Document Type: Health Information Policy	**Ref No:** DHA/HISHD/PP-13	**Version Number:** 1
Document Title: Policy for Health Data and Information Sharing	**Issue Date:** 10/08/2024 **Effective Date:** 10/11/2024 **Revision Date:** 10/08/2029	
Ownership: Dubai Health Authority		
Applicability: All Healthcare Entities under the Jurisdiction of Dubai Health Authority		

1. Definitions/Abbreviations:

Anonymisation: Anonymised information does not identify an individual; and cannot be practically used to determine their identity. Anonymisation requires the removal of any direct identifier and quasi-identifiers (e.g. detail, or combination of details, that might enable identification, either by itself or when used with other available information). Effectively anonymised information (where the prospect of identifying individuals is remote), is not seen as personal data and therefore data protection rules do not apply. The anonymised information can be used or disclosed without the Data subject's/Patient`s consent, as the information cannot be used to identify a specific individual. However, the anonymisation must be done effectively, and neither the anonymisation process, nor the use of the anonymised information, should have any direct detrimental effect on any particular individual.

Compliance: Commitment and adherence to applicable legislation and the decisions issued by the authority.

Confidentiality: Protecting data and information from access or disclosure by unauthorized persons in accordance with applicable legislation in this regard.

Consent: Permission given by the Data Subject/Patient to access/process his/her personal data. Consent should be specific, clear, and unambiguously.

Controller: It is the Entity that has health data and information, and by virtue of its activity, determines the method, standards, and criteria for processing this data and information; and the purpose of the processing. In this Policy, the Controller is the Entity.

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: Evaluation of potential risks to the privacy and confidentiality of health data. It proposes procedures/measures to reduce potential risks to the protected health information, and how to avoid these risks at an early stage of processing and to the greatest extent possible.

Data Sharing Agreement: A formal agreement between the Entity (as the controller) and a requester (as a. processor) to share information/data according to specific terms and conditions and consistent with the principles of data sharing.

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

Direct identifiers: Any data which can be used, directly or indirectly to identify a person (the 'Data Subject').

Disclosure: The passing of information from the Data Controller to another Entity/ individual.

Electronic Medical Record (also known as Electronic Health Record): is a systematic collection of electronic health information of an individual in a digital format that conforms to nationally recognized interoperability standards and enables information to be used and shared over secure networks.

Encryption: The use of an algorithmic process to transform Data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. This will prevent unauthorized access to/use of information.

Entity: Any Entity or institution within the Emirate of Dubai that provides health services to people, including: the areas of prevention, treatment, and recovery, whether owned or managed by a natural or legal person. It may also include providers of health insurance or health insurance services, third party claims administrators, or those managing insurance requirements/services; or Electronic services in the health field, or any services directly or indirectly related to the application of the provisions of this policy.

Health Information: Health data that has been processed and made apparent and evident

whether visible, audible or readable, and which are characterized by a health nature whether related to health facilities, health insurance agencies, or beneficiaries of health services.

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

Health Registry: is a regular collection of data and information from the patient's file on certain diseases and health conditions.

Good Clinical Practice: Good clinical practice is an international quality standard for conducting clinical trials that in some countries is provided by International Conference on Harmonisation (ICH), an international body that defines a set of standards, which governments can then transpose into regulations for clinical trials involving human subjects.

Information Asset: Health assets within the Entity including:

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

Incidents: A security incident is an event that leads to a violation or imminent threat of violation of information security policies, acceptable use policies, or Entity`s security standard; and puts sensitive data at risk of exposure.

Incompetent Data Subject: Refer to the Data Subject/Patient who either lack the full legal

capacity (minor, or has intellectual disability; or mental incapacity) or have the full capacity, but is unable to provide a Consent (e.g. unconscious).

Legal Guardian: A person appointed by the law to consent in place of an incompetent Data Subject/Patient based on UAE federal laws and/ or local regulation, when the Patient is unable to provide Consent due to an illness or incompetency.

Medical Records (also called Health Records): It is a systematic collection of an individual's electronic health data and information in a digital format that conforms to nationally recognized interoperability standards and allows the information to be used and shared over secure networks.

Medical/Dental Resident: is a Sharyan registered medical/dental doctor who is taking part in a post-graduate medical/dental training program accredited by the UAE; under the direct or indirect supervision of a senior registered medical/dental clinician.

Minor: Any person below eighteen (18) years of age.

Primary Use of Health Information: The information collected by the healthcare provider for the primary purposes of giving treatment and health care to the Data Subject/Patient.

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.

