HR 1	Human Resources Security Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
HR 1.1	The healthcare entity shall develop, enforce and maintain a human resources security policy covering the security aspects of employment and termination The policy shall: 1. Define management requirements on; a. Background verification for employees and contractors b. Roles and responsibilities c. Compliance with acceptable usage and other organizational security policies d. Training and awareness needs e. Return of assets during exit 2. Mandate the requirements of non-disclosure and confidentiality during and after employment 3. Include reference to organizational disciplinary process	**Basic**

UAE IA Reference: M3.1.1, M4.1.1

HR 2	Prior to Employment

Control Demands		Control Criteria Basic/Transitional/Advanced
HR 2.1	The healthcare entity shall conduct background verification checks on all candidates for employment, contractors and third-party users The healthcare entity shall: 1. Define background verification process addressing provisions of government mandates and entity demands 2. Establish criteria for background verification checks based on: a. Role of the individual b. Classification of information access needed c. Access to critical areas d. Risk identified	**Basic**
HR 2.2	The healthcare entity shall establish specific terms and condition of employment The terms and condition shall: 1. Include control requirement specific to employees, contractors and third parties, relevant to their roles and risk profiles 2. Include information security responsibilities of the healthcare entity and of the employees, contractors and third parties 3. Include standard information security requirements 4. Be read, understood, agreed and signed by employees, contractors and third parties The healthcare entity shall: 5. Conduct mandatory briefing sessions to employees, contractors and third parties on standard and specific information security requirements of the terms and condition 6. Maintain adequate records on employee, contractor and third party briefing 7. Maintain terms and conditions signed by employee, contractor and third-party resources in-line with entity retention requirements	**Basic**

UAE IA Reference: M4.2.1, M4.2.2

HR 3	During Employment

Control Demands		Control Criteria Basic/Transitional/Advanced
HR 3.1	The healthcare entity management shall ensure employees, contractors and third party users adopt and apply security in accordance with established entity policies and procedures The healthcare entity shall: 1. Ensure employees, contractors and third party users are briefed on the entity's information security compliance requirements 2. Establish acceptable usage policy and ensure users read, accept and sign the policy prior to the provision of system, application or information access 3. Consider segregation of duties to avoid potential misuse of position or conflict of interest	**Basic**
HR 3.2	The healthcare entity shall develop new or modify existing awareness and training programs to include requirements of governmental and organizational information security demands The healthcare entity shall: 1. Ensure all employees and where relevant contractors and third parties receive appropriate awareness and training to enhance the entity's security posture and to minimize probabilities of information security risks 2. Ensure that an awareness and training program is formally launched and professionally managed 3. Enhance training contents and enrich delivery of awareness aspects based on evolving needs 4. Evaluate effectiveness and maintain appropriate record of awareness and trainings delivered	**Transitional**
HR 3.3	The healthcare entity shall identify and address skill and competency demands and gaps The healthcare entity shall: 1. Assess and identify skill and competency gaps on information security demands 2. Implement skill and competency development programs	**Basic**

HR 3.4	The healthcare entity shall conduct periodic security awareness campaigns, based on established yearly schedules The healthcare entity shall: 1. Conduct awareness campaign for general and targeted user groups 2. Identify innovative methods and medium to communicate security requirements 3. Include incentive programs for user participation and adherence to security practices The awareness campaign shall: 4. Present current risks around the work and industry, and ways to address 5. Present learning from incident 6. Demonstrates the need to protect healthcare information 7. Include benefit of information security compliance 8. Demonstrate stakeholder responsibilities 9. Highlight entity, government and regulatory demands	**Basic**
HR 3.5	The healthcare entity shall establish and enforce a disciplinary process for employees, where relevant contractors and third parties, who have committed security breaches The healthcare entity shall: 1. Ensure employees, contractors and third party resources are aware of the entity's disciplinary processes 2. Enforce disciplinary processes and maintain necessary records on the breaches and on management's actions	**Transitional**

UAE IA Reference: M3.2.1, M3.3.1, M3.3.2, M3.3.3, M3.3.4, M3.3.5, M3.4.1, , M4.3.1, M4.3.2

