دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

ABU DHABI - HEALTHCARE INFORMATION AND CYBER SECURITY STANDARD

February 2019

PUBLIC عـــام

Document Title:	Abu Dhabi - Healthcare Information and Cyber Security Standard		
Document Ref. Number:	DOH/SD/ADHICS/0.9	Version	0.9
Publication Date:	03 February 2019		
Applies To:	This standard covers all DOH regulated health care entities and services within the Emirate of Abu Dhabi, and shall be applicable to all healthcare/medical facility(s), healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s).		
Effective Date:	The effective date of this Standard will be the date of its publication.		
Document Classification	◉ Public		
Document Owner/Control	Support Services Division		

Table of Contents

Section A - Introduction, Governance and Framework Definition

Section B - Abu Dhabi Healthcare Information and Cyber Security Requirements

Section A

Introduction, Governance and Framework Definition

1. Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard Introduction

1.1. Introduction

The Department of Health (DOH) intends to establish the Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard, a strategic initiative in support of DOH's vision and Federal/National mandates, endorsed by DOH's Executive Committee. The provisions of this Standard are harmonized with industry and international expectations towards Information Security.

The adoption of ADHICS Standard by DOH regulated healthcare entities will prepare and enable Abu Dhabi Health Sector to uphold privacy and security. Its implementation complements Government's initiatives towards Health Information Exchange (HIE), enhancing security and public trust.

1.2. Document Organization

This document is organized in two sections:

- "Section – A" defines the introductory, governance and framework aspects of the Abu Dhabi Healthcare Information and Cyber Security program;
- "Section – B" documents the control requirements of the Abu Dhabi Healthcare Sector Standard.

1.3. Overview

The requirements of this Standard are based on governmental and industrial demands, and Information Security and Cyber Security international best practices. DOH has invested time and effort to understand the demands, define Abu Dhabi Health Sector-specific Information and Cyber Security requirements, and define timelines towards compliance.

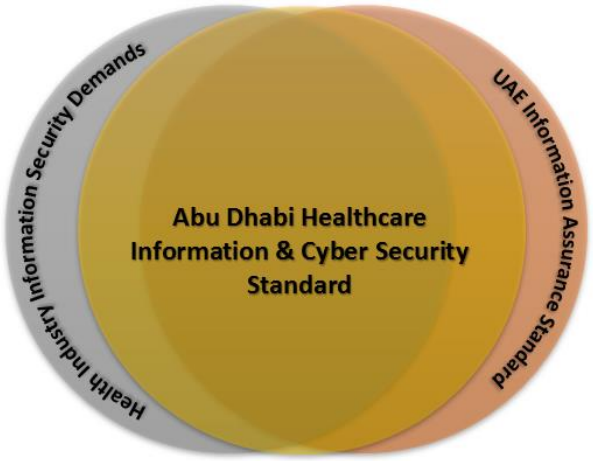

Figure 1: Abu Dhabi Healthcare Information and Cyber Security Standard – Relational Representation

The Standard focuses on the specifics of protecting and/or securing personal health information. It defines the controls applicable to healthcare entities based on their capability, maturity and risk environment. Compliance with this Standard increases Information assurance level between healthcare entities, public (citizens, residents and visitors) and governmental bodies.

1.4. Purpose and Background

Patients' trust in a healthcare entity and its staff members is a vital element in the continuous improvement in healthcare management. As personal health information is regarded as the most confidential of all types of personal information, it is essential that healthcare entities and professionals, inclusive of management/support/administrative/clerical staff members:

- Ensure confidentiality, and maintain privacy of subjects-of-care (personal health information);
- Protect the integrity/accuracy and quality of health information, to ensure patient safety and such information remains valid through its life cycle to be auditable;
- Confirm such health information is available, to the right entities/systems/resources at the right time, to support effective and organized delivery of care, and to prepare and predict future demands & trends, and;
- Ensure that the healthcare entity meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks.

ADHICS Standard outlines the control mandates essential to protect health information during its creation, maintenance, display, processing, usage, transmission and disposal, and to maintain the information's confidentiality, integrity and availability *(including authenticity, accountability and auditability).* The Standard defines governing principles, essential to establish and operate a successful Information Security Program by Abu Dhabi Emirate-based healthcare entities. It summarizes procedures and technical standards that should be incorporated and sets out requirements and desired goals at various levels of a healthcare entity's maturity, operational complexity and risk environment.

Application of this Standard is based on the risk appetite, defined in Section 4 - Risk Management, and Section 6 - Control Adoption, Compliance and Audit.

By implementing this Standard healthcare entities and/or other custodians of health information will be able to ensure the minimum requisite level of security that is appropriate for them to uphold public trust, improve delivery and maintain the confidentiality, accuracy, quality and availability of personal health information.

Adoption and application of the requirements of the Standard is based on the approach and criteria defined in Section 4 - Risk Management, and Section 6 -Control Adoption, Compliance and Audit.

2. Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) Scope & Applicability

2.1. Scope and Applicability

The scope of ADHICS Standard:

- Covers all DOH regulated health care entities and services within the Emirate of Abu Dhabi, and shall be applicable to all healthcare/medical facility(s), healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s),

- It includes information (in physical and digital forms), medical device and equipment, applications and software, information system, physical infrastructure (data centre, access barriers, electrical facilities, HVAC systems, secure areas, etc.) and human resources (in support of care delivery)

- This standard applies to any/all systems and applications fully owned by healthcare entity, as well as healthcare entity's access and usage of partners' and third party systems and applications utilised within Abu Dhabi Healthcare ecosystem (Shafafiya portal, Health Information Exchange platform, DoH e-Services, Medical Tourism portal, etc..).

- Applicability of specific control mandates/requirements of the Standard, is defined based on the maturity, operational complexity and risk environment of the implementing entity, as defined in Section 4 - Risk Management and Section 5 – Methodology.

- The content of the standard, while comprehensive, is not exhaustive. Depending completely on the adoption and application of the Standard without due consideration of the actual or tangible business requirements does not adequately discharge the healthcare entities' management responsibility to provide and maintain healthcare information security that protects the information's confidentiality, integrity and availability.

The development and application of Information Security policies and procedures, additional or as required by this Standard, is the responsibility of participating/implementing healthcare entity.

2.2. Benefits

By adopting and complying with the provision of this Standard, healthcare entities demonstrate their commitment to uphold Government's values, and secure personal and/or protected health/healthcare information. The following are the benefits to be derived by an entity from implementation of this Standard:

1) Enhancing trust in individual (patient) relationships: The Standard's holistic approach covers the whole organisation, not just IT, and encompasses people, processes and technology. This enables employees and patients to readily understand risks and embrace security controls as part of their everyday working practices.
2) Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable level.
3) Clarity on information ownership. When a business grows rapidly, it does not take long before there is confusion about who is responsible for which information assets. The Standard helps businesses by clearly setting out information ownership and risk responsibilities.
4) Reducing operational costs by providing predictable outcomes—mitigating risk factors that may interrupt the process, service, out-comes, values and/or assets.
5) The Standard takes into consideration the accepted global benchmark for the effective management of information assets, enabling organizations to avoid costly penalties and financial losses.
6) Decreasing the likelihood of violations of data privacy.
7) Enabling new and better ways to process electronic health related transactions.

3. Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Governance Structure

Governance has been described as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly"[1]. Information security governance is a subset of organizational governance.

The governance structure of the Information and Cyber Security program is based on Federal and Local Government mandates, and is aligned with the principles of corporate governance. The establishment of Healthcare Information Infrastructure Protection (HIIP) Workgroup at Abu Dhabi Health Sector level, with participation from all sector operators or healthcare entities, is essential to ensure collaboration and coordination of efforts towards Program implementation and progression across Abu Dhabi Health Sector.

Healthcare entities shall establish independent internal structures, appoint Chief Information Security Officers (CISO) to lead the structure and allocate other appropriate and competent resources as necessary to coordinate, implement, comply, enhance, maintain and manage Information Security demands as required by:

- Federal and Local Authorities
- Legislations and Regulations
- Local entity needs and risk environment
- Industry specific needs

The entity Management shall fund the program with a defined Information Security budget. The funding shall be prioritized based on needs, appropriate to address risk environments that would impact Government interest, public trust and entity objectives.

Healthcare entities shall submit quarterly progress and compliance reports, approved by the Chair of the entity's Information Security Governance Committee (ISGC). It is the responsibility of the ISGC to update the entity's top Executive, on the performance and progress of the entity's Information Security program.

ADHICS Program Governance structure is a Government mandate to achieve success, and demands a comprehensive security strategy that is explicitly linked to the healthcare entity's strategy and business processes. Information Security shall be an integral component of enterprise governance, aligned with IT governance and integrated into corporate strategy, concept, design, implementation and operation. Protecting critical/classified health information is a priority demand, and shall constitute healthcare entity's major risk environment.

[1] Information Security Governance – A Practical Development and Implementation Approach, by Krag Brotby

Healthcare entities should implement the following Governance Structure:

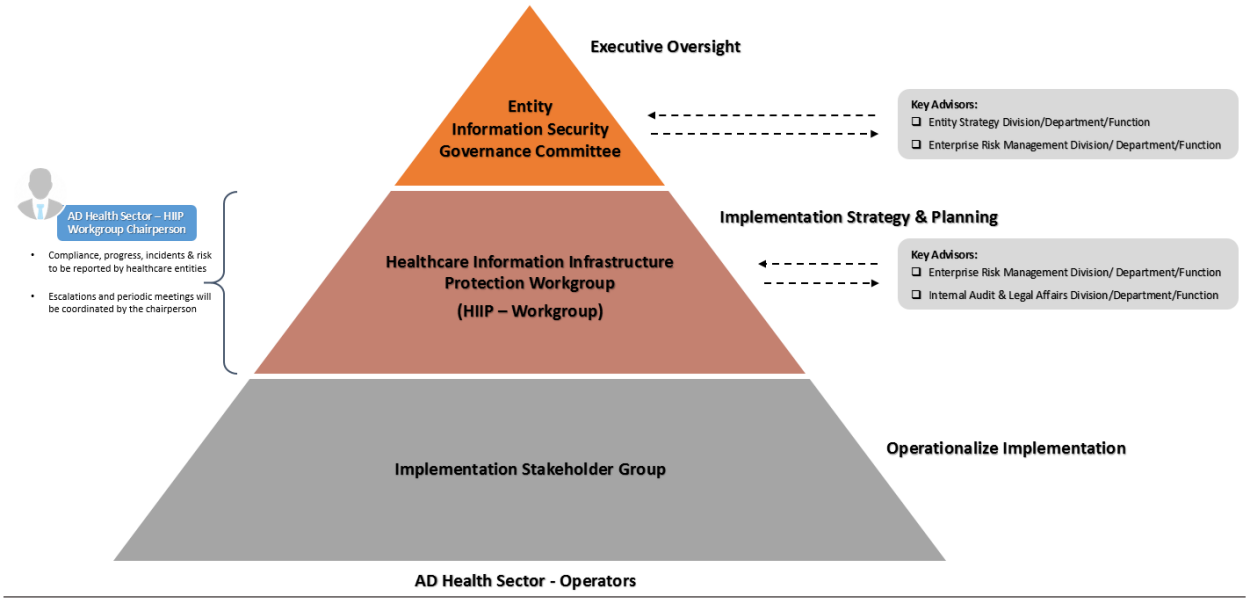

Figure 2: Abu Dhabi Healthcare Information Security – Governance Structure

The Governance pyramid is led by Information Security Governance Committee. The Committee's role is to provide management oversight and direction for both physical and logical aspects of information security. It is chaired by the entity's nominated/appointed senior/management resource, and includes Corporate/Business Leaders and Senior Management members from across the entity's various business lines. It shall have adequate power and authority, with a quorum strength of 60% to conduct Committee meetings.

Important Committee decisions on the entity's Information Security affairs will be communicated to the Chair of Abu Dhabi Health Sector – HIIP Workgroup, through entity HIIP – Workgroup. The Committee will have the following roles:

1) Provides direction and recommendations to the entity's HIIP - Workgroup on the overall strategic direction and priorities in support of the Government's interest, public trust and entity objectives concerning Information Security and Technology.
2) Enforces ADHICS standards and policies, and monitors compliance;
3) Recommends and allocates adequate budget towards entity Information Security initiatives;
4) Acts appropriately on HIIP team reports concerning Information Security performance metrics, security incidents, investment requests etc.

The Committee relies on feedback and reports from the HIIP and other personnel from various functions namely: Strategy, Medical & Clinical Affairs/Practices, Internal Audit, Enterprise Risk Management, Compliance, Legal and others to ensure that the principles, axioms and policies are complied with in practice.

