Standards for Health Information Consent and Access Control

Version (1)

Issue date: 02/01/2025

Effective date: 02/04/2025

Health Informatics and Smart Health Department

Dubai Health Authority (2025)

ACKNOWLEDGMENT

The Health Informatics and Smart Health Department (HISHD) developed this Standard in collaboration with subject matter experts and would like to acknowledge and thank these health professionals for their dedication toward improving quality and safety of healthcare services in the Emirate of Dubai.

Dubai Health Authority

TABLE OF CONTENTS

INTRODUCTION

Dubai Health Authority (DHA) is mandated by Local Law No. (14) Of 2021 on amending the local Law No. (6) of 2018 concerning the Dubai Health Authority , to undertake several functions including but not limited to:

- Developing regulation, policy, standards, guidelines to improve quality and Data Subject/Patient safety and promote the growth and development of the health sector.
- Licensure and inspection of Healthcare Facilities as well as Health professionals and ensuring compliance to best Facility.
- Governing of health information, e-health and promoting innovation.

The "Standards for Health Information Consent and Access Control" aims to fulfil the following overarching Dubai Health Sector Strategy 2026:

- Pioneering Human-centered health system to promote trust, safety, quality and care for Patients and their families.
- Become a global digital health hub.

EXECUTIVE SUMMARY

The purpose of this document is to set out Dubai Health Authority (DHA)`s requirements for access to Protected/Personal Health Information (PHI) through Health Information Systems (HIS) in the Emirate of Dubai; in line with the United Arab Emirates (UAE) laws, Emirate of Dubai legislations, and DHA regulatory frameworks.. The Standard has been developed to align with the evolving health information necessities and international best practices. This document should be read in conjunction with other Health Information Governance regulations released by DHA:

- Policy for Health Information Assets Management
- Policy for Health Information Sharing
- Health Data Quality Policy
- Health Data Classification Policy
- Policy for Health Data Protection and Confidentiality
- Incident Management and Breach Notification policy
- Subject of Care Rights
- Consent and Access Control
- Incident Management and Breach Notification Policy
- Data Management and Quality Policy (Primary and Secondary Use)
- Health Information Audit Policy
- Identity Management Policy

- Authentication and Authorization Policy
- Information Security Standards
- Interoperability and Data Exchange Standards
- Technical and Operational Standards
- Artificial Intelligence Policy

DEFINITIONS

Access control: Is the practice of managing and regulating who can access specific resources, systems, or data within an organization's network or information technology environment.

Access privileges: Refer to the level of access granted to a user to perform his/her job duties.

Audit Log (Trails): A security-relevant sequential record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Authentication: The process of reliable security identification of subjects by incorporating an identifier and its authenticator.

Authorization: The granting of rights, which includes the granting of access based on access rights.

Breach: Any unauthorized access, disclosure, acquisition or use of Subject of care Data, whether by willful misconduct or otherwise or any breach of DHA Policies. A Breach is a Reportable Event that, once investigated, is confirmed to have compromise the security or privacy of the Personal Health Information (PHI).

Break The Glass: Allows health professionals to gain access to protected health information (PHI) in the health information system (HIS), without the Patient's consent, when necessary to lessen or prevent a serious threat to a Patient's health such as emergency situations.

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

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

Data: 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 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 organization/ individual.

Electronic Medical Record (also known as Electronic Health Record): 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.

Entity: Entity in Dubai that is involved in the direct delivery of healthcare and/or supportive healthcare services, or in the financing of health such as health insurer and health insurance facilitator, healthcare claims management Entity, payer, third party administrator, hospital,

medical clinic, medical center, telemedicine provider, laboratory and diagnostic center, and pharmacy, etc.

External/Third Party: An individual or organization that deals with the Entity through a business relationship and has access to Entity`s health information as per contractual terms and conditions.

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

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

Health Information System (HIS): Systems that collect, store, and process Protected Health Information (PHI) regardless of the owner of the system; for example: Electronic Medical Record (EMR), Health Information Exchange (Nabidh), Claims Management system, Public health portals, Practice Management Software, Patient Portals, Remote Patient Monitoring (RPM) Also known as telehealth, Laboratory Information System (LIS).

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: Refers to the Data Subject/Patient who either lack the full legal capacity or have the full capacity, but unable to provide a Consent.

Information security: The act of protecting information that may exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity and minimizing business risk.