HR 4	Termination or Change of Employment and Role

Control Demands		Control Criteria Basic/Transitional/Advanced
HR 4.1	The healthcare entity shall define responsibilities concerning information security for performing employment termination or change of employment The healthcare entity shall: 1. Establish internal and external communication protocol on employment exit 2. Ensure adequate knowledge transfers and responsibility handovers	**Basic**
HR 4.2	The healthcare entity shall ensure recovery of all organizational assets upon termination of employment, contract or agreement The healthcare entity shall: 1. Ensure all organizational assets are recovered and necessary acknowledgement and clearance obtained from appropriate stakeholders 2. Ensure all information, with special focus on healthcare information, has been recovered and cannot be misused anywhere, anytime 3. Ensure resources leaving the entity formally acknowledges and conforms that no information is under their direct or indirect possession or use	**Basic**
HR 4.3	The healthcare entity shall remove access rights and revoke privileges of individuals upon termination of employment, contract or agreement The healthcare entity shall remove access to systems, applications, information, secure areas, and work areas. The healthcare entity shall: 1. Ensure access to systems, application, information, secure areas, work areas and identified critical areas are revoked upon termination 2. Communicate with health sector regulator or Abu Dhabi government to revoke any relevant system and application access upon termination	**Basic**
HR 4.4	The healthcare entity shall develop internal process to manage internal transfers and change of role The healthcare entity shall: 1. Ensure communication to all necessary internal and external stake holders on change of role or internal transfers 2. Revoke access and privileges associated with old role and reassign privileges on system, application and information access and utilization consistent with their new role based on necessary authorization	**Basic**

UAE IA Reference: M4.4.1, M4.4.2, M4.4.3

2. Asset Management

Asset Management is an essential part of effective healthcare Information Security management. Healthcare entities are witnessing an influx of new asset classes that are very different from the ones they used to deal with. Innovative care delivery mandates that healthcare entities and professionals deal with a large number of relatively small, mobile and sophisticated pieces of equipment/devices, and to keep them running at all times as they are often critical to the patient's health, safety and wellbeing. In order to be effective and supportive of organizational business and security objectives, healthcare entities shall maintain an updated version of asset inventory, available to relevant management, business and support stakeholders.

Information assets includes information/data in all its form, as well as the underlying application, technology, and physical infrastructure to support its processing, storing, communicating and sharing. The following are considered information assets:

- Information (in physical and digital forms)
- Medical device and equipment
- Applications and Software
- Information System
- Physical Infrastructure (Data centre, access barrios, electrical facilities, HVAC systems, etc)
- Human resources (in support of care delivery)

Objective:

The regulatory structure surrounding nearly every facet of the healthcare operations, from protecting patient data and improving health outcomes, to reporting on compliance-related issues, necessitates healthcare entities to monitor and record the use of information assets.

Supporting or dependent entity policy references:

1) Data Retention and Disposal Policy
2) Physical and Environment Policy
3) Portable Device Security Policy
4) Acceptable Usage Policy

AM 1	Asset Management Policy

Control Demands		Control Criteria Basic/Transitional/Advanced
AM 1.1	The healthcare entity shall develop, implement and maintain an asset management policy to: 1. Be relevant and appropriate for entities operational and risk environment 2. Establish framework to effectively manage the entity's information assets through ownership assignment, accountability & responsibility definition, recording and maintaining of all/relevant properties of asset 3. Define roles and responsibilities for actions expected out of asset management policy, and shall have functional KPI's for business/function leaders 4. Define and enforce classification schemes, as applicable for AD Health Sector (Public, Restricted, Confidential & Secret) 5. Identify requirements of data retention, handling and disposal 6. Have provisions to manage Bring Your Own Device (BYOD) arrangements 7. Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier 8. Be approved by the entity's top management or its head and shall be communicated to all employees and third parties having a role in care delivery	**Basic**
AM 1.2	Where applicable, the healthcare entity shall pay specific attention to medical equipment and devices while defining policy, and shall categorically address the following demands: 1. Roles that will be allowed to access, use and maintain medical devices and equipment shall be established 2. To the extent possible, medical devices and equipment to authenticate users, based on healthcare entity authentication and authorization process 3. The need for handling procedures for each medical device and equipment in use shall be defined and updated as required to stay current 4. The need to establish and maintain risk log concerning medical devices and equipment 5. Decommissioning and/or disposal of medical devices and equipment	**Basic**