The next layer of Governance is led by Healthcare Information Infrastructure Protection (HIIP) Workgroup. It coordinates activities with "Implementation Stakeholders" across various functional/business verticals, ensuring that suitable Information Security policies and procedures are in place to support Abu Dhabi Healthcare Information and Cyber Security Standard. The team is led by the CISO, who shall also be the entity point of contact to coordinate information security related matters with sector regulator, and comprises of members from various business and support verticals. The HIIP - Workgroup will have the following roles:

1) Developing Information Security policies and ensuring their compliance with the principles approved by the Information Security Governance Committee;
2) Coordinating and managing the Information Security initiatives and its control demands;
3) Periodically reviewing the Information Security policies to ensure the efficiency and effectiveness of control/risk environment and recommending improvements where necessary;
4) Reviewing and monitoring compliance with the policies and assisting in Internal Security audit and self-assessment processes;
5) Identifying significant trends and changes in information security risks and, where appropriate, proposing changes to the controls framework and/or policies;
6) Reviewing critical security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;
7) Periodically reporting on the status of the security controls to the Information Security Governance Committee and to the Chair of the Abu Dhabi Health Sector HIIP – Workgroup;
8) Conduct Information Security awareness campaign, to enhance Information Security culture and develop understanding of the requirements.

At the bottom of the Governance pyramid is the "Implementation Stakeholders" team. The team is responsible for the day-to-day operational activities of implementation and maintenance of requirements as needed by the Standard. The team comprises of Information Security officers, information technology professionals, and business representatives. The role includes:

1) Day-to-day operational activities for implementation and maintenance of the Information Security Standard and respective policies and procedures;
2) Ensuring suitable technical, physical and procedural controls are in place in accordance with the Standard, and are implemented at all levels within the entity.
3) Collecting, analyzing and reporting on information security metrics and incidents;
4) Reporting to HIIP – Workgroup confirmed or suspected policy violations (Information Security Incidents) affecting the entity's assets;
5) Evaluating compliance with the Information Security policies through regular self-assessment process and internal audits.

4. Risk Management

Risk assessment can guide a healthcare entity in determining the level of effort and resources needed to protect confidentiality, integrity and availability. The results of regular risk assessment must be aligned with the implementing entity's priorities, initiatives and investments. A healthcare entity should undertake the following three activities, as a minimum to meet its responsibilities in managing risk towards healthcare information.

4.1. Periodic assessment of risk related to healthcare information and supporting resources

As a minimum, healthcare entities shall adhere to all the areas and their mandated requirements listed in this Standard. For each perceived risk, the assessment must cover the following:

a) Probability of the risk event occurring
b) Impact if the risk event occurs and
c) Possible risk mitigation actions and counter-measures.

4.2. Implement measures to remediate identified risks

A healthcare entity shall invest effort and resources, to mitigate identified risk factors. The entity shall develop and maintain risk mitigation strategy, as appropriate and relevant, with details of efforts, resources and cost involved, along with the benefit towards the entity, Government and public. The mitigation strategy shall prioritize control implementation based on the impact of identified risk, and the priority of the control implementation as required by this Standard and Government demands. The health care entity shall:

- Establish and maintain policies in support of risk mitigation demands
- Define procedures in support of established policies
- Implement any essential controls, and controls from this Standard, to address entity risk

4.3. Periodic reporting on control performance

A healthcare entity shall periodically monitor the following implemented controls-related factors:

- Relevance and need of the controls to the entity's risk environment
- Performance of the controls
- Effectiveness in addressing and maintaining the risk, within acceptable risk level

The outcome of monitoring shall be recommendations that shall complement and enhance control effectiveness, relevance and performance. The recommendations may have the following elements, but should not be limited to:

- Control adequacy
- Control gaps
- Control enhancements
- Additional control requirement
- Policy update and amendments
- Control withdrawal/termination

5. Asset Classification

The value of assets shall be represented through appropriate classification reflecting their critical importance to healthcare entities, government and relevant stakeholders. Classification is the first visual and digital representation that an asset is critical or least critical, and shall be protected accordingly.

Healthcare entities shall classify their assets, including information, based on the following classification factors and colouring themes:

Asset Classification	Classification Factor and Criteria
Public C100 M0 Y100 K0 R0 G150 B64 # 009640 GREEN	Information destined to be used in public domain or public use, and has no legal, regulatory or organizational restrictions for its access and/or usage. Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping citizens, patients and other stakeholders understand better the country's/governmental/organizational vision and values.
Restricted C100 M0 Y0 K0 R0 G158 B227 # 009EE3 BLUE	Information that must be afforded limited confidentiality protection due to its use in the day-to-day operations. Disclosure of such information could have limited adverse impact on the functioning or reputation of the entity or the government/health sector. Information that relates to the internal functioning of the entity and will not have general relevance and applicability to a wider audience. Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary, if they were to be revealed.
Confidential C0 M80 Y95 K0 R232 G78 B27 # E84E1B ORANGE	Information that requires robust protection due to its critical support to decision-making within the entity, and across health sector and government. Information that could disclose designs, configurations or vulnerabilities exploitable by those with malicious intent. Information that the entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody (e.g. critical personal information, health/healthcare information, government information, financial information etc.).
Secret C0 M100 Y100 K0 R227 G5 B19 # E30513 RED	Information that requires substantial and multilevel protection due to its highly sensitive nature. Disclosure of such information could have a serious and sustained impact upon the government, national security, social cohesion, economic viability and health of the country. Information disclosure could potentially threaten life or seriously prejudice public order.

6. Control Adoption, Compliance and Audit

The Abu Dhabi Healthcare Information and Cyber Security Standard sets out the minimum requirements of control mandates essential to secure healthcare information and processing facilities. The control requirements specified by ADHICS Standard are grouped into three different categories (individually referred as standard, in the context of the area/section under consideration or being discussed), applicable to entities based on their risk environment, value of healthcare information under custody and maturity. It is essential that healthcare entities comply with the provisions of all "Basic" level requirements, within six months of the official release of ADHICS Standard. Health entities shall define road map for initiatives towards complete compliance/implementation of ADHICS Standard, consistent with Government interest and objectives, and entity risk environment. Entities shall review and submit their updated compliance status to DOH, as part of periodic compliance reporting, highlighting road map timelines and deviations. Healthcare entities shall invest time, effort and resource to progress their compliance to "Advanced" level.

Control categories are based on continuous improvement aspect of Information Security life cycle, which ensures capabilities are continuously adapted and evolved in line with changing environment and maturity level. To attain "Transitional" level, a Healthcare entity must meet all demands of "Basic" and "Transitional" criteria for each specific requirement/section. Similarly, to attain an "Advanced" level, demands of all "Basic", "Transitional" and "Advanced" criteria for each specific requirement/section must be met.

Control Category	Definition, Applicability and Timelines of Compliance
Basic	Control demands outlined in this category are the absolute minimum essentials of Information Security, and shall be considered high priority to be complied with. The control implementation shall protect Information assets from critical threats, and shall be considered foundational to build on assurance capabilities. **Applicability:** Control demands of this category is always applicable. All healthcare entities, shall comply with the provisions of this category, irrespective of their facility status. However, if the control demands are not relevant to an entity's business operation, the entity shall produce valid business justification as part of their reports to health sector operator of Abu Dhabi, along with necessary supporting evidence and records. **Timeline for compliance:** Within six months of official program induction/on-boarding or official release of ADHICS Standard, whichever comes first.

<table>
<tr>
<td>Transitional</td>
<td>
Control demands outlined in this category are high priority controls to enhance security posture of healthcare entities. The control implementation shall protect information assets from a wide range of threats, inclusive of critical and high impact threats, based on the value of information assets owned, managed and handled by the healthcare entity. The control implementation directly complements in redefining/improve Healthcare Entities risk environment.

Applicability: Control demands of this category are applicable based on a healthcare entity's risk posture. They are applicable to the following types of entities:
<table>
<tr><td>Hospitals</td><td>With bed capacity 1 to 20</td></tr>
<tr><td>Center</td><td>Day Care Surgery Center
Primary Health Care
Diagnostic Center
Rehabilitation Center
Dialysis Center
Fertilization Center
Mobile Healthcare Unit
Provision of Health Service (Home care)</td></tr>
<tr><td>Pharmacy Establishment</td><td>Drug Store (Medical Store)</td></tr>
</table>
Timeline for compliance: Within one year of official program induction/on-boarding or official release of ADHICS Standard, whichever comes first.

Note: All controls categorized as "Basic" are considered essential, and are applicable by default.
</td>
</tr>
<tr>
<td>Advanced</td>
<td>
Control demands outlined in this category are essential controls, based on an entity status, and shall enhance security posture of healthcare entities. The control implementation shall protect information assets from a wide range of threats, inclusive of critical and high impact threats, based on the value of information assets owned, managed and handled by the healthcare entity. The control implementation elevates the healthcare entity's maturity level, and complements improvement of internal processes and risk environment.

Applicability: Control demands of this category are applicable based on a healthcare entity's risk posture, and shall be applicable to the following types of entities:
<table>
<tr><td>Hospitals</td><td>With bed capacity of 21 and above</td></tr>
</table>
Timeline for compliance: Within one year of official program induction/on-boarding or official release of ADHICS Standard, whichever comes first.

Note: All controls categorized as "Basic and Transitional" are considered essential, and are applicable by default.
</td>
</tr>
</table>

The standard establishes the potential security controls to cover a range of Information Security domains. Each domain area includes various security best practices and controls that Healthcare Entity should consider for implementation in a phased manner, based on its risk level and resource availability. Implementation of these Information Security control criteria's shall be monitored periodically to ensure they are adequate, appropriately implemented, maintained and that associated responsibilities, deliverables, and timelines are documented and reported.

Any policy established, in support of the implementation of this standard, shall have:

- Statement of management commitment
- Purpose of the policy
- Objective of the policy
- Scope of the policy

6.1. Compliance

The healthcare entity shall identify and maintain records of all legislative, regulatory and governmental executive orders relevant and applicable to its business. Such records shall establish:

- Demands, with references, applicable to the entity's business;
- Stakeholders for implementation and maintenance;
- Compliance checklists;
- Reporting obligations;
- Escalation demands.

Compliance with and deviations from the provisions of such legislative, regulatory and governmental executive orders shall be monitored and reported to relevant internal and external authorities periodically. Risk of such non-compliance shall be recorded in the entity's enterprise risk manual, and shall be suitably addressed.

The healthcare entity shall also demonstrate compliance with applicable intellectual property rights (IPR) and the export/import and use of cryptographic keys and mechanisms.

It is essential healthcare entities establish reliable metrics and measurement to identify the state and effectiveness of compliance with required controls. This shall produce comparable results through timelines.

6.2. Audits and Assessments

The healthcare entity shall develop formal yearly audit programs to validate and verify compliance with the provisions of this Standard, and any other information security compliance requirements as they becomes relevant and valid.

The ethical aspects of functional independence shall be considered to avoid conflict of interest and to aid in the efficient identification of facts and their unbiased reporting to relevant authorities.

The healthcare entity shall conduct technical assessments on its information system and application environment periodically to identify any weakness or potential point of compromise. The outcome of assessment shall be shared with relevant stakeholder for necessary containment and remedial actions.

Outcome of audits and assessments shall be preserved (i.e. filed, stored, saved and protected) with the highest level of access protection and secure storage facilities. Tools used for audit and assessments shall be protected from unauthorized access and usage to ensure critical audit and assessment information are not modified and/or misused.

Entity ISGC shall be briefed on the outcomes and action of audits and assessments, on a regular bases as defined by the CISO.

7. Healthcare Entity Responsibility

The healthcare entity shall be committed and responsible to address all information and cyber security risks to its environment. The entity shall invest time, effort and resources to remediate and reduce the impact of risk to maintain a secure and trusted environment and practices.

Based on their job assignment or association, everyone associated (including third parties/ contractors/vendors) with the healthcare entity has certain responsibilities to maintain day-to-day security of the Entity's environment, services, systems and Information. Main responsibilities of involved stakeholders/parties concerning Abu Dhabi Healthcare sector are listed below:

Stakeholder	Responsibility
Department of Health	1) Establish Abu Dhabi Healthcare Information and Cyber Security Standard. 2) Enforce ADHICS Standard for Abu Dhabi Healthcare sector, covering all healthcare entities/operators. 3) Enhance/modify/amend ADHICS Standard, based on learning and industry evolution. 4) Provide training and support to healthcare entities to implement ADHICS Standard. 5) Conducts periodic review meetings with healthcare entities to support compliance. 6) Monitor compliance and risk status and report/escalate to necessary Federal and Local Authorities.
Healthcare Entity Management	1) Overall accountability for the implementation of ADHICS Standard within respective entities. 2) Fund and manage program implementation. 3) Approve entity program plan, strategies, initiatives and policies. 4) Accept Information Security risk that might impact the entity, patients and Abu Dhabi healthcare sector.
Healthcare Entity - InfoSec Stakeholders	1) Responsible for the internal coordination and implementation of ADHICS Standard. 2) Monitor and report/escalate the entity's Information Security program progress to entity management and Abu Dhabi Healthcare sector – HIIP Chairperson. 3) Educate business users and conduct periodic Information Security awareness trainings/sessions. 4) Responsible for ensuring that security requirements are adequately addressed during the design, development, implementation and maintenance of any existing or new information systems. 5) Maintain system accreditation as per policy.
Healthcare Entity - Business / End User	1) Adhere to and comply with ADHICS Standard and Entity policies and demands. 2) Align business processes as per Information Security demands.