Protected Health Information: also referred to as Personal Health Information; is any data that can be used, directly or indirectly to identify a person (the 'Data Subject'). In particular by reference to an identifier such as a name, an identification number, location data, an

online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. This include any of the 18 types of direct identifiers specified below[1]:

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

[1] The HIPAA Privacy Rule

- 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: Covers creating, entering, using, modifying, updating, deleting, storing, disclosing and disposing of data.

Pseudonymisation: is where an individual's identity is disguised/concealed by using a unique identifier (a pseudonym). Other terms that are used for this kind of dataset are masked, key-coded, single coded, obscured, and obfuscated. Pseudonymised information is still considered personally identifiable information and therefore although it does not reveal an individual's 'real world' identity, it allows the linking of different data sets for the individual concerned; leading to re-identification of PHI. Therefore, data should be handled cautiously, and must only be transferred using secure means.

Quasi-identifiers: are variables in the dataset that are not directly identifying but can be known by an adversary and used to re-identify an individual.

Secondary Use of Health Information: is using health information for purposes other than treating the individual Data Subject/Patient, such as for Research, Public Health, Quality Improvement, Safety Initiatives, and marketing. Some secondary uses directly complement the needs of primary use. Examples include medical billing, hospital administrative, and management operations.

Sensitive Health Information: special categories of personal health information that require

greater protection and justification for usage and sharing. This data is previously defined under the DHA Health Information Assets Classification policy Health Information Assets Classification and includes:

- Drug abuse.
- Alcohol abuse.
- Sexual health (including sexually transmitted diseases and Human immunodeficiency virus infection).
- Reproductive health.
- Mental health / Behavioral health.
- Genetic information.
- Child pregnancy.
- Child Protection and Safeguarding related issues.

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

DSA : Data Sharing Agreement

DHA : Dubai Health Authority

DPIA : Data Protection Impact Assessment

EMR : Electronic Medical Record

HISHD : Health Informatics & Smart Health Department

HRS : Health Regulation Sector

ICH_GCP	:	International Conference on Harmonisation _ Good Clinical Practice
ICT	:	Information and Communications Technology
IG	:	Information Governance
IS	:	Information Security
IT	:	Information Technology
PHI	:	Protected/Personal Health Information
UAE	:	The United Arab Emirates.

2. Purpose

2.1. To set out Dubai Health Authority (DHA)`s requirements for sharing health data and Protected/Personal Health Information (PHI); in line with the United Arab Emirates (UAE) laws, Emirate of Dubai legislative, and DHA regulatory frameworks.

2.2. To assure Entities under jurisdiction of DHA are providing a secure channel for sharing of health data and information, especially PHI.

2.3. To provide a framework for the controls needed on PHI sharing, and ensure the expected standards are met.

2.4. To govern the procedures for health data and information sharing, ensuring its confidentiality and protecting it from unauthorized persons, preserving the privacy of the Data Subject/Patient.

3. Scope

3.1. All Protected Health Information (PHI) within the Emirate of Dubai shared by Entities under jurisdiction of DHA.

3.2. Health Information as defined by UAE Information and Communications Technology (ICT) in Healthcare law includes information/data in all its form. This includes but is not limited to:

3.2.1. Medical records (health and care records) and health registries – for example: birth, death, accident and emergency, theatre, minor operations, etc.).

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

3.2.3. Laboratory assets (paraffin blocks, slides, digital images etc.) and Patient test reports.

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

3.2.5. Identifiable and non-identifiable data.

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

3.2.7. Microform (microfiche or microfilm).

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

3.2.9. Physical or digital forms of data/records.

3.2.10. Structured record systems (Paper and electronic).

3.3. All users accessing and using health data and PHI in healthcare sector in the Emirate of Dubai; including all employees, trainees, students, contractors, consultants, suppliers, vendors, partners, health insurance stakeholders, customers and wider stakeholders where appropriate.

4. Policy Statement:

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

4.2. All applicable UAE laws, Emirate of Dubai legislations, and DHA regulations on health data and information are considered in this policy.

4.3. The Collection, Use and Sharing of Personal Health Information

4.3.1. Consent of the Data Subject/Patients needs to be sought for the collection of health data and information (Health Information Assets Classification); and also before their health data and information is shared for any reasons other than direct provision of health care and where it is not covered by any other legal condition in the UAE Laws and DHA regulations.

4.3.2. Consent should be as per DHA requirements (Consent & Access Control Policy).

4.4. Systematic Versus Ad-hoc Sharing of Protected Health Information

This policy covers both systematic and ad-hoc health data and information sharing:

4.4.1. Systematic/routine information sharing:

a. The same data sets are shared between the same Entities for an established purpose in accordance with the provisions of applicable legislation, as it is prohibited to circulate any health data and information without the written consent of the patient, except in legally specified cases.

b. Systematic information sharing should be governed by a written agreement/contract between the Entities that sets out the rules and process for access and use of the PHI.