UAE IA References: T1.1.1

AM 2	Management of Assets

	Control Demands	Control Criteria Basic/Transitional/Advanced
AM 2.1	The healthcare entity shall have all their information assets identified, recorded and maintained through an information asset inventory. 1. The inventory shall be updated periodically, or during change in the environment, and shall be accurate and reliable 2. The inventory can be centralized or distributed (function/line-of-business/service wise) based on the entity's internal structures, and shall be updated 3. The inventory shall establish the relations between various types of information assets, in support of care delivery; Sample illustration: **Service** A ➔ needs B **Information** ➔ supplied by C **Device/Equipment/Process/Dependent-Service** ➔ processed using D **Application** (ERP/EMR/Office Automation Applications/etc.) ➔ running on E **Technology** (server/systems) ➔ supported/operated/managed by XYZ **Roles** (human resources involved in care delivery)	**Basic**
AM 2.2	Ownership for each identified assets shall be assigned to a designated role: 1. The owner of an information asset shall define/identify the control requirements to minimize the impact of risk, due to the compromise of assets under his ownership 2. The owner shall review the adequacy of implemented control measures periodically and amend/modify the control environment as necessary 3. The owner shall ensure effectiveness of the implemented controls, in addressing the risk environment 4. Access and/or use of information assets shall be authorized by the asset owner Ownership of shared IT resources (email system, Active Directory, Common File Server, etc.) shall be collectively owned by the entity's Information Technology/System or Information and Communication Technology Function.	**Basic**

AM 2.3	The healthcare entity shall establish and enforce rules on the acceptable use of information assets: 1. The rules shall be communicated to all employees and contractors in support of care delivery, and shall be read and acknowledged by all 2. Entities shall maintain records of user acceptance on the acceptable use of information assets The rule shall consider general requirements and industry best practices and shall have management requirements to reduce probabilities of information leakage/loss/theft and system compromises.	**Basic**
AM 2.4	Entity management shall be aware of emerging cyber risks, and shall address risk due to the exploitation of the concept-in-practice "Bring Your Own Device (BYOD)" 1. Probabilities of compromise through the use of personal devices shall be addressed through suitable rules and role-based usage agreements 2. Authorization to use personal devices to access/view/use/share/process/store personal health information is subject to user acknowledgement on the usage agreements Control process and technology solution shall be implemented to reduce/address/contain factors of risk.	**Basic**

UAE IA References: T1.2.1, T1.2.2, T1.2.3 & T1.2.4

AM 3	Asset Classification and Labelling

	Control Demands	Control Criteria Basic/Transitional/Advanced
AM 3.1	The healthcare entity shall classify all information assets, that categorises information assets into one of the following classification scheme: • Public • Restricted • Confidential • Secret	**Basic**
AM 3.2	Information classification shall consider value of the information and shall be more restrictive/deterrent based on the entity's tolerance of financial impact due to compromise of the information considered.	**Transitional**
AM 3.3	The level of essential protection needed for an asset shall be considered while determining asset classification.	**Transitional**
AM 3.4	The healthcare entity shall establish process to reassess and/or change information classification, based on the following: 1. Change in the value of information 2. Changes to environment (location, access, storage, processing, usage, etc.) 3. Changes in protection levels	**Transitional**
AM 3.5	The healthcare entity shall establish process to interpret classification schemes, while receiving information from other entities/3rd parties and shall apply all essential control measures to safeguard/protect against compromise.	**Transitional**
AM 3.6	The healthcare entity shall establish criteria for automated classification of information and shall consider using technology solutions to do so based on established classification scheme and criteria.	**Advanced**
AM 3.7	The healthcare entity shall establish process to label its information assets in all its form (physical & digital) in a way that is consistent with its classification scheme.	**Basic**