Section – B

Abu Dhabi Healthcare Information and Cyber Security Requirements

1. Human Resources Security

Human resources are critical and valuable assets essential to conduct organizational business, and are considered the weakest link within the security framework. Healthcare entities shall take adequate measures to ensure that the right resources are hired to deliver the right values, are equipped to safeguard organizational interest, and are relieved in a manner that shall not impact organizational assets, values, reputation and financial conditions at any time, current or future.

Healthcare entities shall be aware of the risk environment towards and from human resources, and shall define adequate contractual, administrative, technical and process oriented controls to minimize probabilities of:

- Information leakage
- Unauthorized access
- System compromise
- Misuse of privilege, facilities and information
- Loss of information
- Credential sharing and misuse

The entity's management shall be aware that human resources are easy targets for social engineering and phishing attacks, and can be involved in accidental and deliberate attempts to cause disruptions to the entity's services. Entity management shall consider risk environment concerning third party and contract resources.

Administrative and cleaning staff pose new challenges and threats to healthcare entities, and the entity's management shall apply adequate control measures to address those risks.

Objective:

To ensure right resources are hired and utilized to support secure delivery of organizational objectives and services, and are relieved in a manner that does not impact organizational assets, value, reputation and financial conditions any time current or in future.

Supporting or dependent entity policy references:

1) Information Security Management Policy
2) Acceptable Usage Policy
3) Compliance Policy
4) Disciplinary Actions Policy

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

AC 5	Network Access Control

Control Demands		Control Criteria Basic/Transitional/Advanced
Ac 5.1	Access to the entity's network and network services shall be controlled, and shall be provided based on specific need for which the user is authorized for	**Basic**
AC 5.2	The healthcare entity shall use appropriate authentication methods to control access of remote users The healthcare entity shall: 1. Ensure all remote login and access are only through secure channels 2. Consider usage of multifactor authentication scheme to control access by remote users	**Basic**
AC 5.3	The healthcare entity shall identify all equipment and devices connected to its network, and shall have automated mechanism to detect unauthorized equipment and devices	**Basic**
AC 5.4	The healthcare entity shall control access for the purpose of diagnostic and configuration The healthcare entity shall: 1. Identify and whitelist all ports, services and utilities that are used for troubleshooting, and for diagnostics and configuration purposes 2. Define protection mechanism for the diagnostic and configuration services and utilities that are essential, and disable services and utilities that are not required. 3. Restrict access for remote troubleshooting, diagnostic and configuration to authorized roles and shall be allowed from authorized workstations 4. Log all remote access activities related to troubleshooting, diagnostic and configuration	**Advanced**
AC 5.5	User access to shared and isolated networks shall be restricted The healthcare entity shall: 1. Provide access to shared and isolated networks in line with its Access Control Policy, requirements of business applications and need to access shared resources	**Basic**

AC 5.6	The healthcare entity shall define and implement network routing controls to ensure information flow and system, devices, equipment connections are not compromised and are in line with requirements of Access Control Policy The healthcare entity shall: 1. Establish processes for secure configuration and rules application for network routing requirements 2. Always ensure source and destination address and services or ports are used while defining and applying routing rules 3. Enable routing protection countermeasures to avoid manipulation of routing systems and tables 4. Define and implement network architecture that segregates and isolates internal and publically accessible systems. 5. External connections to information systems and networks outside entity shall be managed through interfaces consisting of perimeter protection devices (such as firewalls) 6. Ensure that communications with external systems, networks and key internal systems are always monitored for malicious and suspicious payloads 7. Periodically scan for any covert channel connections to public networks bypassing entity security defence	**Transitional**
AC 5.7	The healthcare entity shall ensure wireless access within the entity is secured. The healthcare entity shall: 1. Establish usage restrictions and secure configuration requirements 2. Establish authorization process for wireless access and usage 3. Ensure public and guest access are segregated and isolated from the entity's internal network 4. Ensure that internal wireless is not broadcasted 5. Authenticate wireless connections using strong encryption mechanism and based on entity's internal authentication scheme 6. Control privileged and administrative activities are not carried out through the entity's wireless network 7. Restrict wireless access capabilities of medical equipment and devices	**Transitional**

UAE IA Reference: T5.4.1, T5.4.2, T5.4.3, T5.4.4, T5.4.5, T5.4.6, T5.4.7

AC 6	Operating System Access Control

Control Demands		Control Criteria Basic/Transitional/Advanced
AC 6.1	The healthcare entity shall establish and enforce secure log-on and log-off procedures to control access to system and applications. The healthcare entity shall: 1. Ensure that access to entities systems, applications and services that process, use or store healthcare information are authenticated 2. Enforce automated locking of workstation/system after a predefined period of inactivity 3. Establish authorization procedures, based on classification of systems, application, services and information in scope 4. Establish and enforce idle session time-out requirements 5. Automatically terminate inactive sessions after a predefined period of session inactivity 6. Display a logon banner that requires the user to acknowledge and accept security terms and their responsibilities before access to the system is granted	**Basic**
AC 6.2	The healthcare entity shall create unique identifier (user ID) for each users who require access to entities systems, applications or services, and shall implement a suitable authentication technique. The healthcare entity shall: 1. Grant each user with a unique identifier 2. Ensure all user activities are logged with the associated identifier	**Basic**
AC 6.3	The healthcare entity shall restrict and control the use of utility programs and tools that might be capable of overriding system and application controls. The healthcare entity shall: 1. Identify essential system utilities and tools and enforce appropriate controls for use 2. Provide access to system utilities and tools based on appropriate authorization 3. Maintain inventory of access to system utilities and tools 4. Monitor use of system utilities and tools	**Advanced**

UAE IA Reference: T5.5.1, T5.5.2, T5.5.4

AC 7	Application and Information Access Control

	Control Demands	Control Criteria Basic/Transitional/Advanced
AC 7.1	The healthcare entity shall restrict access to information and application system functions in accordance with the access control policy. The healthcare entity shall: 1. Ensure access to information and application access is restricted and based on need-to-know principles and appropriate authorization 2. Enforce role-based access mechanisms 3. The need for access shall be justified by individuals responsibilities 4. Ensure that office assistants, cleaning staffs and other unauthorized personnel do not have access to healthcare data	**Basic**
AC 7.2	The healthcare entity shall isolate sensitive systems in a dedicated environment.	**Transitional**
AC 7.3	The healthcare entity shall implement controls and shall not expose non-public information to the general public. The healthcare entity shall: 1. Establish and enforce procedures for publishing of public information to ensure non-public information is not exposed accidently or deliberately 2. Establish and enforce procedure to periodically validate that non-public information is not exposed to the public domain 3. Validate relevance of publicly available information 4. Ensure no healthcare and related data is exposed to the public domain	**Transitional**

UAE IA Reference: T5.6.1, T5.6.2, T5.6.3

5. Operations Management

Healthcare entities continual effort to sustain and improve risk environment demands the need for effective management of operational activities in support of information handling, processing, sharing and storage. Operations management aims to establish and/or strengthen healthcare entities processes and efforts to improve and enhance control environment. Objective outcome of effective operations management includes, but is not limited to:

- Improved security and reduce probabilities of compromise
- Reduced errors
- Controlled unauthorized activities
- Regulated efforts
- Increased efficiency
- Reduced security incidents

The objectivity of providing healthcare services shall consider security and safety of assets (data, technology, and application) in support of service delivery and healthcare entities shall demonstrate commitment in defining and controlling of operational activities concerning service delivery.

Objective:

To ensure that activities concerning support and maintenance of data, technology, and application are controlled and carried out in a standardized manner to reduce probabilities of errors and compromises, and to increase efficiency and security.

Supporting or dependent entity policy references:

1) Change Management Policy
2) Capacity Management Policy
3) System Acceptance Policy
4) Quality Management Policy
5) Backup Policy
6) Monitoring Policy

OM 1	Operations Management Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
OM 1.1	The healthcare entity shall develop, enforce and maintain an operations management policy to ensure support and maintenance activities concerning data, technology and application are controlled. The policy shall: 1. Be relevant and appropriate to the healthcare entity's operational and risk environment concerning data, technology and application 2. Establish management demands on: a. Segregation of duties b. Configuration management c. Change control d. Baselines and minimum security configurations e. Standard operating procedures f. Capacity management g. System acceptance h. Malware control i. Quality management j. Backup management k. Logging and monitoring l. Patch management 3. Provide framework for managing operational activities	**Basic**

UAE IA Reference: T3.1.1

OM 2	Operational Procedures

Control Demands		Control Criteria Basic/Transitional/Advanced
OM 2.1	The healthcare entity shall develop and enforce baseline and recommended configuration settings for common information technology products and applications, medical devices and equipment The healthcare entity, while developing baseline and recommended configuration setting, shall consider: 1. Manufacturer's security recommendations 2. Requirements of this Standard 3. Industry best practices 4. Risk mitigation strategies 5. Corrective and preventive actions (audit, assessment and incident outcomes)	**Transitional**
OM 2.2	The healthcare entity shall document operating procedures for all support, operational and maintenance activities of information systems and application, medical devices and equipment The healthcare entity shall: 1. Disseminate operating procedures and ensure all relevant stakeholders are aware of their responsibilities as needed by their role 2. Ensure operating procedures are relevant and are updated on defined timelines or when essential 3. Ensure system documentation includes up-to-date diagrams.	**Transitional**

OM 2.3	The healthcare entity shall control changes to information systems and application, medical devices and equipment The healthcare entity shall: 1. Establish a Change Advisory Board to authorize changes 2. Define and enforce a change management process that addresses the following elements: a. Identification and recording of significant changes b. Planning and testing of changes c. Assessment of potential impacts d. Formal approval procedure e. Communication of change to all relevant stakeholders f. Roll-back plan to be utilized during unsuccessful changes g. Post implementation assessment h. Maintenance of previous version of software, code and configurations 3. Define information systems and applications, medical devices and equipment that shall be covered by the Change Management Process	**Transitional**
OM 2.4	The healthcare entity shall establish a process that controls transition of information systems and applications The healthcare entity shall: 1. Ensure that movement of system and applications from development or project state to operational or production state are managed through the Authorization and Change Process	**Transitional**
OM 2.5	The healthcare entity shall identify and segregate roles of conflicting interests and assign responsibilities accordingly The healthcare entity shall: 1. Implement suitable alternative or compensating controls when roles of conflicting interests cannot be assigned to different individuals	**Transitional**
OM 2.6	The healthcare entity shall identify and separate development, test, staging and operational environments The healthcare entity shall: 1. Identify the appropriate level of protection between operational, staging, test, and development environments 2. Document and apply clear processes for the transfer of data, information, code, configuration, software and systems between environments 3. Ensure as-is operational data is not used in test environment 4. Restrict usage/migration of test data into operational environment	**Transitional**

UAE IA Reference: T3.2.1, T3.2.2, T3.2.3, T3.2.4, T.3.2.5

OM 3	Planning and Acceptance

Control Demands		Control Criteria Basic/Transitional/Advanced
OM 3.1	The healthcare entity shall identify and document current and future capacity requirements while planning for new information systems and applications The healthcare entity shall: 1. Have the ability to monitor and measure the capacity of current systems and estimate future information systems and application demands 2. Ensure there is sufficient capacity with information systems to support good system performance and reliability. 3. Identify capacity thresholds for all information systems and applications, and shall define advance escalation matrix to ensure capacity demands are met 4. Establish process to: a. decommission systems that are no longer needed b. optimise databases c. archive data that is not accessed regularly	**Advanced**
OM 3.2	The healthcare entity shall establish acceptance criteria for new information systems and applications, changes, upgrades and releases, in addition to satisfactory test results The healthcare entity shall: 1. Establish processes for system acceptance, and ensure system acceptance is acknowledged by the relevant authoritative individual 2. Develop test cases for each of the requirements and changes and ensure tests are carried out and test results documented prior to usage in an operational environment 3. Ensure testing is never performed on production systems 4. Ensure user profiles (with permissions appropriate for the tasks) used for testing are different from the ones used for operational and development activities 5. Ensure development tools and/or editors are not installed on operational systems	**Transitional**

UAE IA Reference: T3.3.1, T3.3.2

OM 4	Malware Protection

Control Demands		Control Criteria Basic/Transitional/Advanced
OM 4.1	The healthcare entity shall protect its information assets from malware The healthcare entity shall: 1. Ensure minimum security configurations is maintained in all information assets, as applicable and as relevant 2. Implement anti-malware and anti-virus protection mechanisms for network and individual information systems (server, workstation, mobile/portable computing devices) 3. Ensure anti-malware and anti-virus protections mechanisms are updated and current 4. Enable real-time protection capabilities 5. Establish and enforce periodic scan schedules 6. Scan removable media for viruses and malware on all occasions when they are connected to information systems 7. Disable auto-run features for removable media on information systems 8. Configure anti-malware and anti-virus protection systems to alert responsible stakeholders on event, incident or anomaly detection 9. Provide ongoing awareness for users on techniques, tactics and procedure to avoid and minimize probabilities of malware and virus attacks	**Basic**
OM 4.2	The healthcare entity shall deploy gateway level protection mechanisms to detect and defend against malware and viruses The healthcare entity shall: 1. Deploy gateway level protection for web and email traffic from and to the entity 2. Implement technology that can detect and prevent access to malicious websites or sites from prohibited categories.	**Advanced**

