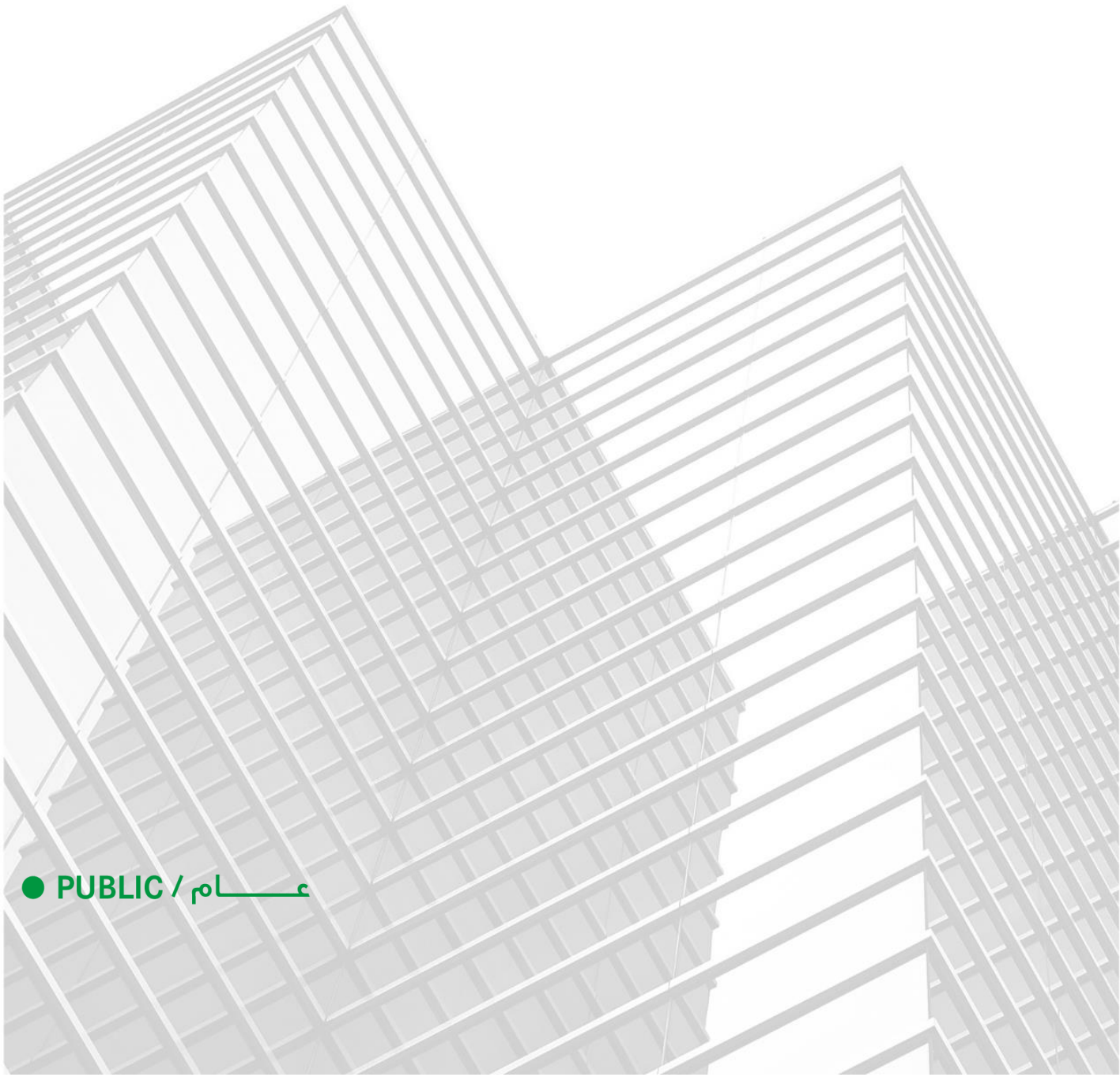
دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

Abu Dhabi Healthcare Information and Cyber Security Standard



● PUBLIC / عـــــــام

Document Title:	Abu Dhabi - Healthcare Information and Cyber Security Standard		
Document Ref. Number:	DOH/SD/ICSO/ADHICS/V2/2024	Version:	V2
New / Revised:	Revised		
Publication Date:	May, 2024		
Effective Date:	August, 2024		
Document Control:	Department of Health (DoH) - The Health Sector Regulator in the Emirate of Abu Dhabi		
Applies To:	Any entity Including but not limited to, Healthcare Facility, Payer, Healthcare Technology and Service Provider in the Emirate of Abu Dhabi that generate, access, store, use, process and/or transmit health information.		
Owner:	DoH Information & Cyber Security Office		
Revision Date:	May, 2027		
Revision Period:	Three years from publication date		
Contact:	DoH Information & Cyber Security Office: is@doh.gov.ae		

1.Standard Scope

The scope of Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS):

a) Any health sector (referred to as "entity") including but not limited to, Healthcare Facility, Payer, Service Provider in the Emirate of Abu Dhabi that generate, access, store, use, process and/or transmit health information.
b) Any healthcare professional or other/support staff who has access to patient's health/diagnostic/personal information.
c) All information (in physical and digital forms), medical device and equipment, applications and software, infrastructure, information system, physical infrastructure (data center, access barriers, electrical facilities, HVAC systems, secure areas, etc.) and human resources (in support of care delivery).
d) Any/all systems and applications fully owned by entity, as well as entity's access and usage of partners' and third-party systems and applications utilized within Abu Dhabi Healthcare ecosystem e.g., Shafafiya, Health information Exchange Platform, Electronic Medical Records, Web and Mobile Application etc.
e) 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 health information security that protects the information's confidentiality, integrity, and availability. The entity shall consider applicable laws, Federal/National and Local demands, regulatory requirements, and own risk management while establishing and operating information security and data privacy mandates.

The development and application of additional information security policies and procedures, or as required by this Standard, is the responsibility of the entity.

2. Definitions and Abbreviations

No.	Term / Abbreviation	Definition
2.1	TCP	Transmission control protocol
2.2	ACL	Access Control List
2.3	DOS	Denial of Service
2.4	CAB	Change Advisory Board
2.5	IPS	Intrusion Prevention System
2.6	VLAN	Virtual Local Area Network
2.7	NDA	Non-Disclosure Agreement
2.8	NTP	Network Time Protocol
2.9	PIN	Personal Identification Number
2.10	HTTPS	Hyper Text Transfer Protocol Security
2.11	CIA	Confidentiality, Integrity & Availability
2.12	DNS	Domain Name System
2.13	UDP	User Datagram Protocol
2.14	RPO	Recovery Point Objective
2.15	RTO	Recovery Time Objective
2.16	Adversaries	Person or group contending against another
2.17	Asset Custodian	Employee within an organization who is responsible for physically safeguarding and maintaining an asset. The asset custodian is responsible for the day-to-day management of physical IT assets, such as computers, servers, and mobile devices. They are responsible for ensuring that these assets are properly stored, maintained, and accounted for throughout their lifecycle. They are accountable for the physical security and maintenance of the asset.
2.18	Asset Owner	An asset owner is the individual or department within an organization who is responsible for managing a particular asset throughout its lifecycle. The asset owner is responsible for making decisions about the asset, such as

