuracy of personal data records and to correct them, as necessary to ensure that the personal data collected is in line with the purpose.
DP-DA-06	<p>The entity shall ensure appropriate procedures and agreements with relevant clauses, as denoted below, are in place if the personal data is being handled by third parties on behalf of the entity, including notifying patient and obtain their consent prior to disclosing personal data to a third party if needed.</p> <p>I) Confidentiality and non-disclosure.</p> <p>II) Security requirements to process (i.e. at store, at transfer etc.) the personal data securely.</p> <p>III) Providing data timely when and as required.</p> <p>IV) Incident handling and reporting in case of personal data breach.</p> <p>V) Retention requirements and secure data disposal.</p> <p>VI) Restriction clauses for no further subcontracting without permission of the entity.</p> <p>VII) Liabilities and indemnifications.</p> <p>VIII) Clause to periodic audits to ensure compliance.</p> <p>etc.</p>
DP-DA-07	The entity shall ensure that patient's data is not transferred out of the country as per local laws and regulations.
DP-DA-08	The entity shall take relevant administrative and technical measures to ensure security of personal data that includes establishing policies, processes, and procedures for authorizing data processing (e.g., organizational decisions), revoking authorizations, and maintaining authorizations etc.
DP-DA-09	Entity shall ensure that protected health information is secured as appropriate from accidental errors or loss, and from malicious acts such as hacking or deliberate theft, disclosure or loss.
DP-DA-10	The entity shall have a documented policy on encryption and pseudo-nomination of personal data and systematically verified.



DP-DA-11	The entity shall establish and ensure that the access provisioning mechanism to users are based on roles, least privilege, segregation of duties and legitimate business needs to access the personal data and that it also covers necessary authentication mechanism such as unique username and password, certificate or token based on the criticality of the data.
DP-DA-12	The entity shall implement intrusion detection and monitoring systems as needed. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
DP-DA-13	The entity shall ensure that the personal data is protected by using appropriate encryption mechanism (Data at rest / Data in transit).
DP-DA-14	Entity shall ensure network integrity is protected as appropriately by implementing necessary controls (e.g., network segregation, network segmentation).
DP-DA-15	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
DP-DA-16	The entity shall ensure configuration change control processes are established and in place. A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).
DP-DA-17	The entity shall have a process in place for periodic backups of data are conducted, maintained, and tested.
DP-DA-18	Entity shall have a vulnerability management plan / procedure to ensure the vulnerabilities are identified and necessary remediation are taken timely.
DP-DA-19	Entity shall establish procedure / process to ensure removable media is protected and its use restricted as appropriately.
DP-DA-20	The entity shall implement relevant mechanisms such as failsafe, load balancing, hot swap to avoid single point of failure and to achieve resilience requirements in normal / adverse situations.
DP-DA-21	Entity shall periodically assess data processing systems using audits, test results, or other forms of evaluations to confirm they are meeting their contractual / regulatory / privacy obligations.

13. Retention of Records

The entity shall ensure that personal data is retained for minimum period of 25 years as mandated by “the use of information technology and telecommunication in healthcare field- law no. 2, 2019”.

DP-PR-01	<p>The entity shall:</p> <ul style="list-style-type: none"> I) Document its retention policies and disposal procedures for personal data. II) Make sure that the personal data is not kept beyond the established retention time unless there is a justified business or legal reason. III) Communicate retention time policies to respective stakeholders in its privacy statement as needed. IV) Retain, store, and securely dispose records in accordance with its retention policies. V) Consider the additional requirements / controls when data is retained longer than necessary as exceptions based on legal / regulatory obligations.
----------	--



14. Secure disposal

Entity shall have a process to anonymize / secure dispose of personal data once it is crossed its retention date.