UAE IA Reference: T3.4.1

OM 5	Backup and Archival

	Control Demands	Control Criteria Basic/Transitional/Advanced
OM 5.1	The healthcare entity shall maintain backup copies of essential information and software needed to support care delivery and its operations The healthcare entity shall: 1. Establish backup management process that identifies; a. Essential and critical information in support of care delivery, business and entity operations b. Data owner c. Data recovery point and time requirements d. Backup frequencies, time of execution and methods e. Data restoration frequencies and test criteria 2. Ensure backup of all identified essential and critical data 3. Ensure data restoration requirements for continuity and recovery are adequately met	**Basic**
OM 5.2	The healthcare entity shall establish data archival requirements that satisfies entities retention demands The healthcare entity shall: 1. Establish formal processes for archival and destruction of data 2. Identify data-sets and establish retention requirements as needed by law, regulation, and entity demands 3. Identify and enforce archival criteria (what and when to archive, how long to archive) and methods (physical/electronic) that satisfies established retention timelines 4. Preserve data during archival 5. Destroy data that has crossed retention timelines and are no longer required by the entity 6. Maintain adequate record on archival and destruction	**Advanced**

UAE IA Reference: T3.5.1

OM 6	Monitoring and Logging

Control Demands		Control Criteria Basic/Transitional/Advanced
OM 6.1	The healthcare entity shall establish and enforce monitoring procedures for information systems and application, medical devices and equipment Monitoring procedures shall: 1. Identify aspects (system use, changes, unauthorized activities, internal processing, exception, information exchange, integration, access, etc.) to be monitored 2. Establish frequency and methods (dashboards, web-link, mobile-app, scheduled tasks, parameter validation, logs, records, manual verification, etc.) of monitoring 3. Establish minimum information gathering requirements for each monitoring activities 4. Define minimum time requirements for maintaining information gathered from monitoring activities 5. Define criteria for alerting and escalation 6. Have defined criteria that quantifies specific outcomes of monitoring as incidents 7. Establish roles for monitoring activities and assign specific responsibilities	**Advanced**
OM 6.2	The healthcare entity shall enable audit logs recording administrator, operator and user activities, exceptions and security events. The log shall include faults related to information processing and communication The healthcare entity shall: 1. Identify all activities to be captured in logs for all hardware devices, equipment, operating systems and applications 2. Identify minimum required information to be logged 3. Define minimum frequency requirements for reviewing each type of log 4. Define minimum time requirements for maintaining each type of log commensurate with legal, regulatory and entity demands 5. Ensure that logs are not tampered with or modified or destroyed 6. Ensure unauthorized access to logs are controlled	**Advanced**

OM 6.3	The healthcare entity shall preserve logs in a centralized log management system The healthcare entity shall: 1. Control access to the centralized log management solution 2. Ensure the centralized log management solution is managed by individuals who do not have operational role in implementing or maintain information systems or application 3. Retain logs for a period commensurate with legal, regulatory and entity demands on each type of log 4. Define use cases and dashboards based on the entity's needs and industry recommendations, and shall consider: a. System utilisation and performance trends b. Deviation from entity policy and procedures c. Access control variances and violations d. Any potential sign of security breach or attack	**Advanced**
OM 6.4	The healthcare entity shall synchronize clock of all information systems with an agreed time source The healthcare entity shall: 1. Standardize date/time format and enforce the standard time to be used in all systems 2. Ensure clock of medical devices and equipment are same as that of the connected systems 3. Regularly check that the clocks of all relevant information processing systems are synchronized.	**Basic**
OM 6.5	The healthcare entity shall define and establish formal procedure for updates and patching of information system and application, medical devices and equipment The healthcare entity shall: 1. Ensure all systems and devices that process or communicate information are patched and protected 2. Define criteria and process for application of standard, urgent and critical patches 3. Ensure all critical security patches are applied as soon as practicable from the date of release. 4. Ensure patches are deployed to a subset of systems or devices to allow testing before deployment to all. 5. Ensure firmware on devices are updated 6. Periodically validate patch status of systems and devices in use	**Basic**

OM 6.6	The healthcare entity shall monitor information processing systems to prevent opportunities for information leakage The healthcare entity shall: 1. Implement data leakage prevention (DLP) measures	**Transitional**

UAE IA Reference: T3.6.1, T3.6.2, T3.6.3, T3.6.4, T3.6.5, T3.6.6, T3.6.7, T7.6.4, T7.7.1

OM 7	Security Assessment and Vulnerability Management

	Control Demands	Control Criteria Basic/Transitional/Advanced
OM 7.1	The healthcare entity shall conduct periodic independent assessment to ensure information assets are secure and always protected The healthcare entity shall: 1. Establish yearly schedules and conduct: a. Penetration testing on the entity's system, network, applications and security infrastructures and environment b. Vulnerability assessment on all entity's system, network, applications and security infrastructures and environment c. Web security assessments on web applications accessible over internet 2. Establish processes to conduct security testing and authorization by authorized business and security stakeholders for new system/application and upgrades prior to production roll-out and usage 3. Establish processes to mitigate and manage identified findings and vulnerabilities 4. Share reports on identified findings and vulnerabilities and the status of mitigation with: a. The entity's management b. Department of Health, Abu Dhabi's health sector regulator 5. Periodically follow up on the progress and status of mitigation measures with the appropriate stakeholders 6. Verify effectiveness and efficiency of mitigation measures	**Transitional**
OM 7.2	The healthcare entity shall ensure that assessment data is not available with third parties engaged to conduct assessments beyond the time of engagement The healthcare entity shall: 1. Ensure that system, network, applications and security related information is shared with third parties when they are on-site 2. Ensure that all information related to the entity's system, network, applications and security infrastructures and environment and assessment outcomes are erased from the involved third party's assets and environment after the completion of the assessment activity 3. Ensure that any shared reports are suitably protected through an adequate encryption mechanism	**Transitional**

UAE IA Reference: T7.7.1

6. Communications

Abu Dhabi Government's vision towards modernization and enhancement of society and services necessitates sharing of appropriate information with eligible stakeholders within and across entities. Stakeholder utilization of information from within and across entity has influenced decisions, and improved outcomes. It is essential that the communication between various information processing components are provisioned through controlled communication process and channel. It is essential healthcare entities define criteria, rules and controls that secure communication processes, components, interfaces, channels and stakeholders to securely aid human to machine, machine to machine, machine to human and human to human communication to facilitate information exchange.

Risk environment of the connected world demands that an entity's management be conscious of the current risk environment concerning communication and information exchange, and that it defines proactive measures that shall:

- Secure entities communication infrastructures
- Ensure information exchange are controlled through formal exchange agreements and controls
- Ensure information is delivered to right stakeholders or information processing components
- Minimize probabilities of unauthorized access

Objective:

To ensure information exchanged between authorized resources are secured within and across entity boundaries.

Supporting or dependent entity policy references:

1) Communication & Operation Management Policy
2) Cryptography Policy
3) Network Access Policy
4) Wireless Access Control Policy
5) Cloud Security Policy

CM 1	Communications Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
CM 1.1	The healthcare entity shall develop, enforce and maintain a communications policy, to ensure information in transit and information being exchanged are adequately protected The policy shall: 1. Be relevant and appropriate to the entity's information exchange and communications demands 2. Demonstrate management commitment, objectives and directions 3. Establish management demands on: a. Protection of communication infrastructure b. Communication and protection of personal health information c. Information exchange agreements d. Integration methods e. Physical mode of information exchange f. Electronic and/or online transactions g. Information exchange within and beyond entity boundaries h. Business information systems 4. Provide framework to protect information in transit from interception, copying, modification, misrouting, destruction and any other unauthorized activities	**Basic**

UAE IA Reference: T4.1.1

CM 2	Information Exchange

Control Demands		Control Criteria Basic/Transitional/Advanced
CM 2.1	The healthcare entity shall develop, enforce and maintain formal procedures on information exchange and transfer incorporating control measure that protects information during information exchange and transfer The procedures shall: 1. Include control measures to protect and reduce probabilities of compromise during information exchange and transfer taking into account: a. Classification and value of information b. Information exchange and processing environment c. Stakeholders involved 2. Identify minimum technical standards for packaging and transmission of health information 3. Establish responsibilities and sanctions for actions and deviations 4. Define actions to be taken during issues, incidents and deviations	**Transitional**
CM 2.2	The healthcare entity shall ensure that critical and private information is protected while in transit The healthcare entity shall: 1. Ensure that user-name and password are communicated using two different communication channels (email and SMS-text, or email and phone, etc.) 2. Encrypt critical information before transferring and sharing encryption/decryption key using a different communication channel	**Basic**
CM 2.3	The healthcare entity shall develop secure practices and capabilities while sharing information The healthcare entity shall: 1. Protect information that is exchanged within the entity 2. Ensure that information exchanged between entities, and information sharing communities are protected 3. For custom-developed applications, ensure that the exchange or transfer of information between systems and applications uses appropriate interoperability standards 4. Identify and implement security requirements for exchanging information and software with third parties	**Basic**

CM 2.4	The healthcare entity shall establish agreements between the entity and external parties for the exchange of information and software The healthcare entity shall, prior to the beginning of exchange of information and software: 1. Brief and agree with the external parties on all security requirements to be included in the agreement 2. Include additional control requirements when exchange of information includes: a. Protected health information (PHI) b. Personally identifiable information (PII) 3. Clearly define roles and responsibilities of each party to the agreement 4. Establish non-disclosure agreements for all disclosures between the entity and the external parties 5. Include in the agreements: a. Definitions of information to be protected b. Duration of agreement c. Process for notification of leakage d. Ownership e. Right to audit and monitor activities that involve personal health information and personally identifiable information	**Basic**
CM 2.5	The healthcare entity shall ensure that external parties involved in the exchange of information and software are aware of the security requirements to be implemented The healthcare entity shall: 1. Ensure all security requirements formally agreed between the entity and the external parties are implemented and are effective	**Transitional**

CM 2.6	The healthcare entity shall protect physical media containing information during transit The healthcare entity shall: 1. Identify and ensure that physical media containing sensitive is classified in accordance with the established classification scheme 2. Ensure that physical media in transit containing sensitive information is protected against: a. Information disclosure or leakage b. Loss of information or media c. Modification d. Unauthorized access 3. Ensure that physical media in transit containing sensitive information is adequately tracked 4. Utilize trusted entity staff or courier service for transporting media	**Basic**
CM 2.7	The healthcare entity shall protect information involved in electronic messaging The healthcare entity shall: 1. Identify and categorize all means of electronic messaging through which the entity information can be transmitted 2. Define specific control requirements for each identified category of electronic messaging 3. Ensure exchange of information is based on need and are addressed to authorized and legitimate resources 4. Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging.	**Transitional**
CM 2.8	The healthcare entity shall develop, enforce and maintain procedures to secure information transferred across business information systems The procedures shall: 1. Identify all points of interconnections and integrations between business information systems and identify the information to be protected 2. Identify adequate security measures to be applied to protect each type of information	**Advanced**

UAE IA Reference: T4.2.1, T4.2.2, T4.2.3, T4.2.4, T4.2.5

CM 3	Electronic Commerce

Control Demands		Control Criteria Basic/Transitional/Advanced
CM 3.1	The healthcare entity shall protect electronic commerce service and information involved passing over public and untrusted networks from service compromise and fraudulent activity, contract dispute, unauthorized disclosure and modification The healthcare entity shall: 1. Maintain a list of electronic commerce services along with details of: a. Service details and information involved b. Electronic commerce service provider and partner detail c. Beneficiary details 2. Identify and implement security measures to protect information used in electronic commerce services 3. Ensure security requirements are agreed and captured in service agreements with electronic commerce partners	**Transitional**
CM 3.2	The healthcare entity shall protect information involved in online transactions against incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure and unauthorized message duplication or replay The healthcare entity shall: 1. Identify all information used in online transactions 2. Identify and implement security measures to protect information used in online transactions 3. Ensure security requirements are agreed and captured in service agreements with partners involved in online transactions	**Transitional**
CM 3.3	The healthcare entity shall protect information available through the publicly accessible system The healthcare entity shall: 1. Identify all information available through the publicly accessible system 2. Establish process to publish and maintain information on the publicly accessible systems 3. Ensure information is sanitized and approved before publication 4. Define security measures to publish information on publicly accessible systems 5. Ensures that information available through the publicly accessible system is always available and is protected against unauthorized modification	**Advanced**