4.4.2. Ad-hoc information sharing:

a. Is a one-off disclosure of PHI to the authorized person under applicable legislation. In some cases, this may involve a decision about sharing of PHI in emergency cases/situations (e.g. public health emergency); in accordance with the provisions of applicable legislation, as it is prohibited to circulate any health data and information without the written consent of the patient, except in legally specified cases.

b. All ad-hoc sharing decisions must be carefully considered by Entity`s Information Governance team and documented properly. The requests must be carefully evaluated case by case and decision taken based on:

i. Type of health data and information requested (e.g. Identifiable or non-identifiable data/information).

ii. Sensitivity of health information: some information have high sensitivity and utmost caution should be taken while sharing. This include but not limited to chemical dependency, human immunodeficiency virus infection, mental health conditions, behavioral health reports (details can be found on: Health Information Assets Classification).

iii. Information timeline (months, years, etc.)

iv. Purpose of sharing health data/information.

v. Who will access the health data/information.

vi. What other data is collected along with the requested health information.

4.5. Prerequisite of Protected Health Information Sharing

4.5.1. All PHI sharing with external Entities must be governed by an appropriate Data Sharing Agreement (DSA); and must meet the requirements of the relevant UAE legislations and DHA Policies.

4.5.2. Data sharing agreements should be registered by the Information Governance team within the Entity; and all data flows should be recorded on the Information Asset Register.

4.5.3. Protected health information must be shared only in accordance with the provisions of applicable legislation and by those authorized to do so depending on

the nature of each case, and access to PHI must be role-based with an appropriate credible mechanism. The facility must monitor and audit access to PHI on a regular basis.

4.5.4. The two parties' sharing PHI should come to an agreement on baseline data standards and description.

4.5.5. Only the minimum amount of PHI requested should be shared, and should be checked for accuracy before release; to avoid errors.

4.5.6. Health Data and information should only be shared via secure and authorised means, and appropriate technical safeguards must be in place to protect the PHI.

4.6. Protected Health Information Sharing for Care Purposes (Primary use of PHI)

4.6.1. Health care professionals may share information in the best interests of Data Subjects/Patients within the framework set out by the UAE ICT Law and DHA "Health Data & Information Protection and Confidentiality Policy" (Health Data & Information Protection & Confidentiality Policy).

4.6.2. The primary concern must be for the individual receiving direct care, and a failure to share information (both efficiently and securely) may have serious consequences for Data Subject/Patient welfare.

4.6.3. Protected health Information sharing within the Entity should be limited to staff who have a legitimate professional reason to access the PHI as part of their contract with the Entity.

4.6.4. Where a Patient's care/treatment is transferred to another Entity, a copy of the medical record may be transferred directly with the Data Subject/Patient or via a request from the other Entity (separate Patient consent is required in this case).

4.6.5. Below table demonstrates different settings that PHI can be shared for Data Subject/Patient care purposes:

Care Purpose/Primary Use of Health Information		
Between Entities in Dubai	Medical record transfer with Patient consent	Nabidh access with Patient consent
Between Entities of the same organization in the UAE	Patient consent needed	
Between Entities (not within the same organization) in the UAE	Patient transferring his/her own Health Information	• Referral process with clear signed consent • HIE Exchange (Nabidh, Malaffi, Riayati) with Patient consent
Patients who are being treated outside the UAE, within the limits of the necessary treatment procedures.	Patient consent needed	
Health Data related to samples that are sent to laboratories outside the UAE.	Patient consent needed	

4.7. Protected Health Information Sharing for non-Care Purposes (Secondary use of Health Information)

4.7.1. All Entities that share PHI are required under UAE laws and DHA "Health Data &

Information Protection and Confidentiality Policy" (Health Data & Information Protection & Confidentiality Policy) to protect it from inappropriate disclosure.

4.7.2. For data associated with "UAE National Genome Project", it should be as per UAE National Genome Repository Data Access Framework and related policies.

4.7.3. Effective pseudonymisation and anonymisation techniques enable the Entity to undertake secondary use of PHI in a safe, secure and legal way. Through de-identification, users may make use of individual data for a range of secondary purposes without having to access the identifiable PHI.