UAE IA Reference: T1.3.1, T1.3.2

AM 4	Asset Handling

	Control Demands	Control Criteria Basic/Transitional/Advanced
AM 4.1	Handling procedures shall be defined for information, consistent with their classification. 1. Handling procedures shall detail security requirements during: • Access granting and privilege allocation • Processing • Storing • Communication/sharing • Printing 2. Security requirements based on asset value shall be considered in the handling procedures	**Basic**
AM 4.2	Ensure adoption and application of handling procedures while handling information.	**Basic**
AM 4.3	The healthcare entity shall manage removable media in accordance with the classification scheme, handling procedures and acceptable use of assets. The entity shall: 1. Establish media management procedures to address lifecycle requirements (setup, distribution, utilization and disposal) 2. Implement rules and guidelines for protecting assets against unauthorised access, misuse or corruption during movement.	**Basic**
AM 4.4	Access and usage of removable media shall be controlled and shall be based on the entity's management approval. Entity management shall: 1. Accept all involved/inherent risk concerning the use of removable media, and shall bear all responsibilities and is held accountable for the risks inherent in authorizing the use of removable media	**Basic**
AM 4.5	The healthcare entity shall establish medical devices and equipment management procedures for each category of identified medical devices and equipment.	**Basic**

AM 4.6	Access and privilege allocation for medical devices shall be provided to defined roles, with essential qualification and experience required to operate. The healthcare entity shall: Secure and safe-guard medical devices and equipment in accordance with its classification scheme and risk factor	**Basic**
AM 4.7	The healthcare entity shall prevent unauthorized disclosure, modification, destruction or loss of patient health information stored on medical devices and equipment. Entities shall ensure; 1. Information stored within the medical devices and equipment shall be encrypted 2. Electronic communication between medical devices and equipment shall be encrypted 3. Healthcare entities shall define minimum essential qualification required to operate and/or handle medical devices and equipment 4. Copies of valuable health data is moved to a secure storage/location to reduce the risk of its data damage or loss	**Transitional**
AM 4.8	Healthcare facilities shall consider wired communication facility for medical devices and equipment. Usage of wireless communication facility with medical devices and equipment shall be avoided to the extent possible.	**Transitional**
AM 4.9	Entity shall deploy technology solution to white list removable media, and shall be complemented by content encryption and biometric based access provisioning.	**Advanced**
AM 4.10	The healthcare entity shall establish control procedures for the removal, movement, and transfer of information assets (information, equipment, medical devices, and information processing equipment/systems). Healthcare entities shall; 1. Authorize removal, movement and transfer of information assets 2. Maintain records of removal, movement and transfer	**Transitional**

UAE IA Reference: T1.3.3, T1.4.1, T2.3.7

AM 5	Asset Disposal

	Control Demands	Control Criteria Basic/Transitional/Advanced
AM 5.1	The healthcare entity shall dispose information assets, when no longer required: • by the entity • on basis of regulatory demands • for legal proceedings	**Basic**
AM 5.2	The healthcare entity shall establish a control process that ensures data once destroyed is not recovered	**Basic**
AM 5.3	Media, both digital and physical, when no longer required shall be destroyed by the entity	**Basic**
AM 5.4	The healthcare entity shall establish control procedures for the secure disposal or reuse of media, equipment, devices and systems, containing classified information. The healthcare entity shall: 1. Ensure sensitive data and licensed software has been securely removed beyond recovery, prior to disposal	**Transitional**
AM 5.5	Retention requirement of data/information contained within media and system shall be verified and complied with, prior to disposal	**Basic**
AM 5.6	All disposal requirement shall be authorized by entity management prior to disposal	**Basic**
AM 5.7	The healthcare entity shall maintain records, on media disposal. The records shall have, but not be limited to, the following fields: • Information and/or asset owner • Type of media • Classification • Disposal type • Reason for disposal • Retention expiry date (if data) • Data removal confirmation and evidence • Disposal authorized by	**Advanced**