		when to upgrade or replace it, ensuring that it is properly maintained, secured, and used effectively to achieve the organization's goals.
2.19	Assets	Data or images collected and stored (in a digital or hard copy format) and the information systems that are used to generate, collect, store or exchange these data or images and/or support in entity operations for care delivery
2.20	Authentication	Establishing that an agent using a computer system is the agent in whose name the account is registered.
2.21	Availability	Information is accessible and useable on demand by authorized entities.
2.22	Back up (verb)	To make a copy of data for the purpose of recovery.
2.23	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.
2.24	Business Continuity Plan (BCP)	Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
2.25	Classification	Accords different levels of protection based on the expected damage, prejudice and/or loss the health information might cause in the wrong hands.
2.26	Cloud Environment	Computer resources housed in a distant data center and controlled by a cloud services provider, such as programs, servers (both physical and virtual), data storage, development tools, networking capabilities, and more.
2.27	Confidentiality	Information is not available or disclosed to unauthorized individuals, entities, or processes.
2.28	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.
2.29	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. An entity may have custodianship over health care information.
2.30	Data integrity	Data must not be altered or destroyed in an unauthorized manner and accuracy and consistency must be preserved regardless of changes.

2.31	Data Privacy Impact Assessment (DPIA)	Assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes protected health information for taking actions as necessary to treat privacy risk
2.32	Data Subject	A natural person about whom the entity holds protected health information and who can be identified, directly or indirectly, by reference to that information
2.33	Disaster recovery (DR)	Disaster recovery is the process, policies and procedures related to preparing for recovery critical to an organization 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. 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.
2.34	Disruptive event	Any event, regardless of cause, that disrupts (or has the potential to disrupt) an organization's ability to maintain identified critical functions.
2.35	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
2.36	Facility	A single physical location from which health goods and/or services are provided. A health care organization may consist of multiple facilities
2.37	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.
2.38	Health information	Information regarding the health of a subject of care in physical and/or computer-processable form. It can be present as text, video, audio, photos and images.
2.39	Health Information Exchange (HIE)	Malaffi - that safely and securely connects public and private healthcare providers in the Emirate of Abu Dhabi
2.40	Health Sector Entity	Herein referred to as "entity" Including but not limited to, Healthcare Facility, Payer, Service Provider in the Emirate of Abu Dhabi that generate, access, store, use, process and/or transmit health information
2.41	Healthcare Facility	A 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

2.42	Healthcare Technology and Service Providers	Any external party that provides medical device, system, application, infrastructure or database, both individually or collectively that generate, access, store, use, process and/or transmit health information
2.43	Key Management	Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding and replacement of keys.
2.44	Malware	Software developed for malicious intent. This includes viruses, worms, adware, Trojan horses, key-loggers.
2.45	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 e.g., paper.
2.46	Medical device	An article, material, instrument, implant, software, apparatus, or machine to be used, alone or in combination for 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. Some medical devices have the capability to collect, record data and to transmit over the internet and to other devices that are equipped to receive said data
2.47	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.
2.48	Patient / Subject of care	One or more persons scheduled to receive, receiving, or having received a health service
2.49	Payers	Insurers, Third Party Administrators and Brokers that provide operational services such as health insurance, Claims processing, Policy benefits management etc.
2.50	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.)
2.51	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 (e.g., emergency procedures).
2.52	Professional	An individual who is engaged in a health care related occupation.

2.53	Personally Identifiable Information (PII)	Personally identifiable information (PII) is any data that could potentially identify a specific individual
2.54	Protected health Information (PHI)	Protected health information (PHI), also referred to as personal health information, is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.
2.55	Recovery Point Objective (RPO)	Point in time to which data are to be recovered after a disruption has occurred
2.56	Recovery Time Objective (RTO)	Period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions are to be recovered after a disruption has occurred
2.57	Risk management	The identification, assessment, and prioritization of risks including using resources to minimize, monitor, and control the impact of these risks.
2.58	Secure Coding	The practice of developing software that is safeguarded from security vulnerabilities.
2.59	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.
2.60	Standard	Unless specified otherwise, the term refers to ADHICS Standard
2.61	Supply Chain	The sequence of processes involved in the production and distribution of a product or a service
2.62	Systems	Applications or electronic business processes which support the collection, access, processing and exchange of health information
2.63	Telehealth	The use of electronic information and communication technologies to support long-distance virtual clinical healthcare practice, patient and professional health-related education, public health and health administration
2.64	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 (e.g., home), usually with the aid of information technology and communications.
2.65	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.

Section A

Introduction, Governance and Framework Definition

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

1.1 Introduction

Information and cyber security requirements are dynamic and ever evolving with technological advancement and service capabilities. This document demonstrates the Abu Dhabi Government's commitment towards health information and cyber security, and identifies requirements and enhancements needed to establish a cybersecure healthcare ecosystem. This document shall be formerly referred as Abu Dhabi Health information and Cyber Security (ADHICS) Standard – Version 2 or ADHICS V2.

ADHICS V2 is aligned with the strategic demands of Abu Dhabi Healthcare information and Cybersecurity Strategy, published in the year 2021, and supersedes the mandates provided by Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard V 0.9 of 2019, Internet of Medical Things (IoMT) Security Standard V 0.9 of 2020 and Standard on Patient Healthcare Data Privacy V 0.9 of 2020, published by Department of Health.

The provisions of this standard are harmonized with industry and international expectations towards health information and cyber security, and it intends to ensure entities demonstrate their Information and Cybersecurity compliance efficiently and address the specific management needs of the health sector in their unique operating environments. The adoption of ADHICS V2 Standard by entities will facilitate secure usage of medical technology and exchange of information, maintaining public trust in healthcare operations and Government's initiatives towards healthcare delivery.

1.2 Document Organization

This document is organized in two sections:

a) "Section – A" defines the introductory, governance and framework aspects of the Abu Dhabi Healthcare information and cyber security program.

b) "Section – B" documents the control requirements of ADHICS - Version 2.

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 efforts to understand the demands, define Abu Dhabi Health Sector-specific Information and Cyber Security requirements, and define timelines towards compliance.

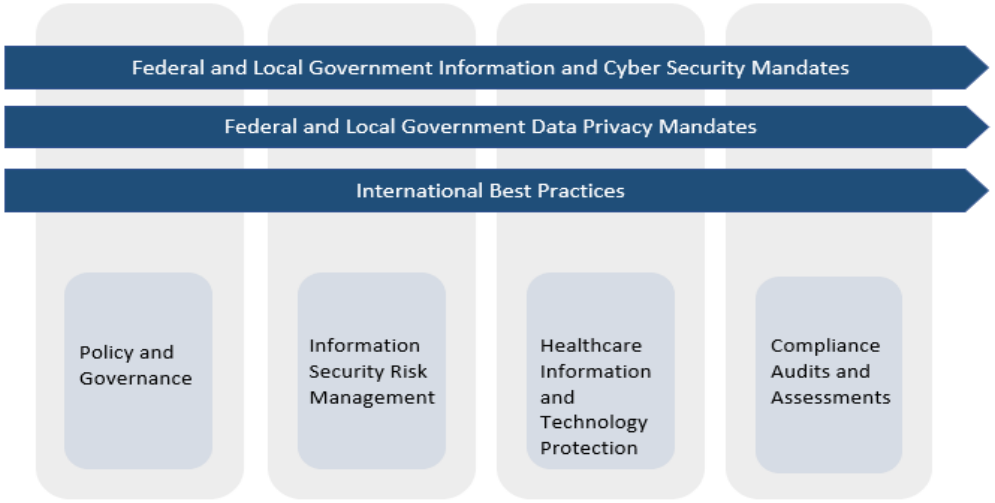


Figure 1: Abu Dhabi Healthcare Information and Cyber Security Standard – Relational Representation