4.7.4. The Entity is legitimate to process the PHI without Data Subject/Patient consent in certain circumstances, as per article (16) of UAE ICT Health law and article (4) of UAE Data Protection Law. In accordance with Article (16) of Federal Law No. (2) of 2019 regarding the use of information and communications technology in health fields and Article (4) of Federal Law No. (45) of 2021 regarding the protection of personal data, everyone who handles patient data and information must maintain It confidential and not use it for purposes other than health purposes without the written consent of the Data Subject/Patient, except in certain cases and in accordance with applicable legislation.

4.7.5. Below table elaborates more in details the secondary use of PHI:

Sharing PHI for Non-Care Purpose/Secondary Use of Health Information without Data Subject/Patient Consent	
Justification	**Type of Information**
At the request of the competent judicial authorities.	Identifiable Health Information
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.	
Health information required by the health insurance companies or any provider of health services in respect of the health services received by the Patient for purposes of auditing, approving, monitoring, verifying or reimbursing healthcare claims	
At the request of the health authorities (Ministry of Health and Prevention (MOHAP) and Dubai Health Authority (DHA)) to 1. Take preventive and curative measures related to public health. 2. Maintaining the health and safety of the Data Subjects/Patients or any other individual in contact with the Data Subjects/Patients (e.g. protection against communicable diseases/epidemics and serious cross-border threats to health). 3. In cases of Public safety emergencies to maintain the health and safety of Data Subjects/Patients, their families or any other persons in contact with them, or the wider community.	
Public health authorities (MOHAP and DHA) who are legally authorized to receive reports for the purpose of preventing or controlling disease, injury, or disability.	
At the request of the DHA for the purposes of audit, inspection, supervision, risk management, and error management.	
To determine the availability, quality, safety, equity and cost-effectiveness of healthcare services.	Non-identifiable Health Information
At the request of the DHA for analysis or compiling of statistical information with respect to the management of, evaluation or monitoring	

of, the allocation of resources to or planning for all or part of the health system including delivery of services.	
For the purposes of scientific and clinical research, provided that the ethics and rules of scientific research are followed as per ICH_GCP principles and guidelines.	Non-identifiable If Identifiable data needed, then Patient consent required
For development and innovation activities or health registries	

4.8. Protected Health Information Sharing

4.8.1. Sharing of any PHI should be governed by clear rules that satisfy the requirements of UAE laws and DHA regulations to enable efficient practices by both the disclosing and receiving parties.

4.8.2. Individuals' rights regarding the sharing of their PHI must be supported by the Entity. The Entity must set out high-level commitments for protecting and safeguarding PHI; particularly in relation to how PHI will be shared (both internally and externally).

4.8.3. The DHA has set out a series of Data Subject/Patient rights and pledges (Health Data & Information Protection & Confidentiality Policy) which all Entities under it`s jurisdictions are required to comply with. This includes respecting individual's right to preserve their privacy and confidentiality, and to expect the Entity to keep (their) confidential information safe and secure.

4.8.4. The Entity must ensure that all information transfer/sharing in or out of the organisation are protected by appropriate information sharing protocols and that the receipt and transfer of all PHI and Entity`s confidential information occurs

within the boundaries of UAE laws and DHA regulations.

4.8.5. Consent must be obtained as appropriate from Data Subject/Patient before sharing PHI as per this policy.

4.8.6. There must be regular reviews/audit of PHI sharing practices within the Entity.

4.9. Sharing Protected Health Information with Police

4.9.1. Protected health information can be disclosed to the police in order to assist in the prevention or detection of crime and/or the apprehension of prosecution of offenders.

4.9.2. If the Data Subject/Patient is available and capable, they should be asked to provide their consent to disclose the information requested.

4.9.3. If the Data Subject/Patient is not able to provide consent (including but not limited to: unconscious Patients; subjects with an intellectual disability or mental incapacity); or if the Patient is minor (under 18 years), then signature of the parent or legal guardian is required on the consent to share PHI.

4.9.4. For the Entity to consider releasing any PHI without Data Subject/Patient consent, the request must relate to a serious crime, otherwise the Police should be asked to obtain a Court Order or written signed consent from Data Subject/Patient.

4.9.5. All requests from the police should be submitted in writing (electronic or hard copy), ideally presented on an appropriate official form of documentation.

4.9.6. Requests must be dealt with by the Entity`s Information Governance team for

review/reject/approval.

4.9.7. Occasionally urgent requests might be made asking for specific information to be provided in a short period of time. Often this is due to strict timelines imposed on the police to make decisions to charge suspects or to support urgent lines of investigation. In these circumstances, decisions should be taken by the medical director of the Entity and/or the Entity's legal Team before any disclosure is made.

4.9.8. A copy of the Police request, the decision made and any information supplied must be recorded on the Data Subject's/Patient`s medical record.