UAE IA Reference: T1.4.2, T2.3.6

3. Physical and Environmental Security

Information and information processing equipment(s)/facilities has greater dependence on physical environment to achieve business objectives. Physical environment and its security are foundational elements to define secure data processing, data storage, data communication/sharing, data hosting and data disposal. Physical and environmental security programs and efforts define the various measures or controls that protect healthcare entities from loss of connectivity, availability of information processing facilities, storage (backup and archival) equipment(s)/facilities and medical equipment's/devices caused by theft, fire, flood, intentional destruction, unintentional damage, mechanical failure, power failure, etc. Physical security measures shall be adequate to deal with foreseeable threats and should be tested periodically for their effectiveness.

The following aspects of physical and environmental security shall be considered;

- Physical protection of data center and information processing equipment(s)/facilities
- Physical entry control for secure areas
- Medical devices/equipment(s) protection
- Heating, ventilation, and air conditioning of critical areas and work places
- Supporting mechanical and electrical equipment's
- Surveillance of critical areas and work places
- Security and protection of physical archives
- Fire and environmental protection
- Visitor management

Objective:

To ensure that information assets receive adequate physical and environmental protection, and to prevent or reduce probabilities of physical and environmental control/security compromises (loss, damage, theft, interference, etc.)

Supporting or dependent entity policy references:

1) Clear Desk and Clear Screen Policy

PE 1	Physical and Environmental Security Policy

Control Demands		Control Criteria Basic/Transitional/Advanced
PE 1.1	The healthcare entity shall develop, implement and maintain a physical and environmental security policy, to ensure adequate physical and environmental protection of entities information assets. The policy shall: 1. Be relevant and appropriate for entities operational and risk environment, concerning internal and external threats 2. Address requirements of secure storage of hazardous or combustible materials that ensures avoidance of: • human injuries or loss of life • damage to information and information systems 3. Consider classification of information assets and their physical presence 4. Define roles and responsibilities for actions expected out of physical and environmental security policy 5. Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier 6. Be read and formally acknowledged by all users 7. Be approved by entity's top management or head of the entity, and shall be communicated to all employees and third parties having role in care delivery	**Basic**
PE 1.2	The healthcare entity shall establish procedures and guidelines in support of policy implementation	**Transitional**
PE 1.3	The physical and environmental policy shall consider equipment and medical devices, with specific focus on their: 1. Physical and environmental demands, as needed by the manufacturer recommendations and regulatory requirements 2. Placement and physical access 3. Probabilities of data loss during maintenance, decommissioning and/ or authorized off-site activities	**Basic**

UAE IA Reference: T2.1.1, T2.3.5

PE 2	Secure Areas

Control Demands		Control Criteria Basic/Transitional/Advanced
PE 2.1	The healthcare entity shall define and use security perimeters to protect facilities that contain information and information systems. The healthcare entity shall: 1. Identify secure areas, and define security perimeter, based on information assets contained within or information being processed 2. Ensure adequate security counter measures are applied to identified secure areas to protect information and information systems within 3. Secure areas of medical equipment and devices hosting or usage to avoid and minimize probabilities of unauthorized access and usage 4. Consider the impact of compromise of confidentiality, integrity and availability of information or information assets while applying security counter measures	**Basic**
PE 2.2	Allocate secure private areas to discuss personal health information by authorized stakeholders	**Advanced**
PE 2.3	Secure areas shall be protected by appropriate control measures to ensure only authorized personnel are provided access and authorized activities are being conducted. The healthcare entity shall: 1. Maintain List of authorised personnel having access to secure areas 2. Authenticate all persons accessing secure areas 3. Maintain records for secure area access 4. Ensure that all employees and contractors wear distinguished form of visible identification (Badge/ID cards) within the premises of the entity 5. Ensure the locking mechanisms on all access doors are adequate, and alarms configured to alert prolonged open-state of doors 6. Escort contractors or third parties while inside the secure areas 7. Deploy closed circuit television (CCTV/surveillance camera) in identified vantage points of secure areas as required by Monitoring and Control Centre (MCC) Abu Dhabi 8. Preserve CCTV footage for a period as required by Monitoring and Control Centre (MCC) Abu Dhabi	**Basic**