UAE IA Reference: T4.3.1, T4.3.2, T4.3.3

CM 4	Information Sharing Platforms

Control Demands		Control Criteria Basic/Transitional/Advanced
CM 4.1	The healthcare entity shall ensure that connectivity to information sharing platforms is secure and controlled The healthcare entity shall: 1. Maintain a list of information sharing platforms that the entity connects to and/or operates 2. Determine security requirements for connecting to or release of information into identified information sharing platforms 3. Establish security requirement for accessing entity operated information sharing platforms 4. Develop required capabilities to establish secure connectivity to any required sector, national or international information sharing community	**Advanced**
CM 4.2	The healthcare entity shall not use cloud services or infrastructure to store, process or share information that contains health information The healthcare entity shall: 1. Ensure that healthcare information is not transmitted outside the UAE 2. Identify and disconnect integration of system that process, store or utilize health information with any of the entity's systems that connect or utilize cloud services 3. Not share identified or de-identified health information with 3rd parties, inclusive of counterparts and partners, unless authorized by the health sector regulator of Abu Dhabi	**Basic**
CM 4.3	The healthcare entity shall ensure that access to health information exchange platforms within the UAE is strictly controlled The healthcare entity shall: 1. Ensure that access to health information exchange platforms are provided to resources with an authorized need and are not misused 2. Periodically validate and verify access requirements to health information exchange platforms 3. Conduct frequent assessments and audits to identify misuse and ensure compliance 4. Report on incidents and misuse to the health information exchange operator and the health sector regulator of Abu Dhabi	**Basic**

UAE IA Reference: T4.4.1, T4.4.2. T.6.3.1

CM 5	Network Security Management

	Control Demands	Control Criteria Basic/Transitional/Advanced
CM 5.1	The healthcare entity shall ensure that all networks and supporting infrastructures are adequately managed, controlled and protected The healthcare entity shall: 1. Ensure that all network components and interconnections are identified and sufficiently documented, including documentation of updates incorporated via the change management process 2. Ensure that network documentation includes up to date diagrams 3. Identify threats and vulnerabilities affecting network components and network as a whole 4. Implement specific security controls to mitigate identified vulnerabilities 5. Centralize the management of access control to networking components 6. Ensure that only trusted devices and users can gain access to internal networks 7. Continually monitor implemented controls for their efficiency and effectiveness	**Basic**
CM 5.2	The healthcare entity shall identify and enforce security requirements, service levels, and management requirements as part of relevant network services agreements The healthcare entity shall: 1. Specify specific security requirements essential for each of its network services 2. Establish minimum security requirements for each identified service 3. Establish service levels for internal and external network service providers 4. Evaluate service level compliance and report deviation to relevant authorities	**Transitional**

CM 5.3	The healthcare entity shall segregate physical, logical and wireless networks based on criticality, nature of services and users information systems The healthcare entity shall: 1. Establish criteria for network segregation 2. Establish and maintain appropriate network security zones, allowing data flow follow through controlled path 3. Establish minimum and specific security requirements for each of the segregated networks, zones and resources 4. Periodically evaluate the adequacy of implemented segregation strategy	**Basic**
CM 5.4	The healthcare entity shall ensure that all wireless networks are adequately protected The healthcare entity shall: 1. Conduct site survey to determine the optimal physical location for the placement of wireless access-points or devices to avoid stray signal leaking outside the entity's physical boundary 2. Ensure that wireless access points are configured to use strong authentication and cryptographic methods 3. Ensure that only trusted devices and users gain access to internal networks via wireless access 4. Ensure that guest access provided to visitors and guest are physically and logically isolated and shall not traverse through the entity's internal network 5. Monitor access and usage of guest wireless facilities	**Basic**

UAE IA Reference: T4.5.1, T4.5.2, T4.5.3, T4.5.4

7. Health Information and Security

Health information has become fundamental to the provision of healthcare services. Healthcare entities generate and utilize healthcare information and establish relations with individuals to give the information a persistent value during its lifecycle of usage and references.

Privacy of health information is a patient's basic right, by law and principles, and shall be protected. Healthcare entities shall demonstrate care, prudence and determination in protecting healthcare information under their custody, and uphold the public trust placed on them.

It is a government mandate that healthcare information be considered as highly classified data element, to be protected through its lifecycle. Healthcare entities shall establish control measures that shall prevent and minimize probabilities of:

- Unauthorized access and/or usage of healthcare data
- Unauthorized or accidental modification of healthcare data
- Leakage of healthcare data
- Loss of healthcare data

Healthcare entities shall consider critical:

- One's physical or mental health conditions or state,
- Clinical decisions and healthcare services provided
- Payments concerning healthcare services provided or envisioned

Objective:

To ensure healthcare information are suitably protected to uphold public trust and reliability on governmental interest and values, and to sustain entity reputation in the provisioning of healthcare services.

Supporting or dependent entity policy references:

1) Information Security Management Policy
2) Acceptable Usage Policy
3) Compliance Policy
4) Disciplinary Actions Policy

HI 1	Health Information Protection Policy

Control Demands		Control Criteria Basic/Transitional/Advanced
HI 1.1	The healthcare entity shall develop, enforce and maintain a health information protection policy that ensures management's commitment to protect healthcare information The policy shall: 1. Define management requirements on; a. Criteria for access and acceptable usage b. Accountability and/or data ownership c. Healthcare data communication or sharing 2. Mandate the requirements of non-disclosure and confidentiality during and after employment 3. Define government sanctions and legal obligations 4. Include reference to organizational disciplinary process	**Basic**

UAE IA Reference: M5.2.4

HI 2	Health Information Privacy and Protection

Control Demands		Control Criteria Basic/Transitional/Advanced
HI 2.1	The healthcare entity shall ensure that healthcare information under its custody is suitably protected The healthcare entity shall: 1. Conduct orientation on healthcare information protection and sanctions to all its employees, relevant contractors and third parties prior to their access to healthcare information 2. Establish stricter process to ensure clear desk and clear screen practices are adhered to in areas where healthcare information is used, processed or handled 3. Define and enforce criteria for healthcare information access 4. Ensure access to health information systems and applications are restricted for individuals possessing a valid licence to practice their profession within the UAE, and any exception shall be authorized by entity CISO based on adequate justification 5. Control and restrict privileges for printing and sharing of healthcare information 6. Ensure cleaning staff access to areas where patient related healthcare information is being viewed, accessed, used, processed, stored and/or destroyed are monitored or under surveillance coverage 7. Ensure any hardcopy/media containing healthcare information is shredded after its usefulness 8. Establish processes for shredding all hardcopy documents before their disposal 9. Ensure that healthcare information with personal identifiers is not available unattended 10. Ensure printing of healthcare information is limited to local printers and are not printed through uncontrolled network printers 11. Establish processes to notify the health sector regulator of any probabilities of breaches involving healthcare information	**Basic**

UAE IA Reference: M5.2.4

8. Third Party Security

Operational efficiency, time to deliver and cost saving aspects compels entity management to utilize third party services or resources to complement service delivery. Involvement of third parties in the process of care delivery and associated areas are inevitable and needs stronger control measures to secure entity assets and information.

Healthcare entity management shall be cognizant of the fact that a significant portion of privacy breaches originates with organizations that contracted activities and services to third parties. Adequate due diligence to activities and services to be contracted, and a proactive identification and definition of control environment to secure privacy and information assets would minimize damages and benefit healthcare entities and the government. Entities that entrust access to third parties acknowledge and share responsibilities for the breaches.

A healthcare entity's management shall be aware of the risk environment related to third party services and resources, establish a suitable framework for third party management and define a control environment that shall:

- Reduce probabilities of information leakage and loss
- Secure information assets
- Minimize unauthorized access and usage
- Uphold organizational and governmental reputation
- Ensure service continuity

Objective:

To ensure third party services are controlled through suitable procedural obligations and contractual terms to secure privacy and protect information assets.

Supporting or dependent entity policy references:

1) Access Control Policy
2) Operations Management Policy
3) Procurement Policy
4) Supply Chain Management Policy
5) Compliance Policy

TP 1	Third Party Security Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
TP 1.1	The healthcare entity shall develop, enforce and maintain a third party security policy to facilitate implementation of the associated controls and to reduce probabilities of risk realization concerning third parties The policy shall: 1. Be relevant and appropriate to the relationship of the entity and the third party 2. Establish a framework that facilitates: a. Secure management of third party services and their role in healthcare and/or related services b. Defining and including information security objectives c. Third party briefing of security requirements d. Definition of roles and responsibilities 3. Demonstrate management's commitment, objectives and directions 4. Establish management's expectations on: a. Privacy and protection of information assets b. Access to system, application, device, equipment and critical area c. Non disclosures and terms of use 5. Be read and acknowledged by stakeholders and third party representatives authorized to sign on their behalf	**Basic**

UAE IA Reference: T6.1.1

TP 2	Third Party Service Delivery and Monitoring

	Control Demands	Control Criteria Basic/Transitional/Advanced
TP 2.1	The healthcare entity shall identify and enforce security requirements, service levels and management requirements as part of relevant third party services agreements The healthcare entity shall: 1. Ensure that specific security requirements essential for each of type of services are included in the service delivery agreement 2. Establish minimum security requirements for each identified service 3. Ensure measures and minimum baselines for each of the identified security requirements are established and monitored 4. Establish service levels for each of the service through third parties 5. Define and document the type of information that third party service provider needs access to 6. Assign responsibility for managing third party relationships to an individual or service management team 7. Identify and include Right-to-Audit terms specific to the provisions and environment of service management 8. Coordinate with entity contract management and legal teams for third party service requirements that needs the storing, processing and transmission of health and/or personally identifiable information	**Basic**
TP 2.2	The healthcare entity shall monitor and review services provided and reports and records submitted by third parties The healthcare entity shall; 1. Monitor compliance of security requirements identified in agreements with third parties 2. Monitor third party services and ensure required reports are received and reviewed by qualified entity resource 3. Implement controls for monitoring the exchange of information between various parties to ensure security compliance 4. Manage incidents and contingencies associated with access and violations 5. Assess and manage business, commercial, financial and legal risk associated with third party services 6. Perform audits of third parties services on a regular basis	**Transitional**

TP 2.3	The healthcare entity shall manage changes to the provisions of third party services through a formal management process The healthcare entity shall: 1. Ensure that changes to activities and provisions are in compliance with security requirements 2. Include as part of the agreement, formal processes to manage changes 3. Define parameters of change that shall be communicated and agreed between the entity and the third party	**Transitional**

UAE IA Reference: T6.2.1, T6.2.2, T6.2.3

9. Information Systems Acquisition, Development, and Maintenance

The demand for systems and applications to host and process information to deliver business values needs careful assessment of lifecycle aspects. Wide options and cost effective delivery models attract entities to determine easy to use and cost effective solutions, ignoring security aspects in order to quickly deliver on business values.

Healthcare entity management shall identify the relevant health information systems and applications,-related risk factors that impact the entities ability to provide reliable services, reputation and reliability of the solution/product or vendor. Healthcare entity management should be aware of the fact that the solution or the product selected will probably introduce new risks that shall managed through their lifecycles.

Based on detailed assessment and entity risk appetite, the healthcare entity's management shall choose from one of the below options:

- In-house development, maintenance and support of application and systems
- Outsource the development, maintenance and support of application and systems
- Out-of-shelf product deployment, maintained and support by the vendor
- Cloud-based application utilization
- Hybrid approach for the development, maintenance and support requirements

Objective:

To emphasis the need for healthcare entities to adopt secure system and software development lifecycle management processes and to ensure that systems and applications in use are securely managed and supported to avoid misuse of privileges and authority, reduce probabilities of information, system and application compromises, and to uphold entity and Abu Dhabi government's reputational value and public trust.