4.10. Sharing Protected Health Information through Emails

4.10.1. Protected Health Information should only be sent via email if it is appropriately encrypted or it contains links to Patient data within technology portal that is already protected by an authentication mechanism.

4.10.2. Only official Entity issued email accounts should be used to send or discuss PHI.

4.10.3. Personal/home email addresses should never be used by staff for any Entity business for sharing PHI.

4.10.4. Where the email is sent from an Entity account to a domain included on the IT (e.g. information technology) secure list, the email and any attachments must be automatically encrypted; the same must be applied for emails sent between Entities. Emails sent to any other address should be manually encrypted and the

word '(Encrypt)' should be added in the subject line of the email.

4.11. Sharing Protected Health Information through Removable Media (USB Sticks, CD's/DVDs etc.)

4.11.1. Protected health information should not be stored on removable media unless absolutely necessary with encryption. If there is a requirement to use removable media, the healthcare provider should discuss the available options with Entity's competent department.

4.11.2. Where the use of removable media is required and approved, the information should only be retained on the device for the minimum period possible (the information should be backed up to a networked storage if it is to remain on the device for more than a simple transfer between Entity systems).

4.11.3. Only an Entity approved encrypted device should be used and the physical security of the device must be protected.

4.11.4. Devices shall be exchanged through identified personnel only.

4.11.5. Non-Disclosure Agreement (NDA) must be mutually signed in case of transit of physical media, when managed through external parties.

4.12. Sharing Protected Health Information through Faxing

4.12.1. Faxing is not encouraged as a method of PHI transfer for the reasons of information safety and confidentiality.

4.12.2. Personal and confidential information must only be sent by fax where it is absolutely necessary to do so, and there is no alternative method of transfer.

4.12.3. The use of secure email should always be considered first, before sending information by fax. Where it is absolutely necessary to send a fax message, this should be sent using the safe procedures as described below:

a. The fax should be sent to a safe location where only individuals that have a legitimate right to view the information can access it.

b. Confidential faxes, both incoming and outgoing must not be left where unauthorised people may see them.

c. Any faxes sent must include a cover sheet, which is marked 'Private and Confidential' and contains a suitable confidentiality clause.

d. The sender must be certain that the correct person will receive the fax. The recipient must be notified when the fax is being sent and should be asked to acknowledge receipt. If possible, a report sheet should be produced to confirm successful transmission.

e. Staff should ensure that the fax number is correct and take care when dialling. Where possible, pre-programmed numbers should be used (and regularly checked for any changes).

f. Only the minimum amount of personal and confidential information should be included in the fax message. Where possible, the information should be anonymised or pseudonymised. If a document is incorrectly received within the

Entity, it is the receiving ward/department's responsibility to ensure that it is given to the named recipient and the sender is notified of the error. The error should also be logged.

4.13. Sharing Protected Health Information through Mailing/Posting/Courier

4.13.1. Envelopes containing PHI must be securely sealed, addressed to a specific individual and care should be taken by staff to ensure that envelopes do not contain information, which is not intended for the recipient.

4.13.2. Care must be taken to ensure that both internal and external mail is addressed correctly and is packaged appropriately.

4.13.3. When sending highly sensitive or confidential information, careful consideration should be given to the method of transport and the suitability of packaging material. When sending by external mail, this must be via a secure method where the package can be traced and is signed for on receipt.

4.13.4. The internal mail should be avoided when sending highly confidential/Secret information – this should be hand delivered where possible. When transporting PHI by hand, it must be appropriately secured to avoid information being lost or inappropriately visible.

4.13.5. Only companies that hold an existing commercial contract with the Entity (with appropriate information governance clauses in respect of data protection, including NDA, within the contract) can be used to transport PHI, staff

information, equipments, medications or documentation. Any PHI transported in this way should be signed in and out appropriately and copy evidence of sending/receipt retained.

4.13.6. In public areas, incoming mail should be opened away from public view and not left unsupervised.

4.13.7. Where applicable identity check should be verified before handing over the envelope containing PHI to the Data Subject/Patient or authorized person.

4.14. Sharing Protected Health Information through Telephones / Answer Machines / Phone Messages / Verbal Conversations

4.14.1. When sharing PHI over the telephone, staff must not play received answerphone messages on speakerphone in public areas or locations where there is a risk that they could be overheard by unauthorised individuals.

4.14.2. Before releasing, any information to a caller who claims to be the concerned Data Subject/Patient, staff should ensure they gain assurance of the caller's identity by obtaining confirmation of certain personal details (e.g. Date of birth, address, postcode, appointment dates, treatment/clinic details, or medical record number). A Data Subject/Patient may choose to apply an additional safeguard to their EMR by insisting that a password they have set up is provided by any caller before any PHI is released.