PE 2.4	The healthcare entity shall nominate owners for each identified secure areas. Nominated owners of secure area shall: 1. Review access records/logs and surveillance footage at least on a quarterly basis 2. Reconcile list of authorized users, having access to secure areas 3. Maintain a list of physical key inventory, as with whom the keys of secure areas are with	**Transitional**
PE 2.5	Offices, meeting rooms and facilities in support of healthcare service delivery shall be equipped with adequate physical security measures. The healthcare entity shall: 1. Demarcate and isolate public access areas and key work areas, to restrict public or visitor or customer access to key work areas of the facilities 2. Avoid obvious signs that indicates the type of information or activities in the secure areas	**Basic**
PE 2.6	The healthcare entity shall design and apply physical protection against natural disasters, environmental threats, external attacks and/or accidents. The healthcare entity shall: 1. Ensure that fall-back equipment, device, system and backup media are protected from damage caused by natural or man-made disasters 2. Battery power backup shall be available to provide power to key information systems and critical data centre infrastructures	**Basic**
PE 2.7	The healthcare entity shall ensure that physical and environmental protection countermeasures and procedures applied are aligned with the outcome of Risk Assessment and regulatory mandates.	**Transitional**
PE 2.8	The healthcare entity shall design physical protection and guidelines for working in secure areas. The healthcare entity shall: 1. Supervise activities in secure areas 2. Control access of mobile, portable and surveillance devices/equipment/utilities, to secure areas	**Basic**
PE 2.9	Ensure all personnel accessing secure areas is aware of security requirements and arrangements, and accepts rules and guidelines concerning security measures. The healthcare entity shall: 1. Educate employees and contractors, not to discuss personal health information in public areas	**Transitional**

PE 2.10	The healthcare entity shall have segregated delivery and loading areas and shall establish control measures over entry and exit. The healthcare entity shall: 1. Establish access procedures to loading and unloading areas to restrict access to only authorized personnel 2. Inspect and register incoming and outgoing materials, in accordance with healthcare entity's asset management procedures	**Basic**

UAE IA Reference: T2.2.1, T2.2.2, T2.2.3, T2.2.4, T2.2.5, T2.2.6

PE 3	Equipment Security

Control Demands		Control Criteria Basic/Transitional/Advanced
PE 3.1	The healthcare entity shall site/position equipment and medical devices in manner that they are always protected. The healthcare entity shall: 1. Establish guidelines on physical protection and unauthorized access of equipment and medical devices 2. Consider environmental risk condition while positioning of equipment and medical devices	**Basic**
PE 3.2	The healthcare entity shall protect equipment and medical devices from disruptions caused by failures in supporting utilities. The healthcare entity shall; 1. Ensure uninterrupted power provisions to information processing systems	**Transitional**
PE 3.3	The healthcare entity shall maintain supporting equipment, to ensure their continued availability. The healthcare entity shall: 1. Document suppliers' recommendations for the maintenance of equipment and make them available to maintenance personnel. 2. Establish operating procedures for commissioning, maintenance and decommissioning of equipment activities 3. Establish maintenance schedule of supporting utilities, and maintain up-to date records for maintenance carried out	**Advanced**
PE 3.4	Power, telecommunication and cables carrying data shall be secured and protected. The healthcare entity shall: 1. Ensure that power, telecommunication and data cables are protected against physical tampering 2. Segregate power and telecommunication/data cables to avoid interference	**Basic**