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

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

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

Privilege Access: Refers to the access which is over and above the normal access required by user for carrying out day to day activities. High privilege access can be Remote Access, usage of super admin, getting access to restricted portals etc.

Protected Health Information (PHI): 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:

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

- Any other unique identifying number, characteristic, or code.

Processing: Any operation or set of operations which is performed upon Subject of care Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use or disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and processed, processes and process should be construed accordingly.

Remote Access: The ability to connect to and access the organization Infrastructure from a remote location using the virtual private network (VPN) of the organization.

Risk: The quantifiable likelihood of potential harm that may arise from a future event.

Secondary Use: Is 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 Personal Information: There are also 'special categories' of personal information which require greater protection and justification for usage and sharing. This data is similar to 'Personal Sensitive Information' 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.

Users: All employees, contractors, consultants, suppliers, external parties, partners, and customers of the Entity using and accessing Entity`s data and information systems.

Virtual Private Networks (VPNs): The technology that enables users to connect to organization private network securely and encrypted over a public network such as the Internet.

ABBREVIATIONS

BTG	:	Break the Glass
DHA	:	Dubai Health Authority
EMR	:	Electronic Medical Record
HIS	:	Health Information System
HR	:	Human Resource
ICT	:	Information and Communications Technology
IG	:	Information Governance
IP	:	Internet Protocol
IT	:	Information Technology
LIS	:	Laboratory Information System
PHI	:	Protected/Personal Health Information
UAE	:	The United Arab Emirates.
VPN	:	Virtual Private Networks

1. BACKGROUND

Dubai Health Authority (DHA) is mandated by Local Law (6) of 2018 Concerning Dubai Health Authority and Local Law No. (14) Of 2021 on amending the local Law No. (6) of 2018 concerning the Dubai Health Authority to undertake several functions including, but not limited to Developing regulation, policy, standards, guidelines to improve and promote the growth and development of the health sector in the Emirate of Dubai.

The "Standard for Health Information Consent and Access Control" aims to fulfil the requirements for accessing PHI as per UAE laws and DHA regulations; in order to position Dubai as a global medical destination by introducing a value-based, comprehensive, integrated and high-quality service delivery system.

2. SCOPE

2.1. All PHI within the Emirate of Dubai accessed by Entities under jurisdiction of DHA.

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

3. PURPOSE

3.1. To set out Dubai Health Authority (DHA)`s requirements for access to PHI through Health Information Systems (HIS) in the Emirate of Dubai; in line with the United Arab Emirates (UAE) laws, Emirate of Dubai legislations, and DHA regulatory frameworks.

3.2. To ensure Entities under jurisdiction of DHA are providing a secure access to PHI.

3.3. To guarantee that Data Subject/Patient can permit or withhold the use and disclosure of PHI through HIS with full autonomy and as per UAE law.

4. APPLICABILITY

4.1. All PHI within the Emirate of Dubai accessed by Entities under jurisdiction of DHA.

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

5. **STANDARD ONE:** CONSENT AND ACCESS CONTROL

5.1. The "Health Information Consent and Access Control Policy" is an integral part of the DHA's approach to Health Information Governance (IG) in the Emirate of Dubai. This policy must be read in conjunction with other related DHA IG Policies.

5.2. All related UAE laws, Emirate of Dubai legislations, and DHA regulations on health IG are considered in this policy.

5.3. All Entities must be able to demonstrate the lawful basis upon which they are accessing PHI via HIS through obtaining consent of the Data Subject/Patient when mandated by UAE law or DHA regulations.

5.4. Access Control is required in order to comply with the UAE laws and DHA regulations and to safeguard the confidentiality, integrity and availability of sensitive and confidential health information.

5.5. All Entities should implement a zero-trust mechanism to ensure that access is not inherently trusted for any user or device. This involves continuously verifying access based on multiple factors, including device health, user context, and the sensitivity of the requested resources, while also enforcing the principle of least privilege.

5.6. All staff with authorised access to PHI, have a duty to keep it confidential, secure and in line with the standards and procedures set out in this and other related DHA policies; in accordance with professional standards and Data Protection legislation.

5.7. Access to Data Subject/Patient's PHI is permitted where there is legitimate clinical, administrative, managerial or reporting reasons.

5.8. Staff must only access a Patients HIS using their own access details

5.9. Entity must train all employees and workforce members (e.g. trainees, vendors, contractors and anyone over whom the Entity exercises direct control) on appropriate HIS access, the terms in the User and Confidentiality Agreement, and it`s health

information consent and access control policy, as necessary and appropriate for them to carry out their functions.