4.14.3. If the individual's identity cannot be verified, no information should be released.

4.14.4. Staff must be aware of issues surrounding Data Subject/Patients whose EMR has been marked with an alert showing the need for anonymity protection or additional safeguards. Any caller wanting information on a flagged Data Subject/Patient should be put on hold and immediate advice sought from senior management.

4.14.5. Protected Health Information relating to Entity`s outpatients should only be disclosed to the individuals authorised to receive the information by the Data Subject/Patient (such as next of kin or legal guardian).

4.14.6. For Entity`s inpatients, all calls must be directed to the ward/department where the Data Subject/Patient is located unless there is an alert preventing this. Therefore, it is imperative that any special circumstances regarding an inpatient's conditions are appropriately raised and recorded.

4.14.7. Health data and information should only be disclosed when the consent of the Data Subject/Patient has been obtained or when it is not applicable to attain a consent because of Patient`s condition (e.g. life-threatening emergencies with inadequate time to obtain consent). It is important to note that next of kin do not have any automatic right to access PHI. However, parents/those with parental responsibility have a right to get information about their children health.

4.14.8. As part of the admission process, Patients may be asked in advance whether they wish for information about their care to be shared with any named individual. Information may then be shared with that individual, either in person or over the

phone, without the need to gain further consent. Where a named representative is confirmed, their contact details should be recorded on the Patient's EMR to ensure the Patient's wishes are consistently followed.

4.15. Remote Working (Home, Off-Site, Community etc.)

4.15.1. Staffs are responsible for the confidentiality and security of any data and information (in paper or electronic format) that they hold remotely, and for its transportation to and from Entity premises.

4.15.2. Staff should ensure they hold only the minimum level of PHI remotely, and guarantee compliance with the relevant IT, IS (Information Security) and Information Governance policies.

4.15.3. The devices used in remote work environment should be highly protected on security aspects and it should be ensured that PHI of Data Subjects/Patients is not stored on those devices; to minimize the risk of data breach in case of device loss or theft.

4.15.4. Staff shall not use their personal devices for remote working and always use Entity provided devices to connect remotely for work related purposes.

4.16. Accessing Protected Health Information by Medical/Dental Residents, Health Care Students, Researchers and Clinical Auditors

4.16.1. <u>Medical/Dental Residents</u>

Medical/Dental Residents who are registered in DHA Sheryan system and are included within the healthcare team providing (or supporting) Data Subject/Patient care, can have access to the Data Subject/Patient's PHI like other team members, unless the Data Subject/Patient objects.

4.16.2. Medical/Dental/Nursing/Allied Health Students and Trainees

Students and trainees in areas of health care learning/training under supervision of Sheryan registered health care providers can see Data Subject/Patient`s PHI as read based aspect only with proper supervision.

4.16.3. Researchers and Clinical Auditors

a. The Entity must ensure that systems of authorisation for research projects are in place and that local ethical and audit committees are aware of the responsibilities of clinical staff and researchers in relation to confidentiality and the promotion of good practice.

b. It is advisable to have only unidentifiable data for research or audit unless it is necessary; and this should go through special process of approval and audit.

c. Data shared with external research collaborators or statisticians for clinical trials and research must be anonymised; all direct identifiers must be removed from the dataset and quasi-identifiers modified.

4.17. Using Protected Health Information for Teaching

4.17.1. Protected health information should not be used as a dataset for teaching purposes

without consent from the Data Subject/Patient.

4.17.2. Fictional convincing information is the most appropriate dataset to be used, where no real person can be identified from the information used. Alternatively, anonymised information on Data Subject/Patients and medical conditions can be used for health education and training. Proper control should be in place to make sure the anonymisation is performed properly.

4.17.3. If information or media is used which can, directly or indirectly, identify an individual, then consent must be obtained from the Data Subject/Patient.

4.17.4. Where PHI has the potential to be used for teaching/training purposes in the future, the Data Subject/Patient must be informed at the time of collecting the data and appropriate consent should be obtained.

4.18. Using Protected Health Information for System Testing

4.18.1. The use of PHI for system testing must be avoided by the Entities.

4.18.2. Where there is no practical alternative way to use live data for this purpose, system administration should develop proper security measures to protect PHI from unauthorised access, disclosure of PHI, corruption/loss of data. Health information should be anonymised; any existing identifiable data (name, address, medical record number, phone number, etc.) must be removed and replaced with generic data. The most secure way to approach this is by using automated test data generation tools designed to support high performance for large data sets.