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

1.4 Purpose and Background

Evolving cyberthreats pose greater threats to healthcare entities that can put patient and patient data at security risk. Aligning cybersecurity with entity operations will not only protect patient safety and privacy, but will also ensure continuity of high-quality care delivery, by minimizing risk probabilities and enhancing public trust and clinical outcomes. As health information is critical for individuals, it remains a key to unlock treasure for cyber criminals. It is critical that entities and professionals, inclusive of management/support/administrative/clerical staff members:

a) Ensure confidentiality and maintain privacy of subjects-of-care.

b) Protect the integrity/accuracy and quality of health information, to ensure patient safety and that such information remains valid and auditable throughout its life cycle.

c) 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

d) Ensure that the entity meets unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks.

ADHICS V2 Standard outlines the control mandates essential to protect health information during its creation, maintenance, access, disclosure, processing, usage, storage, transmission, and disposal, and to maintain the information's confidentiality, integrity, and availability (including authenticity, accountability, and auditability). The standard establishes process and control demands that should be incorporated and sets out requirements and desired goals at various levels of an entity's maturity, operational complexity, and risk environment.

1.5 Benefits

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

a) Comprehensive risk management and compliance towards Health information security mandates and practices.

b) Protect entity's reputation and build patient trust in entity operations health information.

c) Minimize entity's network exposure to unauthorized accesses by adopting policies and procedures.

d) Increased predictability of technology compromises and reduced uncertainty of business operations by lowering information security-related risks to an acceptable level.

e) Safer use of medical devices and equipment for fast, efficient, and secure operations.

f) Secure digital transformation empowering entity to operate more efficiently, intelligently, and effectively.

g) Minimize compliance failures in third-party and cloud services by incorporating security requirements as part of their lifecycles.

h) Increased staff awareness on cybersecurity practices and due diligence to detect and prevent cyber-attacks.

i) Avoid non-compliance penalties, by thoroughly evaluating the processes and technical infrastructure for security gaps.

j) Contribute in DoH initiatives towards strengthening information security landscape of the health sector of the emirate.

k) Avoid financial loss that is mostly due to theft of Personally Identifiable Information (PII and PHI) investigation and Forensics, operational disruption, lost value of patient relationships, loss of intellectual property by taking into consideration the accepted global benchmark for the effective management of information assets.

l) Enable better and secure ways to process health related electronic transactions.

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

2.1 Entity Governance Structure

Information security governance is a subset of organizational governance. It shall resonate with Federal and Local Government mandates and shall be aligned with the principles of organizational governance. The role of information security governance is, to provide management oversight and direction on information and cyber security initiatives, challenges and risk The establishment of Healthcare information Infrastructure Protection (HIIP) Workgroup at Abu Dhabi Health Sector level, with participation from all sector operators and/or healthcare entities, is essential to ensure collaboration and coordination of efforts towards successful Program implementation and progression across Abu Dhabi Health Sector.

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.

ADHICS Program's Governance structure, to achieve success demands a comprehensive security strategy that is explicitly linked to the corporate strategy and business processes. Information security shall be an integral component of enterprise governance, and integrated into corporate strategy, concept, design, implementation, and operation.

The entity, regardless of its type, shall implement Governance structure along the tiers as defined below:

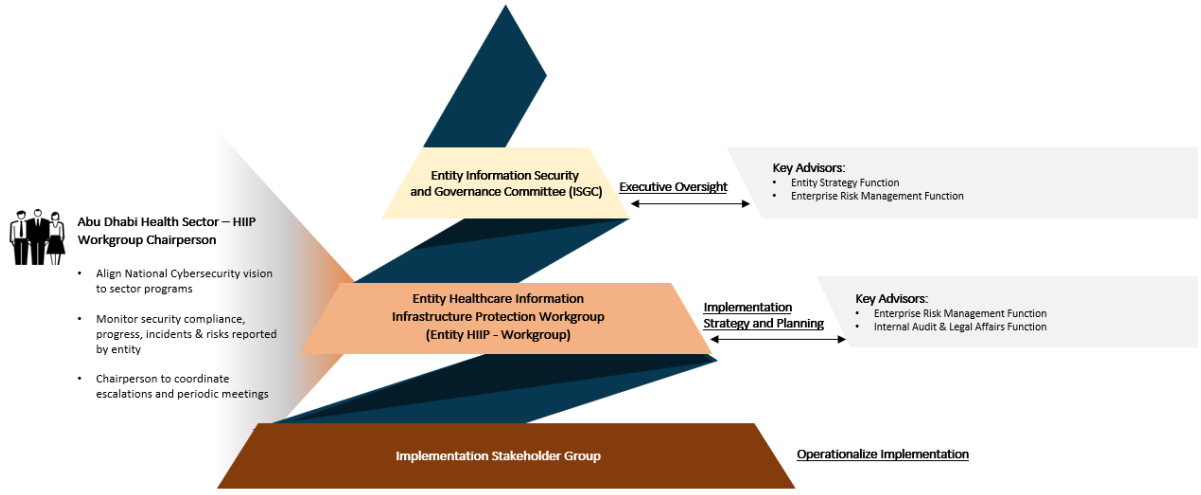


Figure 2: ADHICS Governance Pyramid

The committees of the ADHICS Governance pyramid can be scaled down to match smaller entities provided the three tiers' roles are defined.

2.1.1 Information Security Governance Committee (ISGC)

The Governance pyramid is headed by Information Security Governance Committee (ISGC). 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. The entity shall circulate minutes of meeting along with the action plan for each committee meeting with the stakeholders. 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 shall have the following roles:

a) Set up the goals of health information security and data privacy.

b) Review and approve entity's information security Policy.

c) Review and approve quarterly progress and compliance reports and ensure submission to the Department of Health.

d) Update the entity's top Executive on the performance and progress of the entity's information security program.

e) Provide management oversight and direction for both physical and logical aspects of information security.

f) Provide 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.

g) Enforce ADHICS standards and related policies, and monitor compliance.

h) Recommend and communicate information security budget requirements and allocate adequate to the executive management budget allocation towards entity Information Security initiatives.

i) Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve Information Security.

j) Acts appropriately on HIIP team reports concerning information security performance metrics, security and privacy incidents, investment requests etc.

k) Approve the criteria for accepting the risk and acceptable levels of risk.

l) Decide information security action plan and keep track of the initiatives.

m) Ensure that internal information security and data privacy audits are conducted.

n) Ensure that corrective actions are taken basis on the outcome of internal audits/assessments, management reviews, security incidents, and external audits etc., thus promoting continual improvement and ensuring that the information security achieves its intended outcomes.

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 adhered and followed with in the practice.

2.1.2 Health information Infrastructure Protection (HIIP) Workgroup

The next layer of Governance is led by Health information Infrastructure Protection (HIIP) Workgroup. It coordinates activities with "Implementation Stakeholders" across various functional/business verticals, ensuring that suitable policies and procedures are well implemented to support Abu Dhabi Health information and Cyber Security Standard.