5.10. Entity must maintain a register of employees and workforce members training, and should provide evidence of training upon request.

5.11. No HIS should be accessed until appropriate security and awareness training has been completed.

5.12. The Entity should review the training and awareness courses periodically to reflect current UAE laws and DHA regulations, including health information governance regulatory requirements DHA IG Policies .

6. STANDARD TWO: ACCESSING ELECTRONIC MEDICAL RECORD FOR DATA SUBJECT/PATIENT CARE

6.1. Consent is not required when recording and accessing Data Subject/Patients PHI within Electronic Medical Record (EMR).

6.2. All relevant PHI should be accessed and shared as per necessities of direct care to Data Subject/Patients.

7. **STANDARD THREE:** ACCESSING ELECTRONIC MEDICAL RECORDS FOR SECONDARY USE

7.1. When accessing PHI for purposes other than individual care (such as strategic planning, research, audit, etc.) Entity must always consider whether identifiable Patient information is actually needed.

7.2. If it is not practicable to work with anonymous data, then consent is normally required to access PHI for purposes beyond individual care.

8. **STANDARD FOUR:** CONSENT FOR ACCESSING PHI THROUGH HEALTH INFORMATION SYSTEMS

8.1. Accessing PHI without Data Subject/Patient consent through HIS is allowed in some special cases as per UAE Federal Law No. (2) For the year 2019 On the Use of Information and Communications Technology (ICT) in Healthcare and DHA Health Data Protection and Confidentiality Policy and DHA Policy for Health Information Sharing :

8.1.1. Entering data into Electronic Medical Records (EMR) and Laboratory Information System (LIS).

8.1.2. Data or 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 or verifying the financial benefits related to those services.

8.1.3. For 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.

8.2. Consent is required for accessing PHI through other HIS.

8.3. Entities must initiate registration process of the Data Subject/Patient on current and any future platforms; and record the consent (refusal/withdrawal/re-opt in) with dates.

8.4. Entities must obtain consent from Data Subject/Patient in paper or electronic format.

8.5. If the Entity chooses to use electronic signatures for healthcare transactions, then it must comply with the Dubai electronic signature standard. The UAE electronic signatures is governed by the Federal Decree-Law No. 46 of year 2021 on Electronic Transactions and Trust Services UAE_Electronic-Transactions-and-trust-services-law.

8.6. Consent should be specific, freely given, informed and unambiguous; using clear and plain language that is understood by the Data Subject/Patient.

8.7. Consent should be given in writing either in Arabic or in English.

8.8. The language of the consent should be understandable to the Data Subject/Patient.

8.9. Translation should be provided if necessary. This means that the Data Subject/Patient needs to be told what information is to be collected, accessed, processed, shared, stored, transferred or exchanged; and to whom the PHI will be disclosed and why (for what reason).

8.10. Entities must inform Data Subject/Patient appropriately that accessing relevant PHI with HIS can have a beneficial part on their care/treatment.

8.11. The Data Subject/Patient must have sufficient understanding of the implications of giving consent.

8.12. Entities must capture all mandatory demographics information required to support consent management process to Data Subject/Patient (Emirates ID, home address, mobile number, etc.); and categorize Data Subject/Patient if they are Tourists as per Policy for Health Data Quality .

8.13. The age of consent is 18 years old and above.

8.14. Where information relates to a minor (e.g. child/young person less than 18 years of age); and consent is required for lawful accessing/sharing, this must be obtained from a person with parental responsibility or other legal guardianship for the minor. This authority must be verified and documented with the consent.

8.15. Where the information relates to an incompetent Data Subject/Patient or the Patient is unable to give the consent (e.g. unconscious), and consent is required for lawful accessing/sharing, this must be obtained from the next of kin (e.g. relatives up to the

forth degree) or a person with legal guardianship. This authority must be verified and documented with the consent.

8.16. Consent for accessing HIS remains valid for one year after last health Encounter with the Data Subject/Patient, unless the Patient revokes their consent.

8.17. Consent is not required for uploading health information to the NABIDH by Healthcare Facilities.

8.18. Entities must include a clause within their general consent on sharing PHI with Nabidh (Nabidh HIE Access Consent) as per DHA mandates.