4.18.3. Before commencing any system testing using live data, staff must undertake a Data Protection Impact Assessment (DPIA).

4.19. Sharing Protected Health Information with Private Third Parties within UAE for Processing

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

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

4.19.3. The Entity must ensure the Processor provides "sufficient guarantees" of having the appropriate technical and organisational security measures in place to protect PHI confidentiality.

4.19.4. The Processor must abide with the data and health information protection and confidentiality terms even after the contract expires.

4.19.5. The Entity (as a data and health information controller) 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.

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

4.19.7. Where PHI need to be transported in any media, this process must be carried out to maintain strict security and confidentiality of the information. All portable electronic media must be encrypted.

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

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

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

4.20.1. Protected health information should not be transferred to a country or territory outside the UAE; except for transfer of PHI within the category of Cabinet Decision No. (51) of year 2021 on exemption for storage and transfer of health records and information: Cabinet Decision No. (51) of year 2021

4.20.2. DHA approval must be granted as per DHA Health Information Assets Classification Policy: Health Information Assets Classification

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

4.20.4. 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.

4.20.5. Protected Health Information must be securely encrypted during transit; and the required security measures must be abide to.

4.21. Information/Data Sharing Agreements

4.21.1. All data and information sharing with organizations outside the Entity must be governed by appropriate Data Sharing Agreement (DSA) comprising privacy and security controls; and robust information governance clauses as per DHA`s legislations.

4.21.2. The DSA must comply with the relevant UAE legislations and DHA policies; and should confirm who maintains responsibility and control over the data.

4.21.3. The DSA must set out terms and conditions including details on:

a. All intended/specific purpose(s) for which the health information is being shared.

b. Types/description of data that will be shared, (this may need to be attached as a list of data fields), anonymisation/pseudonymisation arrangements, and frequency of transfers. Information being shared must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are needed to prevent irrelevant or excessive information being disclosed.

c. Attribute on roles of each party; type of authority they will have over the health data and information, and potential recipients /or types of recipient and the circumstances in which they will have access the shared data and information.

d. Description on the retention of shared data and information, and procedures for dealing with cases where variable Entities/organisations may have different retention period.

e. Explanation on disposal/destruction arrangements; including the deletion of shared data and information or its return to the Entity that supplied it originally.

f. Details on privacy and security controls requirements for the Entity receiving the PHI; how health information will be stored and communicated; and and procedures for dealing with any breach of the agreement.

g. Details on timescale for assessing the ongoing effectiveness of the DSA and procedures for dealing with the termination of the DSA, including the deletion of shared data or its return to the Entity that supplied it originally.

h. Attributes on Incident Response Plan for both Entities (controller and processor) that address phases such as preparation, identification, containment, eradication, recovery and lessons learned. The DSA should include information on requirements that the PHI processor must follow and its liability for any incidents associated with loss or unauthorized access to personal data. Sub-processors also will need to comply with the DHA policies based on each contractual relationship established between a processor and sub-processor.

i. Details on Entities/organizations that will be involved in the information sharing along with full contact details for their key members (responsible

persons). If one or more contracts are associated with the DSA, these should also be referenced.

j. Legal basis for sharing the data and information. If consent is required, then how it will be recorded and managed and how Data Subject/Patient will be informed about his/her information sharing.

k. Data Subject/Patients' rights including procedures for dealing with data and information access requests.

l. General information governance arrangements – for example, if one participating Entity/Organization is replaced by another as services are re-procured.

m. Sanctions for failure to comply with the agreement or breaches by individual staff/either parties.

4.21.4. The Entity must review all data sharing agreements on a regular basis ,in order to comply with updates in the UAE laws and legislation, and these updates must be reflected in the agreement to ensure justification for sharing.

4.21.5. Before entering into any data sharing agreement, a Data Protection Impact Assessment (DPIA) should be carried out in order to assess the benefits the information sharing might bring to individuals or society.

4.22. Risk of Re-identification of Data Subjects/Patients

4.22.1. To prevent the risk of re-identification of pseudonymised and anonymised data, the

Entity (as Controller of PHI) must develop best code of practice techniques and process for security and privacy measures.

4.22.2. The possibility of linking several pseudonymised datasets to the same individual can be a precursor to re-identification of Data Subject/Patient. Any concerns regarding re-identification should be discussed with the Entity`s Information Security/Data governance office before any information is shared.

4.23. All Health Entities Must

4.23.1. Develop a Health Data and Information Sharing Policy and procedures to ensure all PHI shared are handled within the information safeguarding principles of the UAE laws and DHA regulations, in a secure and confidential manner.