Supporting or dependent entity policy references:

1) Access Control Policy
2) Operations Management Policy
3) Communications Policy
4) Procurement Policy
5) Third party security policy
6) Compliance Policy

SA 1	Information Systems Acquisition, Development, and Maintenance Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
SA 1.1	The healthcare entity shall develop, enforce and maintain an information systems acquisition, development and maintenance policy to facilitate implementation of secure development and maintenance practices The policy shall: 1. Be relevant and appropriate to the model and relationship of the entity and involved internal and external stakeholders 2. Demonstrate management's commitment, objectives and directions 3. Establish a framework that facilitates: a. Defining and including information security objectives b. Selection of the right model and approach c. Identification and mitigation of risks in involved business and application processes d. Definition of roles and responsibilities 4. Establish management expectations on: a. Privacy and protection of information assets b. Secure design, development, testing, deployment, maintenance and support c. Secure access to systems, applications, devices, and equipment d. Secure processing and communication of information and data e. Non-disclosures requirements f. Cryptographic controls and requirements 5. Be read and acknowledged by involved internal and external stakeholders	**Basic**

UAE IA Reference: T7.1.1, T7.4.1

SA 2	Security Requirement of Information Systems and Applications

	Control Demands	Control Criteria Basic/Transitional/Advanced
SA 2.1	The healthcare entity shall analyse, identify, develop and implement information security requirements for new information systems and applications or enhancements to existing systems and applications The security requirement shall: 1. Be relevant to be used for new information systems or enhancements to existing information systems 2. Be approved by individuals authorized to do so on behalf of business and information security 3. Be compliant with the requirements of this standard and secure coding practices 4. Address all risk elements identified during risk assessments 5. Outline validation criteria to verify control efficiency and effectiveness 6. Define system acceptance criteria 7. Be included and maintained in business and technical requirement documents	**Transitional**
SA 2.2	The healthcare entity shall ensure developer of information systems, system components or information system services are provided suitable training prior to their involvement in development activities The healthcare entity shall: 1. Identify baseline training requirements that are essential to the developer 2. Acknowledge that developer(s) received relevant baseline training prior to their involvement in development activities 3. Identify training requirements based on implemented security functions and features 4. Design and execute training programs to address additional and future security requirements 5. Include training requirement in agreements, when the requirements are delivered and managed by third parties	**Transitional**

UAE IA Reference: T7.2.1, T7.2.2

SA 3	Correct Processing in Applications

Control Demands		Control Criteria Basic/Transitional/Advanced
SA 3.1	The healthcare entity shall validate data input to applications to ensure that the data is correct and appropriate The healthcare entity shall: 1. Define criteria, rules and validation parameters to validate data input into applications 2. Develop or configure applications to drop input data that is identified as incorrect or inappropriate	**Transitional**
SA 3.2	The healthcare entity shall incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts The healthcare entity shall: 1. Establish minimum requirements for validation checks on internal processing of application under development to ensure correct processing of data 2. Require application developers to provide evidence of compliance with minimum requirements 3. Ensure that the incorporated validation checks are valid and relevant over a period of time and meet minimum requirements through the applications' lifecycles	**Transitional**
SA 3.3	The healthcare entity shall ensure the authenticity and integrity of messages in applications The healthcare entity shall: 1. Identify and enforce requirements to ensure authenticity and integrity of messages transmitted between systems and applications	**Transitional**
SA 3.4	The healthcare entity shall validate data output from applications to ensure that data is correct and appropriate The healthcare entity shall: 1. Define criteria, rules and validation parameters to validate data output from applications	**Transitional**

SA 3.5	The healthcare entity shall ensure that all distributed and mobile applications are designed with the ability to tolerate communication failure Distributed and mobile applications shall: 1. Include off-line and duplicate or out-of-sequence response message handling capabilities	**Transitional**

UAE IA Reference: T7.3.1, T7.3.2, T7.3.3, T7.3.4

SA 4	Cryptographic Controls

	Control Demands	Control Criteria Basic/Transitional/Advanced
SA 4.1	The healthcare entity shall establish key management to support the entity's use of cryptographic techniques Healthcare entities shall: 1. Establish process to: a. Securely generate and use cryptographic keys b. Revoke/block keys c. Repair damage or corrupted keys 2. Define standards for: a. Key strength for various environments b. Key storage 3. Protect secret and private keys against unauthorized use and disclosures	**Transitional**

UAE IA Reference: T7.4.2

SA 5	Security of System Files

Control Demands		Control Criteria Basic/Transitional/Advanced
SA 5.1	The healthcare entity shall control the installation of software on operational systems The healthcare entity shall: 1. Ensure software installations are carried out only by authorized resources 2. Keep a copy of all software installed, including any previous versions 3. Ensure software installed in production systems are subject to entity change management process and approval	**Advanced**
SA 5.2	The healthcare entity shall protect system test data The healthcare entity shall: 1. Use sample data sets to test application, business and security functionalities 2. Restrict the use of real data from production systems for testing, allowing it based on appropriate control and authorization from authoritative business and information security stakeholders 3. Maintain records of copying, using and erasing of operational information in test environment 4. Ensure that personally identifiable information is not used as test data 5. Erase any data from test applications immediately after completion of the test	**Transitional**
SA 5.3	The healthcare entity shall restrict access to program source code The healthcare entity shall: 1. Ensure that access to program source code is strictly based on need and is in compliance with entity access control policy	**Transitional**

UAE IA Reference: T7.5.1, T7.5.2, T7.5.3

SA 6	Outsourced Software Development

	Control Demands	Control Criteria Basic/Transitional/Advanced
SA 6.1	The healthcare entity shall supervise and have control over outsourced software development The healthcare entity shall: 1. Establish and enforce a secure coding policy 2. Define quality assurance processes 3. Include in the outsourced software development agreement the requirement to comply with: a. All relevant healthcare entity policies, including information security and quality related policies, requirements and functionalities b. Provisions of this Standard c. Regulatory and legal requirements d. Industry specific secure coding practices (OWASP) 4. Include in the agreement the right to audit clause 5. Conduct source code review to identify potential vulnerabilities, back-door and malicious code 6. Control the number, rotation and termination of staff involved in outsourced development activities to restrict: a. Unauthorized access b. Leakage of information	**Transitional**

UAE IA Reference: T7.6.5

SA 7	Supply Chain Management

Control Demands		Control Criteria Basic/Transitional/Advanced
SA 7.1	The healthcare entity shall develop a comprehensive information security strategy against supply chain threats to the information systems and application, medical devices and equipment The healthcare entity shall: 1. Define policy to regulate the acquisition of products and services 2. Limit sharing of configuration and architecture with suppliers 3. Define system acceptance criteria for all new system purchase 4. Ensure product compliance with entity information security requirements 5. Include in the contract: a. Right-to-Audit clause b. Non-disclosure requirements c. Terms to comply with entity information security policy and requirements d. Terms to comply with relevant federal and local government requirements	**Advanced**
SA 7.2	The healthcare entity shall conduct supplier review prior to entering into contractual agreement to acquire information systems, medical devices and system/devices components or information system services The healthcare entity shall: 1. Define an evaluation process for suppliers of information systems, system components, medical devices and services 2. Periodically review supplier compliance to terms of the agreement and evaluation requirements 3. Include federal and local government requirements as part of supplier review	**Advanced**
SA 7.3	The healthcare entity shall identify and limit harm from potential adversaries targeting the entity's supply chain The healthcare entity shall: 1. Limit information sharing with suppliers 2. When essential, share securely relevant and needed information through secure channel 3. Engage with a diverse set of suppliers for critical products and services	**Advanced**

SA 7.4	The healthcare entity shall employ security controls to protect supply chain operations The healthcare entity shall: 1. Evaluate risks to its information systems, medical devices, services and support operations 2. Agree with suppliers of systems, applications, medical devices equipment, related products/services on control measures and include them in the supplier contract	**Advanced**
SA 7.5	The healthcare entity shall ensure a reliable (i.e. not modified to provide back-door access or covert channels) delivery of information systems, medical devices or system/devices components The healthcare entity shall: 1. Ensure information systems, system components, and medical devices are genuine and are satisfying system acceptance requirements 2. Ensure software delivered has not been altered or modified	**Advanced**
SA 7.6	The healthcare entity shall establish processes to address weakness or deficiencies in supply chain elements The healthcare entity shall: 1. Identify and document supply chain elements and their interdependencies 2. Identify and address issues concerning supply chain elements 3. Conduct regular assessments and audits of supply chain elements	**Transitional**
SA 7.7	The healthcare entity shall ensure adequate supplies of critical information systems, medical devices and system/devices components The healthcare entity shall: 1. Establish contingency plans for the supply of any critical information systems, medical devices and system/devices components 2. Consider stockpiling of essential and critical spare components 3. Utilize multiple suppliers for critical components	**Advanced**

UAE IA Reference: T7.8.1, T7.8.2, T7.8.3, T7.8.4, T7.8.5, T7.8.6, T7.8.7

10. Information Security Incident Management

The value of information has grown exponentially and has become a soft target for malicious intent communities, individuals and nation states to disrupt an organization's ability to conduct and sustain business or to be in business, and to disrupt government's ability to provide services to its citizens and resident communities. Healthcare entities' utilization of technological advancement and innovation shall not be limited to service delivery; rather it shall also be to defend and respond to deliberate and accidental attempts to disrupt the entities' services.

A healthcare entity's ability to quickly and confidently respond to and restore service disruption attempts contributes the entity management's commitment to its vision and objective values towards service delivery. Healthcare entity's management shall be aware that information security incidents may not always be preventable. But adequate procedures, process and technologies to detect, report and handle, combined education and awareness can minimize their frequency, severity and impact on an entity's asset, reputation, financial and legal values.

It is essential that serious information security incidents that can potentially disrupt critical business processes and services are promptly communicated to the appropriate authorities so that they get involved early in the decision-making and communication.

Objective:

To ensure that healthcare entities define and utilize suitable processes and resources to identify and respond to information security and cyber security incidents, that they are not severely impacted by incident outcomes and that they are able to restore affected operations within an acceptable timeframe.

Supporting or dependent entity policy references:

1) Access Control Policy
2) Operations Management Policy
3) Communications Policy
4) Third party security policy
5) Compliance Policy

IM 1	Information Security Incident Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
IM 1.1	The healthcare entity shall develop, enforce and maintain an information security incident management policy, to manage and guide the entity's response to information security incidents The policy shall: 1. Be relevant and appropriate to the entity's operation and risk environment 2. Demonstrate management commitment, objectives and directions 3. Establish incident management roles and responsibilities 4. Establish a proactive, collaborative and sustainable process of identifying and resolving adverse information security incidents. 5. Establish management demands on: a. Incident identification b. Incident response c. Incident notification/communication d. Learning from incident 6. Be read and acknowledged by involved internal and external stakeholders	**Basic**

UAE IA Reference: T8.1.1

IM 2	Incident Management and Improvements

Control Demands		Control Criteria Basic/Transitional/Advanced
IM 2.1	The healthcare entity shall establish process(es) to guide information security and cyber security incident response activities The process(es) shall: 1. Have tested procedures to handle incident situations before, during and after the occurrence of the incident 2. Plan for incident communication to affected stakeholders and relevant authorities 3. Management approval on plans and procedures	**Transitional**
IM 2.2	The healthcare entity shall establish a Computer Security Incident Response Team (CSIRT) responsible for incident management and response efforts The healthcare entity shall: 1. Establish CSIRT organization with adequate authority, essential roles and responsibilities 2. Identify and nominate competent resources for each identified role of the CSIRT 3. Establish communication and response protocols 4. Allocate adequate funds for CSIRT operations 5. Entity CSIRT shall coordinate with its counterparts within the health sector regulator of Abu Dhabi for incidents which will have significant/severe impact on the entity's assets or operations 6. Ensure that significant/severe impact incidents are reported to the health sector regulator of Abu Dhabi 7. Provide suitable training to members of the CSIRT to cover: a. Past incidents and lessons learnt b. Current threat environment of the entity c. New threats and attack trends across the world	**Advanced**
IM 2.3	The healthcare entity shall assess and classify information security incidents The healthcare entity shall: 1. Establish an incident classification scheme in line with the recommendations of the health sector regulator of Abu Dhabi 2. Define workflows to handle incidents of various classifications/severity	**Transitional**

IM 2.4	The healthcare entity shall test its Computer Security incident response capabilities The healthcare entity shall: 1. Develop test procedures to validate the effectiveness of its incident response capabilities 2. Establish the expected outcome of test and compare test results to identify gaps 3. Modify process and procedures to address gaps identified	**Transitional**
IM 2.5	The healthcare entity shall document and preserve records on all information security incidents The healthcare entity shall: 1. Identify all relevant data and evidence to be collected during and after realization of an information security incident 2. Establish procedures for collecting evidence taking into account the: a. Chain of custody b. Safety of evidence c. Safety of personnel d. Roles and responsibilities of personnel involved e. Competency of the personnel f. Documentation g. Briefing h. Other identified requirements 3. Preserve documents, records and evidences in compliance with the entity's retention policy	**Transitional**
IM 2.6	The healthcare entity shall institutionalize the learning from information security incidents The healthcare entity shall: 1. Ensure lessons learnt from past information security incidents are maintained and shared with relevant stakeholders to aid in: a. Addressing future information security incidents b. Minimizing the recurrence of such incidents 2. Build knowledge database on information security incident diagnosis and response	**Advanced**

UAE IA Reference: T8.2.1, T8.2.2, T8.2.3, T8.2.4, T8.2.5, T8.2.7, T8.2.8, T8.2.9

IM 3	Information Security Events and Weakness Reporting

Control Demands		Control Criteria Basic/Transitional/Advanced
IM 3.1	The healthcare entity shall develop a situational awareness culture by participating in the information sharing community and obtaining cybersecurity information from various sources The healthcare entity shall: 1. Identify priority information and share it internally to build the entity's business model based-context 2. Ensure all identified cybersecurity information is relevant to the: a. Entity's business operations b. Entity's information system and application, medical devices and equipment c. Entity's processes and control environment d. Entity's risk environment 3. Establish and coordinate with the healthcare sector regulator of Abu Dhabi to receive relevant cybersecurity information	**Advanced**
IM 3.2	The healthcare entity shall report information security events through appropriate management channels The healthcare entity shall: 1. Establish a formal channel for entities and external stakeholders to report information security events 2. Ensure all employees and third parties are aware of the need for reporting of information security events and breaches 3. Assign designated points of contact for information security events 4. Establish information security event reporting procedures 5. Establish information security event communication and reporting protocol to relevant stakeholders and authorities (including the healthcare sector regulator)	**Advanced**

IM 3.3	The healthcare entity shall report observed or suspected information security weaknesses in systems or application services (inclusive of medical devices and equipment) The healthcare entity shall; 1. Establish a formal channel for entities and external stakeholders to report information security weakness as soon as they are identified 2. Ensure all employees and third parties are aware of the need for reporting of information security weakness 3. Ensure no user exploits information security weakness	**Advanced**

UAE IA Reference: T8.3.1, T8.3.2, T8.3.3

11. Information Systems Continuity Management

Information systems and applications have become fundamental to business operations. The ability of a healthcare entity's systems and applications to support identified critical services and processes would demonstrate the maturity of the healthcare entity's operational capabilities.