9. **STANDARD FIVE:** OPTING OUT OF HEALTH INFORMATION SYSTEMS

9.1. All Data Subject/Patient should be given the opportunity to object the sharing of the PHI through HIS if the UAE law and DHA regulations allow.

9.2. This right is not valid for sharing PHI in EMR, public health portals, and insurance systems as per UAE Federal Law No. (2) For the year 2019 On the Use of Information and Communications Technology (ICT) in Healthcare and DHA Health Data Protection and Confidentiality Policy.

9.3. The Entity should explain to the Data Subject/Patient the potential consequences of not sharing information through HIS. If, after a discussion, the Patient continues to object; Data Subject/Patient must be given the right to withdraw and opt-out.

9.4. The withdrawal of consent should not affect any sharing carried out under consent before its withdrawal. Any Entity that has accessed or received health information via

the HIS prior to such revocation and incorporated such PHI into its records may retain such information in its records.

9.5. In case the Data Subject/Patient has opted out of HIS then:

9.6. Personal Health Information should continue to be received by HIS from the Entity; however, Data Subject/Patient identifiers must be anonymised as per The UAE Federal Law No. (45) of 2021 Regarding Data Protection and Policy for Health Data Protection and Confidentiality.

9.7. Personal Health Information should not be retrieved using BTG access.

9.8. Entities must archive the opting out consents, and it should be provided to HIS management on request.

9.9. Nabidh opt out is managed by DHA through below process:

9.9.1. Entity provides the Data Subject/Patient a copy of the Nabidh opting out consent along with associated DHA email: Nabidh.optout@dha.gov.ae .

9.9.2. The Data Subject/Patient sings the consent and send it to DHA Nabidh team.

9.9.3. DHA Nabidh team will opt out the Data Subject/Patient from Nabidh as per request.

10. **STANDARD SIX:** GRANTING ACCESS TO HEALTH INFORMATION SYSTEMS

10.1. To the extent, technologically feasible users should be granted access only to health information required to perform their appropriate functions at the Entity.

10.2. Access must be restricted to specific functions within some applications; and whenever the software allows, access should be as granular as feasible.

10.3. Each user in the Entity should sign a "User and Confidentiality Access Agreement" before accessing PHI through HIS.

10.4. Entity must issue passwords and Unique User Identification ("ID") for accessing Entity's HIS once the "User and Confidentiality Access Agreement" is completed and submitted. Such passwords and IDs should not be shared with any other individuals or Entities.

10.5. In configuring access, all Entities must follow the concept of "need to know" and 'least privilege': Access should be granted on need-to-know basis and least privileges. Every HIS and every user of the system should operate using the least set of privileges necessary to complete their job. This principle limits the damage that can result from data breach.

10.6. Entity must determine the specific functions and responsibilities for which the individual needs access for each application. The sensitive nature of many restricted functions, and their potential for abuse and error, should be considered when making this determination.

10.7. Entities must ensure that users are associated with at least one standard healthcare role:

10.8. Update (read/write) access: the ability to enter and update data and submit transactions.

10.9. Lookup (read-only) access: the ability to only view health information without being able to enter or change data.

10.10. User access provisioning should be initiated in the following cases, but not limited to:

10.10.1. New employment

10.10.2. Users being promoted /demoted /transferred

10.10.3. Temporary assignment of job responsibilities

10.10.4. Access to external Users (such as vendors, contractors and partners) and external parties, etc.

10.11. For healthcare professionals, the role should be defined by the code associated with the license in Sheryan ID as maintained by DHA.

10.12. For employees who do not have Sheryan ID, the role should reflect one of the standard roles identified by HIS as determined by the Entity.

10.13. For Remote access to HIS, it is recommended to have additional authentication mechanisms, such as two-factor or hardware-backed certificates, to be deployed to individually authenticate and authorise all remote access to all networks and information systems that support staff`s essential service.

10.14. Access to HIS should be granted with approval from the User's Director/Manager and approval from the system owner.

10.15. Access to restricted applications, functions, and/or data sets should always be limited to those that are required for the performance of an individual's current duties.

10.16. Whenever the individual's duties at the Entity change, the individual's access should also be changed to reflect this.

10.17. Authorization for access HIS should be reviewed and validated regularly (at least every year along with the staff reappointment process).

11. **STANDARD SEVEN:** ACCESS CONTROL MANAGEMENT RESPONSIBILITIES

11.1. The Entity is responsible for access control management. The privileged accounts on all of Entity's systems, applications, and servers should be managed by a common access management system.