PE 3.5	The healthcare entity shall identify and apply security measures to protect equipment, medical devices and information processing systems while off-site. The healthcare entity shall: 1. Ensure manufacturer's recommendation and instructions are followed, while equipment, medical devices and information processing systems are off-site 2. Ensure that movement and possession (chain of custody) logs for off-site equipment, medical devices and information processing systems maintained and verified 3. Ensure security measures are applied to protect off-site equipment, medical devices and information processing systems from probabilities of information leakage, tampering and unauthorized activities	**Advanced**
PE 3.6	The healthcare entity shall ensure that unattended equipment, medical devices and information processing systems are protected against information leakage and unauthorized activities. The healthcare entity shall: 1. Define user responsibilities and establish procedures when leaving equipment, medical devices and information processing systems unattended 2. Implement controls to protect equipment, medical devices and information processing systems when left unattended	**Basic**
PE 3.7	The healthcare entity shall define and enforce a clear desk and clear screen policy to paper documents, removable storage media, and information processing systems. The clear desk and clear screen policy shall: 1. Define user responsibilities with respect to clear desk and clear screen requirements 2. Be appropriate to the purpose and objectives of the healthcare entity 3. Read and acknowledged by all employees and contractors of the healthcare entity	**Basic**

UAE IA Reference: T2.3.1, T2.3.2, T2.3.3, T2.3.4, T2.3.5, T2.3.7, T2.3.8, T2.3.9

4. Access Control

Healthcare entities ability to provide authorized access and its commitment to control unauthorized access to information and information processing systems under its custody are key elements to demonstrate the entities' objective interest to protect information that belongs to:

- Its customers,
- Patients of the Abu Dhabi healthcare ecosystem,
- The Government, and
- The healthcare entities themselves.

The influence of information on the delivery of healthcare and related services and the increased dependence on application and technology, demands that the avenues and provisions of access are strictly controlled. It is essential that healthcare entities understand the responsibilities concerning access management and are accountable for the consequences arising from breaches or disclosures from their respective areas of authority. Healthcare entities shall define policy mandates and process mechanisms essential to secure and protect their information and information systems. Healthcare entities shall take specific care when personal health information is being accessed and used s, and shall define access criteria that conforms to the following facts:

- A healthcare relationship exists between the user and the data subject (the subject of care whose personal health information is being accessed),
- The user is carrying out an activity on behalf of the data subject,
- There is a need for specific data to support care delivery or continuum of care.

Healthcare entity's management shall be aware of the risk environment and outcomes of unauthorized access, and are accountable for any and all consequences and impact on:

- Abu Dhabi Government
- Abu Dhabi Healthcare-ecosystem or Health Sector
- Patients concerned
- Healthcare entity itself

Objective:

To ensure access to information and information systems are controlled, and to minimize probabilities of information leakage, tampering, loss and system compromises.

Supporting or dependent entity policy references:

1) Clear Desk and Clear Screen Policy
2) Network Access Control Policy
3) Password Management Policy
4) Information Access Management as part of Administrative Safeguards of HIPAA
5) Facility Access Control as part of Physical Safeguards of HIPAA
6) Access Control as part of Technical Safeguards of HIPAA

The level of applicability of above-mentioned policies will vary depending on the individual healthcare entity.

AC 1	Access Control Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
AC 1.1	The healthcare entity shall develop, enforce and maintain an access control policy to ensure access to information and information systems are adequately controlled and secured. The policy shall: 1. Be relevant and appropriate to control and secure access to information, application, technology, medical devices and equipment 2. Include management demands and directions, scope and specific applicability based on: a. Type of service b. Information c. Application d. Technology e. Medical devices and equipment 3. Emphasize the requirement-of-need and role-based access principles 4. Establish criteria for access, with core focus on; a. granting of access b. access authorization c. access revocation d. access termination 5. Address the healthcare entity needs on secure password management and practices 6. Mandate the usage of unique identity and complex password 7. Where relevant, define control measures and provisions for portable/mobile devices, including user owned devices, that handle the healthcare entity's data or has the healthcare entity application(s) to conduct business transactions 8. Include control requirements for the access and use of network services 9. Include management actions on violations and deviations 10. Define roles and responsibilities for actions expected 11. Be reviewed, updated and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier 12. Be approved by the entity's top management and shall be communicated to all employees and third parties having a role in care delivery 13. Be read and formally acknowledged by all relevant stakeholders	**Basic**