The HIIP - Workgroup will shall have the following roles:

a) Identify processes and systems that are vital in health care.

b) Identify legislative, regulatory, and contractual requirements, including those for the protection of health information.

c) Develop Information Security policies and ensure their compliance with the principles approved by the ISGC.

d) Coordinate and manage the information security initiatives and its control demands.

e) Periodically review the information security policies to ensure the efficiency and effectiveness of control/risk environment and recommend improvements where necessary.

f) Review and monitor compliance with the policies and assist in Internal Security audit and self-assessment processes.

g) Address information security risks related to projects and deliverables throughout the project life cycle.

h) Identify significant trends and changes in information security risks and, conduct periodic risk assessment and where appropriate propose changes to the control's framework and/or policies.

i) Review critical security incidents and, where appropriate, recommend strategic improvements to address any underlying root causes.

j) Periodically report on the status of the security controls to the ISGC and to the Chairperson of the Abu Dhabi Health Sector HIIP – Workgroups.

2.1.3 Chief Information Security Officer (CISO)

The entity shall appoint Chief Information Security Officers (CISO) or AN equivalent resource to lead the HIIP workgroup. The CISO designated shall have the following roles and responsibilities:

a) Provide directions to the HIIP, entity employees and report progress and challenges to ISGC.

b) Establish overall enterprise information security architecture in line with the entity's overall security strategy.

c) Ensure implementation of security initiatives and programs, as necessary to coordinate, implement, comply, enhance, maintain, and manage information security demands as required by:

- Federal and Local Authorities
- Applicable Legislations and Regulations

- Local entity needs and risk environment.
- Industry specific needs

d) Act as entity 's point of contact to coordinate information security related matters with sector regulator, along with representation from various business and support verticals as needed.

e) Define and maintain information security and risk management frameworks.

f) Manage achievement of cybersecurity objectives and goals

g) Maintain information security policies and coordinate review and approval.

h) Oversee implementation of controls in line with the requirements of information security policies and procedures.

i) Manage the implementation of information security training and awareness programs.

j) Ensure the security of medical devices and equipment.

k) Coordinate or assist in the investigation of security threats or other attacks on information assets.

l) Periodically report security incidents and violations of entity's information security Policy and Standards to the ISGC.

m) Supervise or manage preventive or corrective measures when a cybersecurity incident or vulnerability is discovered.

n) Ensure information security effectiveness through audits, objectives/ KPI measurement and reporting.

o) Ensure management reviews are conducted as per defined frequency and as required.

p) Ensure implementation of program/initiatives as needed by the government and/or sector regulator.

2.1.4 Implementation Stakeholders

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, bio-medical stakeholders, and business representatives. The roles and responsibilities include:

a) Day-to-day operational activities for implementation and maintenance of the information security standard and respective policies and procedures.

b) Ensure suitable technical, physical, and procedural controls are in place in accordance with the Standard and are implemented at all levels within the entity.

c) Provide input on process improvements and related documentation.

d) Collect, analyze, and report on information security metrics (KPIs) and incidents.

e) Ensure active participation in initiatives such as training and awareness, internal audits, and reviews.

f) Report to HIIP – Workgroup, on confirmed or suspected policy violations (Information Security Incidents) affecting the entity's information assets.

g) Evaluate compliance with the information security policies through regular self-assessment process and internal audits.

2.2 Information Security Policy

The entity, regardless of its type, shall develop an information security Policy to provide a framework, leadership direction and support for health information security within the entity, in accordance with business requirements, risk management, relevant laws and this standard.

The information security policy shall be supported by the policies and procedures required to address specific control requirements.

The entity shall ensure information security metrics/key performance indicators (KPIs) are established and measured for the effectiveness of the security program at strategic, tactical, and operational levels.

2.3 Control of Documentation

The entity, regardless of its type, shall define a documented procedure to ensure the documents are controlled, tracked, periodically reviewed and managed.

The entity shall establish a document control procedure to ensure quality by:

a) Having the process of review, update as required, and re-approve documents.

b) Ensuring documents are maintained, reviewed, and updated at planned intervals or if significant changes occur to operating or risk environment, whichever is earlier.

c) Ensuring documentation is approved by the entity's top management and shall be well communicated to all relevant internal and external stakeholders.

d) Keeping track of changes and document revision status/current version number

e) Ensuring availability of all documents at any points of use and assure they are legible.

f) Controlling the distribution of external documents

g) Preventing obsolete documents from unintended use

h) Ensuring suitable identification if obsolete documents are retained.

3. Information Security Risk Management

Risk assessment can guide an entity in determining the level of efforts and resources needed to secure and protect their data assets and information processing environments The entity shall define an information security risk management procedure, with a step-by-step approach on how to perform the risk assessment and risk treatment. The process of risk management will enable entity to identify threats to assets, and associated vulnerabilities resulting in the likelihoods of occurrence being evaluated and potential impacts estimated. The results of risk assessment shall align with risk remediation measures. The entity, regardless of its type, shall undertake the following activities, as a minimum to meet its obligation in managing risks towards health information ecosystem.

The entity shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for its information assets by:

a) Defining the scope of the risk assessment exercise; Identify business functions/services.

b) Identifying information assets supporting business critical functions/services within the scope and boundary of the risk assessment.

c) Calculating asset criticality value by rating Confidentiality, Integrity, and Availability on a scale of 1 to 5 for each in scope information asset

d) Doing threat and vulnerability analysis for information assets

e) Assessing realistic likelihood of the occurrence and impact

f) Documenting associated risk and calculating levels of risk

g) Identifying existing information security controls

h) Defining mitigation plans for the identified risks and the expected completion dates.

i) Identifying the risk owners and the expected target date for closure of the control implementation

UAE IAR Reference: M2.1.1, M2.2.1, M2.2.2

3.1 Implement measures to remediate identified risks

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

a) Identify and assess all the mitigation options that are necessary for managing the identified information security risk:

- Risk Reduction - Applying suitable controls to reduce risk.
- Risk Acceptance - Accepting the risk based on entity's risk acceptance criteria.

- **Risk Avoidance** - Avoiding the activity causing risk.
- **Risk Transfer** - Transferring risk to another party

b) Establish and maintain policies in support of risk mitigation demands.

c) Define procedures in support of established policies.

d) Not limit control adoption as per this standard and identify all the controls that are necessary to implement the treatment options.

e) Consider the risk acceptance criteria of the entity while selecting controls.

f) Determine the residual risk and evaluate likelihood and impact ratings after implementation of the controls.

g) Identify proposed start and target completion dates for risk treatment plan implementation.

h) Identity responsibilities and priorities for managing information security risks.

UAE IAR Reference: M2.3.1, M2.3.2, M2.3.3

3.2 Ongoing risk review and monitoring

An entity shall periodically monitor the following factors related to controls implemented:

- 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 requirements
- Policy updates and amendments
- Control withdrawal/termination

UAE IAR Reference: M2.4.1, M2.4.2

4. Statement of Applicability

The entity shall produce a Statement of Applicability (SOA) to justify specific security controls selected for entity's unique information security needs, aiding compliance, and risk management.