11.2. The System Owner or designee(s) will serve as:

11.2.1. Access Granting Authority – the person(s) having managerial authority to approve requests for access rights to the HIS.

11.2.2. Access Control Administration – the person(s) or group (e.g., access control group) responsible for creating, modifying, and terminating a user's ability to access the HIS based on direction from the Access Granting Authority.

11.3. If the individual no longer needs any access (for instance, upon termination of employment), all access should be revoked.

11.4. Attempts by unauthorised users to connect to HIS should be alerted, promptly assessed and investigated where relevant.

11.5. Entities must enforce access control, including verification of consent status, at the time of use/disclosure of PHI by healthcare professionals.

11.6. Entities must ensure that the individuals accessing PHI are responsible for protecting the information or preventing unauthorized access/usage of PHI as mentioned in Policy for Health Data Protection & Confidentiality.

11.7. Entities must ensure access to PHI through HIS is permitted, provided that HIS user is abiding to all Entity`s policies and agreements.

11.8. Entities must ensure all required/relevant information shared with HIS, except where UAE laws or DHA policies prohibit it.

11.9. There should be strong access control measures for protecting confidential and sensitive information accessed by third-party vendors. This ensures that vendors comply with the same stringent security standards as internal users.

12. STANDARD EIGHT: ACCESS RELATED TO EXTERNAL PARTY (VENDORS/CONSULTANTS)

12.1. All contracts with external parties (such as vendors, contractors and partners) should include security requirements and clauses outlining the access requirements to HIS.

12.2. The respective department and Entity`s Information Security Office should review and agree on any special requirements related to providing access to external party and ensure including such requirements in the contracts/agreements.

12.3. The information security office can reserve the right to require additional access controls to be applied in relation to any contract.

12.4. Business unites should maintain records of external party access privileges and should make sure that their access is monitored.

12.5. Entity must revoke all external party accesses by end of the contract/agreement.

13. STANDARD NINE: USERS ACCESS RIGHTS MODIFICATION OR TERMINATION

13.1. The access rights to HIS for all users should be removed upon termination of their employment, contract / agreement, or adjusted upon change.

13.2. Managers or supervisors should promptly notify the appropriate Access Granting Authority whenever a user of a HIS:

13.2.1. Ceases to require access to the HIS (e.g., terminates employment, transfers to another department).

13.2.2. Requires modified access rights to perform required functions (e.g., changes roles within a department).

13.3. Logs or other documentation of all access request approvals, user account creations, modifications, and deletions must be maintained by the Access Control Administration for a minimum of six years.

13.4. Entities must ensure that they immediately suspend or deactivate individual user accounts in cases where:

13.4.1. User leaves the Entity.

13.4.2. User has a change of duties so that they no longer require access to the HIS.

13.4.3. User is found to have violated any policy or misused the provided access in any means.

13.4.4. User has the security of their account compromised.

13.4.5. Requested by the Director/Manager of the concerned department.

13.4.6. External Users (such as vendors, contractors, partners and external parties, etc.) completed their engagement/project.

13.5. The user director and system owners are responsible of initiating and approving any modification of user's access.

13.6. The Human Resource (HR) Department should be responsible of initiating the de-provisioning of user access for the resigned or terminated user, in coordination with the respective manager of the user.

13.7. The Human Resourse department should notify the IT department within three business days and one week before last working day of the staff who has access to Entity's HIS, so that the IT department discontinue such access.

13.8. The HR department, in coordination with the IT department, must ensure that user access is cancelled on the employee's last day.

13.9. The Department Director must verify and sign the termination of access for the user who has resigned or whose services have been terminated.

13.10. When user moves between sections or departments in the Entity or there is a change in the user's job itself in terms of promotion, the application for modifying user access should also be approved by the Department Director.

13.11. Temporary access for external parties should be granted upon approval from Entity`s director. Temporary access privileges or uses should be set with an end date and must be automatically revoked upon completion of the task.

13.12. Information Technology Department is responsible of ensuring that any temporary access granted is revoked on completion of temporary period.

14. STANDARD TEN: REMOTE ACCESS TO HEALTH INFORMATION SYSTEM

14.1. Remote access usage for Entity's employees is restricted to geographical boundaries of the UAE.

14.2. Non-Entity employees should be granted remote access with proper business justification/agreement and Director approval for accessing Entity`s system.