Even-though the demand on system and applications are identified through a different management process (Organizational Business Continuity), it is relevant for healthcare entities to align with such process to establish system, application and resource requirements concerning critical services and processes.

Healthcare entities shall be proactive in identifying threat scenarios that may impact their information systems and application environment, and device strategies and plans to ensure system, application and resource availability to support service continuity of identified critical services.

Objective:

To ensure systems, applications and resources are available to support service continuity requirements of identified critical services and processes during abnormal situations or environment.

Supporting or dependent entity policy references:

1) Entity Business Continuity Policy
2) Entity Business Continuity/Recovery Plan
3) Operations Management Policy
4) Communications Policy
5) Compliance Policy

SC 1	Information Systems Continuity Management Policy

Control Demands		Control Criteria Basic/Transitional/Advanced
SC 1.1	The healthcare entity shall develop, enforce and maintain an information system continuity planning policy to manage scenarios that challenge the continued availability of information systems and applications supporting critical business services The policy shall: 1. Be relevant and appropriate to the entity's information systems and applications continuity demands 2. Demonstrate management commitment, objectives and directions 3. Establish roles and responsibilities of involved stakeholders 4. Establish management expectations on: a. Planning for information system and application continuity during adverse situations b. Compliance with organizational business continuity plans c. Testing of continuity and restoration plans 5. Be read and acknowledged by involved internal and external stakeholders	**Transitional**

UAE IA Reference: T9.1.1

SC 2	Information Systems Continuity Planning

Control Demands		Control Criteria Basic/Transitional/Advanced
SC 2.1	The healthcare entity shall develop information systems and application continuity plans that shall prevent or minimize interruptions to critical business services and processes during adverse situations The plan shall: 1. Identify information systems, processes and information supporting critical business services and processes 2. Be harmonized and support organizational business continuity planning and/or disaster recovery demands 3. Identify individuals with assigned roles and responsibilities, along with necessary contact information 4. Define call tree matrix and escalation matrix 5. Defined criteria and conditions for plan activation 6. Have provisions to address information security incident based scenarios and provide guidance to operate and support critical business services during such scenarios	**Advanced**
SC 2.2	The healthcare entity shall implement the established information system and application continuity plans The healthcare entity shall: 1. Ensure that the capabilities and requirements of the information system and application continuity plans are established and available to be used during plan activation	**Advanced**
SC 2.3	The healthcare entity shall test, reassess and maintain its information systems and application continuity plans The healthcare entity shall: 1. Define schedules and test information system and application continuity plans to ensure: a. Adequacy and effectiveness of the plans b. Entity and resource readiness to execute the plans 2. Document test outcomes and lessons learned 3. Assess plan adequacy during changes to business services, systems and applications 4. Update and maintain information system and application continuity plans based on lessons learned and assessment outcome	**Advanced**

UAE IA Reference: T9.2.1, T9.2.2, T9.3.1

Appendix 1 - Distribution of Control

Sr. No.	Control Criteria	Number of Controls	Number of Sub-Controls	Total
1	Basic	73	255	328
2	Transitional	56	162	218
3	Advanced	33	113	146

Appendix 2 - Summary of Controls

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
Domain 1 - Human Resource Security				
HR 1 - Human Resources Security Policy				
HR 1.1	Security Aspects Of Employment and Termination	3	Basic	M3.1.1, M4.1.1
HR 2 - Prior to Employment				
HR 2.1	Background Verification Check	2	Basic	M4.2.1
HR 2.2	Terms and Condition of Employment	7	Basic	M4.2.2
HR 3 - During Employment				
HR 3.1	Compliance to Organizational Policies and Procedures	3	Basic	M4.3.1
HR 3.2	Awareness and Training	4	Transitional	M3.2.1, M3.3.3, M3.3.4, M3.3.5
HR 3.3	Training Needs	2	Basic	M3.3.1, M3.3.2
HR 3.4	Awareness Campaign	9	Basic	M3.4.1
HR 3.5	Disciplinary Process	2	Transitional	M4.3.2
HR 4 - Termination or Change of Employment and Role				
HR 4.1	Termination Responsibility	2	Basic	M4.4.1
HR 4.2	Return of Assets	3	Basic	M4.4.2
HR 4.3	Removal of Access Rights	2	Basic	M4.4.3
HR 4.4	Internal Transfers and Change Of Role	2	Basic	M4.4.3
Domain 2 - Asset Management				
AM 1 Asset Management Policy				
AM 1.1.	Asset Management Policy	8	Basic	T1.1.1
AM 1.2	Allocation of Assets	5	Basic	T1.1.1
AM 2 Management of Asset				
AM 2.1	Asset Inventory	3	Basic	T1.2.1
AM 2.2	Asset Ownership	4	Basic	T1.2.2

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
AM 2.3	Acceptable Use of Asset	2	Basic	T1.2.3
AM 2.4	Acceptable Bring Your Own Device Arrangements	2	Basic	T1.2.4
AM 3	**Asset Classification & Labelling**			
AM 3.1	Information Classification	NA	Basic	T1.3.1
AM 3.2	Value of Information during Classification	NA	Transitional	T1.3.1
AM 3.3	Identification of Essential Protection	NA	Transitional	T1.3.1
AM 3.4	Reclassification of Assets	3	Transitional	T1.3.1
AM 3.5	Interpretation of Third Party Classification Scheme	NA	Transitional	T1.3.1
AM 3.6	Criteria for Automated Classification	NA	Advanced	T1.3.1
AM 3.7	Asset Labelling	NA	Basic	T1.3.2
AM 4	**Asset Handling**			
AM 4.1	Handling Procedures	2	Basic	T1.3.3
AM 4.2	Enforcement of Handling Procedures	NA	Basic	T1.3.3
AM 4.3	Management of Removable Media	2	Basic	T1.4.1
AM 4.4	Usage of Removable Media	1	Basic	T1.4.1
AM 4.5	Medical Devices Management Procedures	NA	Basic	-
AM 4.6	Access Allocation for Medical Devices	NA	Basic	-
AM 4.7	Security of Information within Medical Devices	4	Transitional	-
AM 4.8	Communication Facility for Medical Devices	NA	Transitional	-
AM 4.9	Removable Media Security	NA	Advance	T1.4.1
AM 4.10	Removal and Movement of Information Assets	2	Transitional	T2.3.7
AM 5	**Asset Disposal**			
AM 5.1	Information Asset Disposal	NA	Basic	T1.4.2
AM 5.2	Secure Disposal	NA	Basic	T1.4.2
AM 5.3	Disposal of Physical & Digital Media	NA	Basic	T1.4.2
AM 5.4	Procedures for Secure Disposal and Re-Use	1	Transitional	T1.4.2 T2.3.6

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
AM 5.5	Verification before Disposal	NA	Basic	T1.4.2
AM 5.6	Authorization for Disposal	NA	Basic	T1.4.2
AM 5.7	Records on Disposal	NA	Advance	T2.3.6 T.1.4.2
Domain 3 - Physical and Environmental Security				
PE 1	**Physical and Environmental Security Policy**			
PE 1.1	Physical and Environmental Security Policy	7	Basic	T2.1.1, T2.3.5
PE 1.2	Procedural Guidelines	NA	Transitional	T2.1.1
PE 1.3	Requirements on Physical and Environmental Policy	3	Basic	T2.1.1
PE 2	**Secure Areas**			
PE 2.1	Physical Security Perimeter	4	Basic	T2.2.1
PE 2.2	Private Areas	NA	Advanced	
PE 2.3	Secure Areas Control Measures	8	Basic	T2.2.2
PE 2.4	Ownership of Secure Areas	3	Transitional	
PE 2.5	Secure Office /Meeting Rooms	2	Basic	T2.2.3
PE 2.6	Protection against External & Environmental Threats	2	Basic	T2.2.4
PE 2.7	Adequacy/Effectiveness of Control Measures	NA	Transitional	T2.2.4
PE 2.8	Working in Secure Areas	2	Basic	T2.2.5
PE 2.9	Stakeholder Awareness	1	Transitional	T2.2.5
PE 2.10	Deliver and Loading Areas	2	Basic	T2.2.6
PE 3	**Equipment Security**			
PE 3.1	Equipment Siting and Protection	2	Basic	T2.3.1
PE 3.2	Supporting Utilities	1	Transitional	T2.3.2
PE 3.3	Maintenance of Equipment	3	Advance	T2.3.4
PE 3.4	Cabling Security	2	Basic	T2.3.3
PE 3.5	Security Of Equipment Off Site	3	Advanced	T2.3.5, T2.3.7
PE 3.6	Unattended User Equipment	2	Basic	T2.3.8

Sr. No Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
PE 3.7 Clear Desk & Clear Screen Policy	3	Basic	T2.3.9
Domain 4 - Access Control			
AC 1 Access Control Policy			
AC 1.1 Access Control Policy	13	Basic	T5.1.1
AC 2 User Access Management			
AC 2.1 User Registration and De-Registration	7	Basic	T5.2.1
AC 2.2 Privilege Management	7	Advance	T5.2.2
AC 2.3 Use and Management of Security Credential	7	Basic	T5.2.3, T5.3.1, T5.5.3
AC3 Equipment and Devices Access Control			
AC 3.1 Access Control for Portable and Medical Devices	5	Transitional	T5.7.1
AC 3.2 Access Control for Assets and Equipment in Teleworking Sites	4	Transitional	T5.7.2
AC 4 Access Reviews			
Ac 4.1 Review of User Access Rights	5	Basic	T5.2.4
AC 5 Network Access Control			
Ac 5.1 Access to Network and Network Services	NA	Basic	T5.4.1
AC 5.2 Remote User Authentication	2	Basic	T5.4.2
AC 5.3 Equipment Identification In Network	NA	Basic	T5.4.3
AC 5.4 Remote Diagnostic and Configuration Protection	4	Advanced	T5.4.4
AC 5.5 Network Connection Control	1	Basic	T5.4.5
AC 5.6 Network Routing Control	7	Transitional	T5.4.6
AC 5.7 Wireless Access	7	Transitional	T5.4.7
AC 6 Operating System Access Control			
AC 6.1 Secure Log-On Procedures	6	Basic	T5.5.1
AC 6.2 User Identification and Authentication	2	Basic	T5.5.2
AC 6.3 Use of System Utilities	4	Advanced	T5.5.4

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
AC 7 Application and Information Access Control				
AC 7.1	Information Access Restriction	4	Basic	T5.6.1
AC 7.2	Sensitive System Isolation	NA	Transitional	T5.6.2
AC 7.3	Publicly Accessible Content	4	Transitional	T5.6.3
Domain 5 - Operations Management				
OM 1 Operations Management Policy				
OM 1.1	Operations Management Policy	3	Basic	T3.1.1
OM 2 Operational Procedures				
OM 2.1	Baseline Configuration	5	Transitional	T3.2.1
OM 2.2	Documented Operating Procedure	3	Transitional	T3.2.2
OM 2.3	Change Management	3	Basic	T3.2.3
OM 2.4	Transition of Information Systems and Applications	1	Transitional	T3.2.3
OM 2.5	Segregation of Duties	1	Transitional	T3.2.4
OM 2.6	Separation of Test, Development and Operational Environment	4	Transitional	T3.2.5
OM 3 Planning and Acceptance				
OM 3.1	Capacity Management	4	Advanced	T3.3.1
OM 3.2	System Acceptance and Testing	5	Transitional	T3.3.2
OM 4 Malware Protection				
OM 4.1	Controls Against Malware	9	Basic	T3.4.1
OM 4.2	Gateway Level Protection for Malware	2	Advanced	T3.4.1
OM 5 Backup and Archival				
OM 5.1	Backup Management	3	Basic	T3.5.1
OM 5.2	Archival Requirements	6	Advanced	T3.5.1
OM 6 Monitoring and Logging				
OM 6.1	Monitoring Procedures	7	Basic	T3.6.1 T3.6.3
OM 6.2	Audit Logging	6	Basic	T3.6.2 T3.6.5 T3.6.6