Statement of Applicability should contain:

a) The controls that have been identified as necessary.

b) Reasons for identification of these controls

c) Current status of implementation

d) Justification for exclusion of any of the "risk-based applicable" controls contained in these Standards.

UAE IAR Reference: M2.3.4

5. Information Asset Classification

The value of assets shall be represented through appropriate classification reflecting their criticality to the entity and relevant stakeholders. Classification is the first visual and digital representation that an asset is critical or not and shall be protected accordingly.

An entity shall classify its information assets based on the below classification scheme or using the predefined entity's classification scheme approved by their management, provided that it is aligned with the classification factors and criteria as defined below, and necessary mapping with the below classification scheme maintained.

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. 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/health 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 nation. Information disclosure could potentially threaten life or seriously prejudice public order.

6. Control Adoption, Compliance and Audit

The Abu Dhabi Health information and Cyber Security Standard sets out the minimum requirements essential to secure health information and processing entities. The control requirements specified by ADHICS Standard are grouped into four categories (individually referred as standard, in the context of the area/section under consideration or being discussed), applicable to entities based on their perceived risk, value of health information under custody service eligibility/ability of the entity. 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. Entities shall invest time, effort and resources to progress their compliance to full compliance.

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

All Healthcare Technology and Services Providers are required to implement controls as per the "Service Provider" control category defined in the table below.

Control Category	Definition, Applicability (Entity Type) and Timelines of Compliance
Basic	Control demands outlined in this category are the absolute minimum essentials of information security and shall be considered a 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 in scope entities shall comply with the provisions of this category. 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 DoH, along with necessary supporting evidence and records. **Timeline for compliance:** Within six months of official program induction/on-boarding or official release of this standard, whichever comes first.
Transitional	Control demands outlined in this category are high priority controls to enhance security posture of 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 entity. The control implementation directly complements in redefining/improve entities risk environment.

	Applicability: Control demands of this category are applicable based on an entity's risk posture. They are applicable to the following types of entities: Hospitals	With bed capacity 1 to 20
	Center	Any Center including but not limited to Diagnostic Center, Dialysis Center, Fertilization Center (IVF), Rehabilitation Center

Timeline for compliance: Within 6 months of official program induction/on-boarding or official release of this Standard, whichever comes first.

Note: All controls categorized as "Basic" are considered essential and are applicable by default.

Advanced

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 entity. The control implementation elevates the entity's maturity level, and complements improvement of internal processes and risk environment.

Applicability: Control demands of this category are applicable based on an entity's risk posture, and shall be applicable to the following types of entities:

Hospitals	With bed capacity of 21 and above
Health Information Exchange (HIE)	Malaffi
Payers	Insurers Third-Party Administrator (TPA)

Timeline for compliance: Within 6 months of official program induction/on-boarding or official release of this standard, whichever comes first.

Note: All controls categorized as "Basic and Transitional" are considered essential and are applicable by default.

Service Provider	The control demands of this category shall protect healthcare technology from critical threats and shall be considered foundational for a secure healthcare service and solution. **Applicability:** Control demands of this category are applicable on any external entity that is providing healthcare technology and service that generate, access, store, use, process and/or transmit health information in any format of information, such as text, video, audio, photos and images These healthcare technology and services providers include but not limited to: • Medical device or technology Providers • Electronic Medical Records (EMR) Providers • Web and Mobile Applications 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 Department of Health, along with necessary supporting evidence and records. **Timeline for compliance:** Within 6 months of official program induction/on-boarding or official release of this standard, whichever comes first.

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 entity should consider for implementation in a phased manner, based on its risk level and resource availability. Information security controls 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
- Objective of the policy
- Scope and applicability of the policy
- Policy Statement

6.1 Compliance

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

- Demands, with references, applicable to the entity's business.
- Stakeholder(s) involved in implementation, maintenance and support.
- Compliance checklists.
- Reporting obligations.
- Escalation demands.

Compliance with, and deviations from the provisions of such legislative, regulatory, and governmental executive orders (Laws/Circulars/Standards/Regulations/Mandates etc.) 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 managed. The 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 that the entity establishes 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 entity, regardless of its type, shall develop an annual audit program to validate and verify compliance with the provisions of this Standard, and any other information security compliance requirements as they become relevant and valid. Independent audits shall be performed at least annually or in case of any significant change with the agreements of the information asset owners/relevant stakeholders to minimize the risk of disruption to business processes. The entity shall appoint internal or external resources to conduct an audit and identify any weakness or potential points of compromise. The responsibility of conducting internal audit shall be aligned considering the ethical aspects of functional independence to avoid conflict of interest and to aid in the efficient identification of facts and their unbiased reporting to relevant authorities.

The outcome of audits and assessments shall be shared with relevant stakeholders for necessary containment and remedial actions.

The outcome of audits and assessments shall be preserved (i.e., filed, stored, saved, and protected) with the highest level of protection and secure storage facilities. Tools used for audits 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 further action of audits and assessments, on a regular basis as defined by the CISO or the designated individual.

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 Information Security Framework. Healthcare entities shall take adequate measures to ensure that qualified resources, are hired to deliver the right values, are equipped to safeguard organizational interests, and are relieved in a manner that shall not impact organizational assets, values, reputation, and financial conditions at any time, current or future.

Objective:

To ensure qualified and competent 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:

i. Information Security Policy

ii. Acceptable Usage Policy

iii. Compliance Policy

HR 1	Human Resources Security Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
HR 1.1	The entity shall develop, enforce, and maintain a human resources security policy covering the security aspects of recruitment, employment and termination of employees, contractors and third-party users The policy shall: 1. Define management requirements on. a) Background verification for employees, contractors, and third-party users 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 IAR Reference: M3.1.1, M4.1.1

HR 2	Prior to Employment	
Control Demands		**Control Criteria** Basic/Transitional/Advanced
HR 2.1	The entity shall ensure background verification checks are conducted for all candidates for employment, contractors and third-party users. The 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) Levels of information access needed c) Access to critical areas d) Risks identified for the role 3. Conduct background verification of its candidates for employment (Permanent employees) 4. Ensure that it receives background verification reports for contractors and third-party users from responsible government bodies/agencies, through their respective company 5. Thoroughly validate the background verification report provided by the third-party prior to granting them access to entity resources or environment 6. Define information security requirements in the Job Descriptions, as required	**Basic**

HR 2.2	The entity shall establish specific terms and condition of employment as part of the employment contract The entity 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 entity and of the employees, contractors and third parties. 3. Ensure employees sign a Non-disclosure Agreement (NDA) with the entity, as required. 4. Ensure the contract includes disciplinary action in case of violation or non-compliance with the information security requirements of the entity. 5. Ensure the Terms and conditions are read, understood, agreed and signed by employees, contractors and third parties. 6. Conduct mandatory briefing sessions to employees, contractors and third parties on standard and specific information and cyber security requirements of the terms and condition. 7. Maintain adequate records on employee, contractor and third-party briefing(s) 8. Maintain Terms and Conditions, Non-disclosure Agreement (NDA) signed by employee, contractor and third-party resources in-line with entity retention requirements 9. Review and update any existing contract with employees, contractors and third-party users, as required	Basic