14.3. Granting remote access to external parties should be based on an approved list of users, their locations/countries from which they are connecting and for a time period required for the activity.

14.4. Remote Access should be strictly controlled by IT Department and monitored by Information Security Office.

14.5. Strong authentication mechanism with two factor authentications should be configured by IT department for all Remote Access while accessing HIS through VPN.

14.6. The Entity should ensure that users have Remote Access to minimum and only necessary HIS.

14.7. All activities carried out using remote access should be logged and monitored by Information Security Office.

14.8. Remote access logs should be maintained for a period of one year.

14.9. The Entity should make sure adequate security controls are implemented on the VPN client laptop/PC, such as authentication, encryption, anti-virus software, personal firewalls, session timeout, content filtering etc.

14.10. Users should be granted remote access with proper business justification falling under any criteria as mentioned below:

14.10.1. Users who have compelling urgency to complete tasks/projects.

14.10.2. Users working on tasks/projects, which requires remote connection after working hours.

14.10.3. Users who need remote access for day-to-day operations.

14.10.4. Users who need remote access for trouble shooting.

14.11. Users of remote access should be provided with an end date to the access. Users requiring access beyond the specified end date should renew their access.

14.12. All remote access should be reviewed in regularly (at least every 6 months).

14.13. Remote Access de-provisioning is valid under the following circumstances:

14.13.1. Users no longer require remote access to the requested Entity systems/applications or when the temporary access permission granted to the User expires and no renewal have been requested.

14.13.2. End of employee's service.

14.13.3. If requested by the Director of the concerned department to which the user belongs.

14.13.4. If user found to have violated the policy or misused the provided service in any mean.

14.14. Remote access provided to external party should be revoked once the approved reason/period of access is over.

15. STANDARD ELEVEN: REMOTE ACCESS USAGE CONTROLS

15.1. Users should refrain from sharing or disclosing remote access credentials with any individuals.

15.2. Users should be held responsible for any misuse of login credentials.

15.3. Devices connect remotely to Entity network should have the Entity`s minimum security requirements enabled.

15.4. All activities carried out using remote access must be logged and monitored.

16. STANDARD TWELVE: MONITORING ACCESS TO HEALTH INFORMATION

16.1. All accesses to HIS should be logged and monitored.

16.2. The Entity should develop and distribute an access control procedure that provides implementation details for users registration, de-registration, and users access privileges modification, disabling or removal, etc.

16.3. Access to Entity`s information services should be controlled through a formal user registration process and should be approved by the respective line manager of the user.

16.4. The HIS owners should generate users list from on regular basis (at least every 6 months) to identify redundant, dormant, expired user accounts or incorrect privileges.

16.5. User accounts that are inactive for a period of 40 days should be disabled on a regular basis. The account lock should be set on the Active Directory level for AD integrated systems/applications.

16.6. All privileged and administrators accounts should be reviewed on a quarterly basis (at least once in 3 months), and changes to such accounts should be logged for periodic review.

16.7. Users should report any violations or suspicious activities found in the access, as per the Entity`s Information Security Incident Management Procedures.

16.8. The reviews of access should include both Entity`s and external users and should cover but not limited to: Shared Folders, Servers, Applications, Databases, Network devices, Physical access to secure areas, remote access (VPN), removable devices, etc.

16.9. Entity should implement session time-out controls to prevent unauthorized access.

16.10. Processes should be implemented to monitor all HIS access and use. This includes regular audits of user access to ensure that access is pertinent to the user`s role and use of the system and related information is in line with the conditions under which access was granted.

16.11. The Account Management standard operating procedure (SOP) must be completed for each HIS and reviewed regularly (at least annually).

16.12. All consents must be archived along with medical records as per DHA regulations.

16.13. Accessing to consent and sharing them with Data Subjects/Patients and/or DHA inspectors (for auditing purposes) should be obtainable.

17. STANDARD THIRTEEN: BREAK THE GLASS ACCESS

17.1. Only physicians who provide direct care to the Data Subject/Patient must be allowed to access to HIS through Break the Glass (BTG).

17.2. The disclosure of PHI via BTG must be granted when:

17.2.1. Treating a Data Subject/Patient with an emergency condition to lessen or prevent a serious threat to the individual's life, health or safety.

17.2.2. Access to the PHI is necessary to lessen or prevent a serious threat to public health or safety (for example, to identify the source of a serious infection and prevent its spread).