UAE IA Reference: T5.1.1

AC 2	User Access Management

	Control Demands	Control Criteria Basic/Transitional/Advanced
AC 2.1	The healthcare entity shall implement a formal user registration and de-registration process. The healthcare entity shall: 1. Ensure request for user registration and de-registration are process driven, and are in compliance with established criteria for access 2. Ensure unique user accounts are created for each individual requiring access, and prohibit sharing of same account with multiple users 3. Ensure group user account are not created or used 4. Revoke user accounts during employee exit 5. Revalidate access requirements during role change 6. Maintain records/list of persons authorised to use healthcare entity's information systems, applications, medical devices and equipment 7. Establish and follow separate user registration and de-registration process for temporary and third party user account requirements	**Basic**
Ac 2.2	The healthcare entity shall restrict and control allocation of privileges, based on principles of need to know. The healthcare entity shall: 1. Ensure normal user accounts are not used as service accounts or used to conduct privileged application and system level activities 2. Privilege or administrative accounts shall be used by individual with a role to conduct privilege activities 3. Ensure users privileges are restrictive in nature, and are assigned based on needs to conduct business activities 4. Privilege or administrative accounts shall not be used for conducting normal day to day operational activity 5. Ensure usage of service accounts are controlled, and are not hardcoded in application codes are scripts 6. Enforce multifactor authentication scheme for all administrative access 7. Mandate administrative or privilege access and associated activities are logged and audited	**Advanced**

AC 2.3	The healthcare entity shall establish process for secure allocation, use and management of security credentials. The healthcare entity shall: 1. Ensure default application and system passwords are changed and not being used 2. Ensure passwords are always hashed and stored in encrypted format 3. During initial user account creation, communicate details of user account and password in two different communication modalities 4. Enforce complexity requirements on password characters, and shall have at least: a. Eight characters b. One number, one upper-case and lower-case character, and a special character 5. Enforce passwords, including that of service accounts and privileged accounts, are recycled at an entity-defined time frame 6. Ensure that password history is maintained, and shall restrict users from using immediately used previous passwords (at least 3 previous passwords) 7. Educate users to adopt good practices while selecting and using passwords	**Basic**

UAE IA Reference: T5.2.1, T5.2.2, T5.2.3, T5.3.1, T5.5.3

AC 3	Equipment and Devices Access Control

	Control Demands	Control Criteria Basic/Transitional/Advanced
AC 3.1	The healthcare entity shall protect confidential and secret information on portable or removable media, mobile or portable devices, and medical equipment or devices. The healthcare entity shall: 1. Authenticate user, where relevant, access to equipment, devices and media 2. Ensure media containing confidential and secret information is password protected and encrypted 3. Where relevant, control access to medical equipment and devices through password enforcement in compliance with the healthcare entities password complexity and usage requirements 4. Control access to mobile and portable devices hosting confidential and secret information 5. Establish mobile device management process to protect entity information being used, processed or stored in mobile devices	**Transitional**
AC 3.2	The healthcare entity shall control access to equipment, devices, system and facilities at teleworking sites. The healthcare entity shall: 1. Ensure access to equipment, devices, system and facilities at teleworking sites are authenticated, and their access to entity resources are authorized based on need 2. Ensure confidentiality and protection of healthcare and personal health information while providing/consuming services through teleworking principles, including telemedicine related services 3. Conduct random audit of equipment, devices, system and facilities at teleworking sites 4. Maintain an inventory of assets in use at teleworking sites	**Transitional**

UAE IA Reference: T5.7.1, T5.7.2

AC 4	Access Reviews

	Control Demands	Control Criteria Basic/Transitional/Advanced
Ac 4.1	The healthcare entity shall review access and privileges granted to its user. The healthcare entity shall: 1. Establish process for the reviewing of user access and associated privileges to various entity resources 2. Define responsibility for access and privileges review, based on entity resources being accessed 3. Conduct user access and privileges review at least once a year or earlier, as required by the entity's risk environment 4. Maintain an up to date inventory of access granted and privileges assigned 5. Define the criteria for the automatic revocation of user access and privileges based on the entity's defined period of inactivity or non-usage of resources	**Basic**

UAE IA Reference: T5.2.4