UAE IAR Reference: M4.2.1, M4.2.2

HR 3	During Employment	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
HR 3.1	The entity management shall ensure employees, contractors and third-party users adopt and apply security in accordance with established entity policies and procedures. The entity shall: 1. Ensure that employees, contractors, and third-party users are aware of security threats and concerns, their information and cyber security responsibilities and compliance requirements. 2. Ensure users read, accept and sign the acceptable usage policy prior to the provision of access to system, application and/or information. 3. Consider segregation of duties to avoid potential misuse of position or conflict of interest	Basic
HR 3.2	The healthcare entity shall conduct periodic security awareness campaigns, based on established schedules The entity shall: 1. Conduct awareness campaign for general and targeted user groups 2. Identify and establish method of delivery 3. Include information security and privacy education as part of the campaign 4. Ensure all the licensed healthcare professionals complete the mandatory training courses assigned to them by DoH 5. Ensure active participation and tracking of training and awareness sessions	Basic

HR 3.3	The entity shall develop new or modify existing information security and privacy education and training program to include requirements of governmental and organizational information security and privacy demands The entity shall: 1. Ensure all employees, and where relevant contractors and third-party users, receive information security and privacy training as part of their onboarding process 2. Ensure that an awareness and training program is formally launched and effectively managed 3. Review and update the training content, as required 4. Assess and identify skill and competency gaps on information and cyber security, data privacy compliance demands 5. Implement skill and competency development programs 6. Periodically review training records to ensure that all participants have received the required instruction	Transitional
HR 3.4	The entity shall provide appropriate role-based trainings to employees, contractors and third-party users with relevant roles and responsibilities. The entity shall: 1. Ensure to provide information security and privacy training: a) Prior to authorizing access to system, network, applications, medical devices and/or cloud environment b) In case of any new role that require specific training 2. As needed by awareness and training program Periodically evaluate effectiveness of the awareness program	Advanced
HR 3.5	The entity shall establish and enforce a disciplinary procedure for employees, where relevant contractors and third parties, who have committed security breaches. The 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 Service Providers

UAE IAR 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 entity shall define responsibilities concerning information security for performing employment termination and/or change of employment The entity shall: 1. Establish internal and external communication protocol on employment exit. 2. Ensure adequate knowledge transfers and responsibility handovers. 3. Ensure employee handover of entity data prior to their exit. 4. Define an employee exit clearance form and ensure it is filled and signed by relevant function/department SPOCs before employee exit	**Basic**
HR 4.2	The entity shall ensure recovery of all organizational assets upon termination of employment, contract or agreement. The entity shall: 1. Ensure all organizational assets are recovered and necessary acknowledgement and clearance is obtained from appropriate stakeholders 2. Ensure all information, with special focus on health 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 entity shall remove physical and logical access rights and revoke privileges of individuals upon exit, termination of employment, contract or agreement. The entity shall remove access to systems, applications, information, secure areas, and work areas. The entity shall: 1. Ensure access to systems, application, information, secure areas, work areas and identified critical areas are revoked in a timely manner within 24 hours upon exit termination. 2. Communicate with DoH and the entity being served to revoke any relevant system and application access upon termination	Basic Service Provider
HR 4.4	The entity shall develop internal process to manage internal transfers and change of role. The entity shall: 1. Ensure communication to all necessary internal and external stakeholders on change of role or internal transfers. 2. Revoke access and privileges associated with previous role and reassign privileges on system, application and information access and utilization consistent with their new role based on necessary authorization. 3. Ensure adequate knowledge transfers and responsibility handovers	Basic

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

2. Asset Management

Asset Management is an essential part of effective health information Security management. In order to be effective and supportive of organizational business and security objectives, entities shall maintain an updated version of asset inventory, available to relevant management, business and support stakeholders.

Information assets include data/information in all its form, as well as the underlying application, technology, physical infrastructure to support its processing, storing, communicating, and sharing and people who have access to data/information.

Information Assets include, but are not limited to:

- Information (in physical and digital forms)
- Medical device and equipment used for diagnosis, therapy, monitoring, rehabilitation, and care etc.
- Applications and System Software's
- Information system
- Network infrastructure devices
- Services and Processes Virtual Infrastructure s
- Physical Infrastructure (Data center, Servers, access barriers, electrical facilities, HVAC systems, etc.)
- Human resources (in support of services/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 entities to monitor and record the use of information assets.

Supporting or dependent entity policy references:

i. Data Retention and Disposal Policy

ii. Physical and Environmental Security Policy

iii. Portable Device Security Policy

iv. Acceptable Usage Policy

AM 1	Asset Management Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
AM 1.1	The 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 Asset classification scheme in line with section A.5 of this standard. 5. Identify requirements of data retention, handling, and disposal	Basic
AM 1.2	The entity shall pay specific attention to medical devices and equipment's while defining policy, and shall categorically address the following demands: 1. Maintain an inventory of medical devices and equipment, and link them to patients while ensuring that sensitive patient information is redacted and not visible 2. Roles that will be allowed to access, use and maintain medical devices and equipment shall be established 3. To the extent possible, medical devices and equipment to authenticate users, based on entity's authentication and authorization process 4. The need for handling procedures for each medical device and equipment in use shall be defined and updated as required to stay current 5. The need to establish and maintain risk log concerning medical devices and equipment 6. Decommissioning and/or secure disposal of medical devices and equipment	Basic Service Provider

UAE IAR References: T1.1.1

AM 2	Management of Assets	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
AM 2.1	The entity shall have all their information assets (connected/not connected) identified, recorded, and maintained through an information asset inventory. The inventory shall: 1. Capture all information assets (Laptops/ Computers, Mobile devices, Servers, Network devices, Applications, Software, Medical devices, equipment's etc.) and necessary asset details in the asset inventory be reviewed and updated periodically , or during change in the environment, and shall be accurate and reliable 2. Be accessed and updated by an authorized individual. 3. Be centralized or distributed (function/line-of-business/service wise) based on the entity's internal structures	Basic Service Provider
AM 2.2	The entity shall ensure asset inventory establishes the relations between various types of information assets, in support of care delivery	Advanced
AM 2.3	Ownership for each identified asset 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. 5. The owner shall define and periodically review access restrictions and classifications, in line with the access control policy of the entity	Basic

AM 2.4	The entity shall establish and enforce policy on the acceptable use of information assets to which users have access: 1. The policy shall be communicated to all employees, contractors and third-party users 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 policy 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 Service Provider
AM 2.5	The entity shall identify and implement "Bring Your Own Device (BYOD)" security controls, to ensure secure usage of employees personally owned electronic devices for official purposes. The entity shall: 1. Identify and address information security risk for the concept-in-practice "Bring Your Own Device (BYOD)" 2. Ensure probabilities of compromise through the use of personal devices are addressed through suitable security controls and role-based usage agreements. 3. Establish an authorization process on the use of personal devices to access/view/use/share/process/store health information. 4. Ensure usage of BYOD is subject to user acknowledgement on the usage agreements. 5. Ensure no healthcare and entity data/information is stored in employee/user's personal devices and/or personal spaces within the devices	Basic Service Provider