17.3. The HIS should involve alerting and control mechanisms, such as a pop-up screen, warning the data about to be accessed is sensitive and restricted.

17.4. The healthcare provider should justify the circumstances that led to the use of the BTG on a case-by-case basis.

17.5. Health information systems must have a BTG procedure that allows physicians who do not have access privileges to certain information to gain access in an emergency situation.

17.6. The reason for initiating BTG access and a detailed audit trail must be documented whenever this procedure is invoked.

17.7. The BTG access should:

17.7.1. Trigger notification.

17.7.2. Be strictly monitored.

17.7.3. Logged to prevent misuse.

17.7.4. Be reviewed regularly for any unauthorized access.

17.8. A consent is not required for accessing HIS to disclose PHI to a healthcare provider through BTG; if the Healthcare provider determines in his/her reasonable judgment that the PHI, which may be available through the HIS, is essential for emergency evaluation/treatment of Data Subject/Patient. Nevertheless, the Entity should ensure that BTG disclosures of PHI via the HIS do not occur after completion of the emergency situation.

18. STANDARD FOURTEEN: ACCESSING SENSITIVE HEALTH INFORMATION

18.1. Sensitive Health Information are described in details in Health Data Classification Policy.

18.2. Entities must assure HIS providing access to PHI enforce protections associated with content marked as sensitive data as per Health Data Classification Policy

18.3. Sensitive Health Information require special protection above that of generic Health Information.

18.4. Sensitive Health Information should be flagged within HIS through special Icons/flag.

18.5. For non-digital assets, a clear RED color tag should be inserted for labelling Sensitive Health Information.

18.6. Access to Sensitive Health Information should be restricted to healthcare professionals as identified by their role.

18.7. Sensitive Health Information may be accessed with a BTG option for defined roles of health professionals as identified by EMR or HIS system administrators.

19. STANDARD FIFTEEN: ACCESSING VERY IMPORTANT PERSON (VIP) HEALTH INFORMATION

19.1. The VIP criteria is defined in details in Health Information Assets Classification.

19.2. The VIP Health Information require special protection above that of generic Health Information.

19.3. The VIP Health Information should be flagged within EMR through special Icons/flag.

19.4. For non-digital assets, a clear RED color tag should be inserted for labelling VIP Health Information.

19.5. The VIP health information should be considered as "SECRET" and the access should be limited to the healthcare professionals who are providing care only.

19.6. Necessary measures should be taken to avoid any unauthorized access to VIP health information.

19.7. Entities must implement necessary internal policies and procedures to prohibit accessing VIP Health information except in accordance with the requirements of DHA.

19.8. The VIP Health Information may be accessed with a BTG option for defined roles of health professionals who are involved in direct care of the Patient.

19.9. The VIP health record should not be shared with HIS.

20. STANDARD SIXTEEN: AUDIT AND MONITORING

15.1. A failure to adhere to this standard is considered a violation that requires investigation. Disciplinary action/dismissal will be taken in accordance with the provision of the current UAE laws and DHA legislations.

REFERENCES

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
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
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
4. UAE Data Protection Law. Available on: UAE Data Protection Law
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
6. Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes. Available on: UAE Cybercrime Law
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

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
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
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 .
11. Federal Decree Law No. (4) Of 2016 on Medical Liability. Available on: Federal Decree Law No. (4) Of 2016
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
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
14. Dubai Health Authority Nabidh policies and standards. Available on: Nabidh policies and standards
15. 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

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

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

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

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

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

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

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

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

24. Joint Commission International Accreditation Standards for Hospital, 7th Edition, (2021). Available on: JCIA Standards for Hospital

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

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

27. Lebkicher, Michael. "Role Based Access". SANS Institute, November 30, 2000. Available on: http://www.sans.org/infosecFAQ/securitybasics/RBAC.htm

28. Smith, Harry. "A Context-Based Access Control Model for HIPAA Privacy and Security Compliance". SANS Institute, July 18, 2001. Available on: http://www.sans.org/infosecFAQ/legal/control_model.htm

29. Government of western Australia, Emergency access to a My Health Record. Available on: https://www.health.wa.gov.au/~/media/Files/Corporate/general-documents/My-health-record/Emergency-Break-Glass-Procedure.pdf

30. HIPAA Security: Information Access Controls Policy. Available on: https://uit.stanford.edu/security/hipaa/info-access-policy