Sr. No Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
OM 6.3 Preservation of Log Information	4	Advanced	T3.6.4
OM 6.4 Clock Synchronization	3	Basic	T3.6.7
OM 6.5 Patch Management	6	Basic	T7.7.1
OM 6.6 Information Leakage	1	Transitional	T7.6.4
OM 7 Security Assessment and Vulnerability Management			
OM 7.1 Technical Vulnerability Assessment	6	Basic	T7.7.1
OM 7.2 Security of Assessment Data	3	Basic	T7.7.1
Domain 6 - Communications			
CM 1 Communications Policy			
CM 1.1 Communication Policy	4	Basic	T4.1.1
CM 2 Information Exchange			
CM 2.1 Information Exchange Procedures	4	Transitional	T4.2.1
CM 2.2 Security of Information During Transit	2	Basic	T4.2.1
CM 2.3 Secure Practices for Information Sharing	4	Basic	T4.2.2
CM 2.4 Agreements on Information Transfer	5	Basic	T4.2.2
CM 2.5 External Party Awareness of Security Requirements	1	Transitional	T4.2.2
CM 2.6 Physical Media in Transit	4	Transitional	T4.2.3
CM 2.7 Electronic Messaging	4	Transitional	T4.2.4
CM 2.8 Business Information System	2	Advanced	T4.2.5
CM 3 Electronic Commerce			
CM 3.1 Security of Electronic Commerce Services	3	Transitional	T4.3.1
CM 3.2 Online Transaction	3	Transitional	T4.3.2
CM 3.3 Publicly Available Information	5	Advanced	T4.3.3
CM 4 Information Sharing Platforms			
CM 4.1 Connectivity to Information Sharing Platforms	4	Advanced	T4.4.1, T4.4.2
CM 4.2 Restriction on Cloud Environment	3	Basic	T6.3.1
CM 4.3 Security While Connecting to Information Sharing Platform	4	Basic	T4.4.1

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
CM 5 Network Security Management				
CM 5.1	Network Controls	7	Basic	T4.5.1
CM 5.2	Security Requirements in Network Services	4	Transitional	T4.5.2
CM 5.3	Segregation in Networks	4	Basic	T4.5.3
CM 5.4	Security of Wireless Networks	5	Basic	T4.5.4
Domain 7 - Health Information and Security				
HI1 Health Information Protection Policy				
HI 1.1	Health Information Protection Policy	4	Basic	M5.2.4
HI2 Health Information Privacy and Protection				
HI 2.1	Security of Healthcare Information	11	Basic	M5.2.4
Domain 8 - Third Party Security				
TP 1 Third Party Security Policy				
TP 1.1	Third Party Security Policy	5	Basic	T6.1.1
TP 2 Third Party Service Delivery and Monitoring				
TP 2.1	Third-Party Service Delivery	8	Basic	T6.2.1
TP 2.2	Monitoring and Review of Third-Party Services	6	Transitional	T6.2.2
TP 2.3	Managing Changes to Third Party Services	3	Transitional	T6.2.3
Domain 9 - Information Systems Acquisition, Development, and Maintenance				
SA 1 Information Systems Acquisition, Development, and Maintenance Policy				
SA 1.1	Information Systems Acquisition, Development and Maintenance Policy	5	**Basic**	T7.1.1 T7.4.1
SA 2 Security Requirement of Information Systems and Applications				
SA 2.1	Security Requirements Analysis and Specification	7	Transitional	T7.2.1
SA 2.2	Developer Training	5	Transitional	T7.2.2
SA 3 Correct Processing in Applications				
SA 3.1	Input Data Validation	2	Transitional	T7.3.1
SA 3.2	Control of Internal Processing	3	Transitional	T7.3.2
SA 3.3	Message Integrity	1	Transitional	T7.3.3

Sr. No Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
SA 3.4 Output Data Validation	1	Transitional	T7.3.4
SA 3.5 Off-line Processing Capabilities	1	Transitional	T7.3.2
SA 4 Cryptographic Controls			
SA 4.1 Key Management	3	Transitional	T7.4.2
SA 5 Security of System Files			
SA 5.1 Control of Operational Software	3	Advanced	T7.5.1
SA 5.2 Protection of System Test Data	5	Transitional	T7.5.2
SA 5.3 Access Control to Program Source Code	1	Transitional	T7.5.3
SA 6 Outsourced Software Development			
SA 6.1 Outsourced Software Development	6	Transitional	T7.6.5
SA 7 Supply Chain Management			
SA 7.1 Supply Chain Protection Strategy	5	Advanced	T7.8.1
SA 7.2 Supplier Reviews	3	Advanced	T7.8.2
SA 7.3 Limitation of Harm	3	Advanced	T7.8.3
SA 7.4 Supply Chain Operation Security	2	Advanced	T7.8.4
SA 7.5 Reliable Delivery of Items and Services	2	Advanced	T7.8.5
SA 7.6 Process to Address Weakness or deficiency	3	Transitional	T7.8.6
SA 7.7 Supply of Critical Information System Component	3	Advanced	T7.8.7
Domain 10 - Information Security Incident Management			
IM 1 Information Security Incident Policy			
IM 1.1 Information Security Incident Management Policy	6	Basic	T8.1.1
IM 2 Incident Management and Improvements			
IM 2.1 Incident Response Process	3	Transitional	T8.2.1
IM 2.2 Computer Security Incident Response Team	7	Advanced	T8.2.2
IM 2.3 Incident Classification	2	Transitional	T8.2.3
IM 2.4 Incident Response Testing	3	Transitional	T8.2.5

Sr. No	Control Number & Control Name	Number of Sub-Control	Control Criteria	UAE IA Reference
IM 2.5	Incident Records	3	Transitional	T8.2.7 T8.2.9
IM 2.6	Learning from Information Security Incident	2	Advanced	T8.2.4, T8.2.8
IM 3 Information Security Events and Weakness Reporting				
IM 3.1	Situational Awareness	3	Advanced	T8.3.1
IM 3.2	Reporting Information Security Events	5	Advanced	T8.3.2
IM 3.3	Reporting Security Weakness	3	Advanced	T8.3.3
Domain 11 - Information Systems Continuity Management				
SC 1 Information Systems Continuity Management Policy				
SC 1.1	Information Systems Continuity Management Policy	5	Transitional	T9.1.1
SC 2 Information Systems Continuity Planning				
SC 2.1	Developing Information System and Application Continuity Plans	6	Advanced	T9.2.1
SC 2.2	Implementing Information System and Application Continuity Plans	1	Advance	T9.2.2
SC 2.3	Testing, Maintaining and Reassessing Plans	4	Advanced	T9.3.1

Appendix 3 - Abbreviations

S.No	Abbreviation	Definition
1.	ADHICS	Abu Dhabi Health Information and Cyber Security Standard
2.	BIA	Business Impact Assessment
3.	CISO	Chief Information Security Officer
4.	IT	Information Technology
5.	ISO 27001	International standard for Information Security
6.	ISMS	Information Security Management System
7.	ISO 31000	Risk Management Standard
8.	DLP	Data Leakage Prevention
9.	HIIP	Healthcare Information Infrastructure Protection Workgroup
10.	HIE	Health Information Exchange
11.	AAA	Authenticity, Accountability and Auditability
12.	IPR	Intellectual Property Rights
14.	ISGC	Information Security Governance Committee
15.	HVAC	Heating, ventilation and air conditioning
16.	BYOD	Bring Your Own Device
17.	ERP	Enterprise Resource Planning
18.	EMR	Electronic Medical Records
19.	CCTV	Closed-Circuit Television
20.	PII	Personally identifiable information
21.	OWASP	Open Web Application Security Project
22.	HR	Human Resource
23.	MCC	Monitoring and Control Centre – Abu Dhabi
24.	SDLC	Software Development Life Cycle
25.	DMZ	Demilitarised Zone
26.	IDS	Intrusion Detection System
27.	QA	Quality Assurance

S.No	Abbreviation	Definition
28.	XSS	Cross-Site Scripting
29.	CWE	Common Weakness Enumeration
30.	SQL	Structure Query Language
31.	TCP	Transmission control protocol
32.	VPN	Virtual Private Network
33.	ACL	Access Control List
34.	DOS	Denial of Service
35.	CAB	Change Advisory Board
36.	IPS	Intrusion Prevention System
37.	VLAN	Virtual Local Area Network
38.	NDA	Non-Disclosure Agreement
39.	NTP	Network Time Protocol
40.	PIN	Personal Identification Number
41.	HTTPS	Hyper Text Transfer Protocol Security
42.	CIA	Confidentiality, Integrity & Availability
43.	DNS	Domain Name System
44.	IT	Information Technology
45.	SMTP	Simple Mail Transfer Protocol
46.	SNMP	Simple Network Management Protocol
47.	PHI	Protected Health Information

Appendix 4 - Glossary

The table below defines the terms and acronyms used for the purposes of this framework.

Term	Definition
Adversaries	Person or group contending against another
Assets	Data or images collected and stored (in a digital or hard copy format) and the information systems that are used to collect, store or exchange these data or images.
Authentication	Establishing that an agent using a computer system is the agent in whose name the account is registered.
Availability	Information is accessible and useable on demand by authorised entities.
Backup (noun)	The process of backing up refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. A backup and the associated procedures and processes can only be verified once the restore procedures and process have been confirmed via an actual restore.
Back up (verb)	To make a copy of data for the purpose of recovery.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Classification	Accords different levels of protection based on the expected damage, prejudice and/or loss the health information might cause in the wrong hands.
Confidentiality	Information is not available or disclosed to unauthorised individuals, entities, or processes.
Cryptography	The science of coding and decoding messages so as to keep these messages secure. Coding (encryption) takes place using a key that ideally is known only by the sender and intended recipient of the message. Cryptographic control is the ability to render plain text unreadable and re-readable using cryptographic techniques. Such techniques are also used to ensure integrity and non-repudiation.
Custodian	In the health information security context a custodian is a person in an appointed role that is entrusted with the custody or care of a person's health information. A healthcare entity may have custodianship over health care information.
Data integrity	Data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes.

Term	Definition
Disaster recovery (DR)	Disaster recovery is the process, policies and procedures related to preparing for recovery critical to an organisation after a natural or human-induced disruptive event. Disaster recovery planning is a subset of a larger process known as business continuity management (BCM). This includes planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure.
Disruptive event	Any event, regardless of cause, that disrupts (or has the potential to disrupt) an organisation's ability to maintain identified critical functions.
Entity	Refers to Healthcare Entity, unless specifically mentioned otherwise.
Environmental (threats/hazards)	Threats or risks of physical harm. From an IT security viewpoint this is to do with physical access to or potential physical risks to hardware
Facility	A single physical location from which health goods and/or services are provided. A health care organisation may consist of multiple facilities
Firewall	A device or set of devices configured to permit, deny, encrypt or proxy all computer traffic between different security domains based upon a set of rules and other criteria.
Healthcare entity (provider)	A person, facility or organisation providing patient health care services, including services to promote health, to protect health, to prevent disease or ill-health, treatment services, nursing services, rehabilitative services or diagnostic services.
Medical device	An article, instrument, apparatus or machine that is used in the prevention, diagnosis or treatment of illness or disease, or for detecting, measuring, restoring, correcting or modifying the structure or function of the body for some health purpose. Typically, the purpose of a medical device is not achieved by pharmacological, immunological or metabolic means
Medical equipment	Medical devices requiring calibration, maintenance, repair, user training, and decommissioning – activities usually managed by clinical engineers. Medical equipment is used for the specific purposes of diagnosis and treatment of disease or rehabilitation following disease or injury; it can be used either alone or in combination with any accessory, consumable, or other piece of medical equipment. Medical equipment excludes implantable, disposable or single-use medical devices.
Malware	Software developed for malicious intent. This includes viruses, worms, adware, Trojan horses, key-loggers.
Media	Any technology used to place, keep, transport and or retrieve data. This includes both electronic devices and materials as well as non-electronic options eg, paper.
Personal health information	Personal health information is health information identifiable to an individual.

Term	Definition
Portable media	Media that can be used to transport electronic information independently of a network. This includes floppy disks, USB storage, portable hard-drives and other devices that have a data storage mechanism (cameras, cell phones, iPods etc.)
Professional	An individual who is engaged in a health care related occupation.
Privacy Impact Assessment (PIA)	An analysis of how an individual's or groups of individuals' personally identifiable information is collected, used, shared and maintained by an organisation.
Procedure	A specification or series of actions, acts or operations which have to be executed in the same manner in order to always obtain the same result in the same circumstances (eg emergency procedures).
Risk management	The identification, assessment, and prioritisation of risks including using resources to minimise, monitor, and control the impact of these risks.
Service level agreements (SLA)	A formally negotiated agreement between two parties that records the common understanding about services, priorities, responsibilities, guarantee, and such collectively, the level of service.
Standard	Unless specified otherwise, the term refers to ADHICS Standard
Systems	Applications or electronic business processes which support the collection, access, processing and exchange of personal health information
Teleworking	A work arrangement in which employees are able to have flexibility in their working location. That is: a central place of work is supplemented by a remote location (eg, home), usually with the aid of information technology and communications.
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. Viruses usually corrupt or modify files on a targeted computer.

Appendix 5 - References

- UAE Information Assurance Standards
- ISO/IEC 27001:2013
- Information Security Governance – A Practical Development and Implementation Approach, by Krag Brotby