UAE IAR 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 entity shall classify all information assets in line with the information asset classification scheme. The entity shall: 1. Determine classification considering the criticality of the information it holds and ensure it is more restrictive/deterrent based on the entity's tolerance of financial and reputational impact due to compromise of the information considered. 2. Ensure the classification scheme is uniform across the entity and well communicated. 3. Establish process for information labelling in accordance with entity's information asset classification scheme. 4. Establish process to reassess and/or update information classification, based on the following: • Change in the value of information. • Changes to environment (location, access, storage, processing, usage, etc.) • Changes in protection levels • Changes in government demands	Basic Service Provider
AM 3.2	The 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 3.3	The entity shall establish process to tag its information assets with unique tags prior to deployment/use in the entity environment. The asset tags can be used for tracking, inventory, and accountability purposes	Transitional

UAE IAR 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 • Removal and disposal 2. Security requirements based on asset criticality shall be considered in the handling procedures	Basic
AM 4.2	The 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 controls for protecting removable media against unauthorized access or misuse. Limit the use of removable media to those with valid business justification. 3. 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 Service Provider

AM 4.3	Access and privilege allocation for medical devices and equipment shall be provided to defined roles, with essential qualification and experience required to operate. The entity shall: 1. Secure and safe-guard medical devices and equipment with adequate security controls in accordance with its classification scheme and risk factors	Basic Service Provider
AM 4.4	The entity shall prevent unauthorized disclosure, modification, destruction, or loss of patient health information stored on medical devices and equipment. The entity shall ensure. 1. Information stored within the medical devices and equipment are encrypted. 2. Secure electronic communication between medical devices and other equipment's 3. To define minimum essential qualification required to operate and/or handle medical devices and equipment. 4. Copies of valuable health information is moved to a secure storage/location to reduce the risks of its data damage or loss	Transitional Service Provider
AM 4.5	Healthcare facilities shall consider wired communication facility for medical devices and equipment. Usage of wireless communication facility with medical devices and equipment shall be considered only when the wired communication facility is not available with the medical device.	Transitional
AM 4.6	Entity shall deploy technology solution to control and monitor removable media and shall be complemented by content encryption and biometric based access provisioning.	Advanced
AM 4.7	The entity shall establish control procedures for the removal, movement, and transfer of information assets (information, equipment, medical devices, and information processing equipment/systems). The entity shall: 1. Authorize removal, movement and transfer of information assets. 2. Maintain records of removal, movement and transfer	Transitional Service Provider

UAE IAR 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 entity shall ensure assets, both digital and physical, when no longer required are disposed beyond recovery. The entity shall 1. Dispose information assets, when no longer required: • by the entity • on basis of legislative and regulatory demands • for legal proceedings 2. Initiate disposal of information assets on authorization of entity management 3. Verify and comply with the data retention policy, regulatory demands and requirements of data/information prior to disposal of any information asset. 4. Establish control procedures for the secure disposal or reuse of media, equipment, devices and systems, containing classified information. 5. Ensure removal of identifiable health information from assets prior to disposal 6. Establish controls that ensure data once destroyed is not recovered	Basic Service Provider
AM 5.2	The entity shall maintain records, on asset 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	Transitional

UAE IAR Reference: T1.4.2, T2.3.6

3. Physical and Environmental Security

Physical and environmental security measures shall be implemented to ensure processing facilities are physically protected from unauthorized access, damage, interference, and equipment is protected from physical and environmental threats.

These security measures or controls shall protect 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.

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:

i. Clear Desk and Clear Screen Policy

ii. Data Privacy Policy

PE 1	Physical and Environmental Security Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
PE 1.1	The entity shall develop, implement and maintain a physical and environmental security policy, to ensure adequate physical and environmental protection of entity's information assets. The policy shall: 1. Be relevant and appropriate for entity's operational and risk environment, concerning internal and external threats. 2. Address requirements of secure storage of hazardous or combustible materials that ensure avoidance of: a) human injuries or loss of life b) damage to information and information systems 3. Consider classification of information assets and their physical presence 4. Consider medical devices and equipment's with special focus on their: a) Criticality of data handled and healthcare operations. 5. Physical and environmental demands, as recommended by the manufacturer and applicable regulatory requirements define roles and responsibilities for actions expected out of physical and environmental security policy	**Basic**

UAE IAR Reference: T2.1.1, T2.3.5

PE 2	Secure Areas	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
PE 2.1	The entity shall define and use security perimeters to protect areas that contain information and information systems. The entity shall: 1. Identify secure areas and define security perimeters, based on information assets contained within or information being processed. 2. Ensure adequate security countermeasures are applied to identified secure areas to protect information and information systems within 3. Consider the impact of compromise of confidentiality, integrity and availability of information or information assets while applying security controls. 4. Ensure secure areas are protected by appropriate control measures and only authorized personnel are provided access and authorized activities are being conducted. 5. Control access of mobile, portable and surveillance devices/equipment/utilities to secure areas	Basic Service Provider
PE 2.2	The entity shall allocate secure private areas to discuss protected health information by authorized stakeholders	Advanced
PE 2.3	Secure areas shall be protected by appropriate control measures to ensure only authorized personnel are granted access and authorized activities are being conducted. The 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. Maintain visitor access logs for visitors to secure areas. 5. Ensure that all employees, contractors and visitors wear distinguished form of visible identification within the premises of the entity 6. Ensure the locking mechanisms on all access doors are adequate, and alarms configured to alert prolonged open state of doors	Basic

	7. Escort contractors or third parties while inside the secure areas 8. Deploy closed circuit television (CCTV/surveillance camera) in identified vantage points of secure areas as required by Monitoring and Control Centre (MCC) Abu Dhabi 9. Preserve CCTV footage for a period as required by Monitoring and Control Centre (MCC) Abu Dhabi	
PE 2.4	The entity shall nominate owners for each identified secure area. Nominated owners of secure areas shall: 1. Review access records/logs and surveillance footage in accordance with entity policy or in case of any security incident, whichever is earlier. 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 4. Ensure to change the combinations and keys for any entity-defined secure zones, entry/exit points, and cabinets, when compromised	Transitional
PE 2.5	The entity shall design and apply physical protection against natural disasters, environmental threats, external attacks and/or accidents. The entity shall: 1. Implement and maintain environmental control systems for data center's, that monitor, maintain, and test the consistency of temperature and humidity conditions in accordance with regulatoryrequirements.s 2. Ensure appropriate fire suppression systems (e.g., sprinklers, fire extinguishers) are located throughout the entity. 3. Ensure fire detectors (e.g., smoke or heat activated) are installed on and/or in the ceilings and floors. 4. Ensure that fallback equipment, device, system and backup media are protected from damage caused by natural or man-made disasters.	Basic Service Provider

	5. Ensure availability of power backup to provide power to key information systems and critical data centre infrastructures	
PE 2.6	The entity shall have segregated delivery, loading areas and shall establish control measures over entry and exit. The 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 entity's asset management procedures. 3. Physically segregate incoming and outgoing materials, as applicable	Basic

UAE IAR 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 entity shall site/position medical devices and equipment in a manner that they are always protected. The entity shall: 1. Consider environmental risk condition while positioning medical devices and equipment. 2. Establish guidelines on physical protection and unauthorized access of equipment and medical devices. 3. Implement controls to protect equipment, medical devices and information processing systems when left unattended	Basic Service Provider
PE 3.2	The entity shall maintain operating procedures to keep equipment in reliable working order. The entity shall: 1. Establish operating procedures for commissioning, maintenance and decommissioning of equipment activities. 2. Maintain up-to date records for maintenance carried out.	Advanced Service Provider