DP-SD-01	<p>The entity shall:</p> <ul style="list-style-type: none">I) Have in place policies and standard operating procedures (SOPs) and evidence of their implementing record retention and disposal practices as per facility policies and SOPs.II) Ensure that record management, retention and disposal procedures are consistent with this Standard and requirements of relevant laws.III) Educate staff within their facility on compliant and sound record retention and disposal practices.IV) Ensure the confidentiality and privacy of records/information during the process of archiving/conciliation/transferring to an offsite location.V) Ensure that storage systems (offsite & onsite) are equipped with environmental control, applicable safety, privacy and security measures. If commercial storage system is opted, regular site visits to such companies/sites must be conducted to confirm safety, privacy and confidentiality of records.VI) Record and maintain / retain destruction logs securely for tracking purposes.
----------	---

9- Appendix B - References

Laws and Regulations	Description	Location
<ul style="list-style-type: none"> The Decision of the Chairman of the Department of Health No (36) of 2019 on the Disciplinary list of Healthcare Sector of Abu Dhabi. 	<ul style="list-style-type: none"> DOH guidelines on the disciplinary actions for the Abu Dhabi health sector for the violation of the Federal law No (2) of 2019 on the use of information and communication technology. 	https://doh.gov.ae/en/resources/Circulars
<ul style="list-style-type: none"> ADHICS – Abu Dhabi Healthcare Information and Cyber Security Standard 	<ul style="list-style-type: none"> ADHICS Standard outlines the control mandates essential to protect health information during its creation, maintenance, display, processing, usage, transmission and disposal, and to maintain the information’s confidentiality, integrity and availability. 	https://doh.gov.ae/en/resources/standards
<ul style="list-style-type: none"> ADHIE – Abu Dhabi Healthcare Information Exchange 	<ul style="list-style-type: none"> The Abu Dhabi Health Information Exchange as operated by the ADHIE Operator. Where the context requires, references to the rights and obligations of ‘ADHIE’ shall mean the rights and obligations of ADHIE Operator. 	https://doh.gov.ae/en/resources/standards
<ul style="list-style-type: none"> ADHIE Platform 	<ul style="list-style-type: none"> The electronic health information exchange platform for the Emirate of Abu Dhabi designed, developed, implemented, maintained and operated by the ADHIE Operator. 	https://doh.gov.ae/en/resources/standards
<ul style="list-style-type: none"> Policy on the Abu Dhabi Health Information Exchange (HIE) 	<ul style="list-style-type: none"> Outlines the sector wide objective and strategy for the meaningful and safe exchange of health information 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Regulator Manual 	<ul style="list-style-type: none"> Describes the main functions of DOH as a regulator for Abu Dhabi health sector. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Healthcare Providers Manual 	<ul style="list-style-type: none"> Set out the duties which apply to the operators of Healthcare Facilities in Abu Dhabi. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Healthcare Professionals Manual 	<ul style="list-style-type: none"> Set out the duties which apply to those individuals who are members of a Healthcare Profession in Abu Dhabi. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Policy on AI 	<ul style="list-style-type: none"> Outline key roles and responsibilities of relevant stakeholders in relation to the use of AI in healthcare. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Insurers Manual 	<ul style="list-style-type: none"> Set out the duties which apply to authorized insurance providers, Insurers and associated persons in Abu Dhabi. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Policy on Medical Tourism 	<ul style="list-style-type: none"> Policy is to support and ensure the interests of all stakeholders in the Abu Dhabi healthcare system are safeguarded in order to support the growth of medical tourism in Abu Dhabi. 	https://doh.gov.ae/en/resources/policies
<ul style="list-style-type: none"> DOH Standard for Medical Tourism in the Emirate of Abu Dhabi 	<ul style="list-style-type: none"> The Standard mandates the minimum specific requirements for healthcare 	https://doh.gov.ae/en/resources/standards



	providers participating in DOH Medical Tourism Program and Network.	
<ul style="list-style-type: none"> HAAD Guidelines for Patient Consent 	<ul style="list-style-type: none"> Sets out the guidelines and best practices for obtaining patient consent for and information discloser. 	https://doh.gov.ae/en/resources/guidelines
<ul style="list-style-type: none"> Federal Law No. (2) for the year 2019 on the Use of Information and Communications Technology (ICT) in Healthcare 	<ul style="list-style-type: none"> Federal law which regulates the use of information technology and communications (ITC) in the healthcare sector in UAE. 	