4.23.2. Policies and procedures should be reviewed at regular intervals (at least once every two years); or whenever there is a change to UAE laws and DHA regulations; to maintain its compliance with recent legislations.

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

4.23.4. All Entities must have in place appropriate measures to investigate and deal with the inappropriate or unauthorised sharing of PHI whether intentional or unintentional:

a. These accidents must be investigated immediately to find the cause.

b. Disciplinary actions must be taken against the person(s) responsible, if appropriate.

c. Appropriate steps must be taken to avoid a repetition.

d. Breach notifications must be reported to both the UAE Information Office and DHA (datacompliance@dha.gov.ae) within 24-48 hours. Details of notification format/content can be found in DHA Policy for Health Data Protection and Confidentiality .

4.23.5. Entity must apply appropriate sanctions against staff, trainees, vendors and third party contractors who violates health data and information sharing policies and procedures.

4.23.6. Entity is responsible for demonstrating its compliance with UAE laws and DHA`s policies and regulations; and will be asked for evidence to demonstrate its fulfilment of the required health information sharing regime to the DHA.

4.23.7. Audit controls are required to keep track of all PHI being shared by the Entity with others; and these logs must be maintained for at least 6 years after the end of DSA.

4.24. Implementation

4.24.1. Entities must train all employees and workforce members (e.g. trainees, vendors, contractors and anyone over whom the Entity exercises direct control) on their

Health Data and Information Sharing Policy, as necessary and appropriate for them to carry out their functions.

4.24.2. No PHI or systems should be handled or used until appropriate training has been completed. All the workforce members are required to undergo security and awareness training before accessing the PHI.

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

4.25. Non-Compliance

4.25.1. All Entities must take into account the provisions of the UAE and Emirate of Dubai legislation, DHA policies and regulations, and any instructions or directives issued by the DHA in this regard. A failure to adhere and comply with legislations and regulations is considered a violation that requires disciplinary action/dismissal in accordance with the provision of the current legislations[2].

4.25.2. Entities must report all violations related to health information sharing to DHA through email: datacompliance@dha.gov.ae within 24-48 hours.

[2]Federal Decree Law No. (4) Of 2016 on Medical Liability. Available on: Federal Decree Law No. (4) Of 2016

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: ICT Health Law

5.2. Resolution No. (2) of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai. Available on: Resolution No. (2) of 2017

5.3. Cabinet Decision No. (32) of 2020 on the Implementing Regulation of UAE Federal Law No. 2/2019 on the Use of Information and Communication Technology in Health Fields. Available on: Cabinet Decision No. (32) of 2020

5.4. UAE Data Protection Law No. (45) of 2021. Available on: UAE Data Protection Law

5.5. Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the UAE. Available on: Federal Ministerial Decision No 51 of 2021

5.6. Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes. Available on: UAE Cybercrime Law

5.7. Ministerial Decision no. (51) of 2021 concerning the health data and information which may be stored or transferred outside the country. Available on: Ministerial Decision no. (51) of 2021

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: Federal Law No. (5) Of year 2012

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

5.11. Federal Decree Law No. (4) Of 2016 on Medical Liability. Available on: Federal Decree Law No. (4) Of 2016

5.12. Executive Council Resolution No. (32) of 2012 on Regulating the Entity of health professions in the Emirate of Dubai. Available on: Executive Council Resolution No. (32) of 2012

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: Law No. (13) of 2021

5.14. Dubai Health Authority Policy for Use of Artificial Intelligence in the Healthcare in the Emirate of Dubai. Available on: Use of Artificial Intelligence in the Healthcare

5.15. Dubai Health Authority Policy for Health Information assets classification. Available on : Policy for Health Information assets classification

5.16. Dubai Health Authority Policy for Health Data Protection and Confidentiality. Available on: Policy for Health Data Protection and Confidentiality

5.17. Dubai Health Authority Policy for Health Data Quality. Available on: Policy for Health Data Quality

5.18. Dubai Health Authority Policy for Health Information Assets Management. Available on: Health Information Assets Management Policy

5.19. Dubai Health Authority Code of Ethics and Professional Conduct (2014). Available on: DHA Code of Ethics

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

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

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

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

5.24. DHA guideline for Patient consent. Available on: DHA Patient Consent

5.25. NHS Data Protection, Access to Information and Information Sharing Policy. Available on: NHS Information Sharing Policy

5.26. Naomi Waithira, Brian Mutinda and Phaik Yeong Cheah. Data management and sharing policy: the first step towards promoting data sharing. BMC Med. 2019 Apr 17;17(1):80.