PE 3.3	Power, telecommunication, and cables carrying data shall be secured and protected. The 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 3.4	The entity shall identify and apply security measures to protect equipment, medical devices, and information processing systems while off-site. The entity shall: 1. Establish an authorization procedure for taking information assets off-site. 2. Ensure manufacturer's recommendation and instructions are followed, while equipment, medical devices and information processing systems are off-site. 3. Ensure that movement and possession (chain of custody) logs for off-site equipment, medical devices and information processing systems maintained and verified. 4. 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	Transitional Service Provider
PE 3.5	The entity shall define and enforce a clear desk and clear screen policy for 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 entity. 3. Be read and acknowledged by all employees and contractors of the entity. 4. Ensure that health information is not left unattended	Basic

UAE IAR 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

Access control processes enforce security requirements such as confidentiality, integrity, and availability of information assets to prevent unauthorized use of resources. Access controls shall be developed by entity to control access of employees, contractors, and third-party users to entity's information assets and to manage their access in reference to internal network, operating systems, and applications to ensure appropriate protection of entity's infrastructure health information protected health information. Entity's management shall be aware of the risk environment and outcomes of unauthorized access, and are accountable for all consequences and impact on Abu Dhabi Government, Abu Dhabi Healthcare-ecosystem or Health Sector, Patients concerned and the entity itself.

Objective:

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

Supporting or dependent entity policy references:

i. Physical and Environmental Security Policy
ii. Clear Desk and Clear Screen Policy
iii. Log management policy
iv. Password Management Policy
v. Cloud Security Policy
vi. Data Privacy Policy

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

AC 1	Access Control Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
AC 1.1	The entity shall develop, enforce, and maintain an access control policy to ensure access to information and information assets is 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) Infrastructure devices f) Medical devices and equipment 3. Emphasize the requirement-of-need and role-based access principles. 4. Establish requirements, with core focus on. a) granting of access b) access authorization c) access revocation d) access review 5. Address the entity needs on secure password management and practices	**Basic**

	6. Mandate the usage of unique identity and complex password where relevant, define access control measures and provisions for portable/mobile devices, including user owned devices, that handle the entity's data or host the entity application(s) to conduct business transactions. 7. Include control requirements for the access and use of network services. 8. Include management actions on violations and deviations. 9. Define roles and responsibilities for actions expected	

UAE IAR Reference: T5.1.1

AC 2	User Access Management	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
AC 2.1	The entity shall have a formal documented and implemented user registration and de-registration process the 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 shall implement a suitable authentication mechanism. 3. Ensure shared user account are not created or used without explicit approval from the Information System Owner, Business Processes Owner & shall have an owner assigned to ensure accountability. 4. Ensure accounts are deactivated within defined duration of inactivity. 5. Revoke user accounts upon exit, termination of employment, contract, or agreement 6. Revalidate access requirements during role changes. 7. Maintain records/list of persons authorized to use entity's information systems, applications, medical devices, and equipment	**Basic** **Service Provider**

AC 2.2	The entity shall restrict and control allocation of privileges, based on principles of need to know. The entity shall: 1. Ensure normal user accounts are not used as service accounts or to conduct privileged application and system level activities. 2. Control and restrict from sharing privilege user IDs to multiple users. 3. Ensure users privileges are restrictive in nature, and are assigned based on needs to conduct business activities supported by necessary approvals. 4. Ensure Privilege or administrative accounts are only used for system administrator activities and not for daily day to day operations. 5. Ensure usage of service accounts are controlled, and are not hardcoded in application codes or scripts. 6. Enforce multifactor authentication scheme for all privilege, administrative and remote access. 7. Ensure remote access is controlled and monitored	Transitional Service Provider

AC 2.3	The entity shall establish a process for secure allocation, use and management of security credentials. The entity shall: 1. Ensure to change default credentials for all information assets before deployment to operational environment. 2. Ensure that passwords are prohibited from being displayed when entered. 3. Ensure passwords are always hashed and stored in encrypted format. 4. Communicate details of user account and password in two different communication modalities 5. Enforce complexity requirements on password characters, and shall have at least: a) Twelve characters b) One number, one upper-case and lower-case character, and a special character 6. Ensure passwords, including that of service accounts and privileged accounts, are changed periodically. 7. Ensure account lockout features are configured to block the users after at least 5 failed attempts. 8. Ensure that password history is maintained, and shall restrict users from using immediately used previous passwords (at least 3 previous passwords) 9. Ensure to change password post remote maintenance session which requires sharing of password. 10. Educate users to adopt good practices while selecting and using passwords	Basic Service Provider

UAE IAR Reference: T5.2.1, T5.2.2, T5.2.3, T5.3.1, T5.5.2, T5.5.3

AC 3	Equipment and Devices Access Control	
	Control Demands	**Control Criteria** Basic/Transitional/Advanced
AC 3.1	The entity shall restrict access to removable media, portable devices, and medical equipment or devices. The entity shall: 1. Ensure access is provided on role-based need-to-know principles with appropriate authorization. 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 entity password complexity and usage requirements	Transitional Service Provider
AC 3.2	The entity shall control access to equipment, devices, system, and facilities at teleworking sites. The 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 health information while providing/consuming services through teleworking principles. 3. Maintain an inventory of assets in use at teleworking sites	Transitional Service Provider
AC 3.3	The entity shall adhere to security and privacy requirements outlined in the DoH standard for Telemedicine, in addition to fulfilling the requirements set forth in this standard when delivering Telehealth services.	Basic Service Provider

UAE IAR Reference: T5.6.1, T5.6.3, T5.7.2

AC 4	Access Reviews	
	Control Demands	**Control Criteria** Basic/Transitional/Advanced
AC 4.1	The entity shall review access and privileges granted to its user. The entity shall: 1. Establish process for the reviewing user access and associated privileges to various entity resources periodically. 2. Define responsibility for access and privileges review, based on entity resources being accessed. 3. Conduct user access 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	Basic Service Provider

UAE IAR 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: The entity shall: 1. Provide access to entity network in accordance with access control rules and depending on necessity. 2. Implement appropriate authentication methods to ensure secure remote access. 3. Ensure all remote login and access are only through secure channels. 4. Identify all equipment and devices connected to its network, and shall have mechanism to detect unauthorized equipment and devices	Basic Service Provider
AC 5.2	The entity shall have mechanism to identify all equipment and devices connected to its network, and shall have automated mechanism to detect unauthorized equipment and devices	Advanced

AC 5.3	The entity shall control access to all information assets for the purpose of diagnosis and configuration. The entity shall: 1. Identify and whitelist all ports, services and utilities that are used for troubleshooting, and for diagnostics and configuration purposes. 2. Provide rationale or define security controls 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	Advanced
AC 5.4	The entity shall define and implement network routing controls to ensure information flow and system, medical devices and equipment connections are not compromised. The entity shall: 1. Establish processes for secure configuration and rules 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 externally accessible systems. 5. Manage external connections to information systems and networks using interfaces made up of perimeter security 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. Review and update the configured rules, as required. 8. Periodically scan for any covert channel connections to public networks bypassing entity security defense	Transitional Service Provider

AC 5.5	The entity shall ensure wireless access within the entity is secured. The entity shall: 1. Ensure that internal wireless is not broadcasted. 2. Establish authorization process for wireless access and usage. 3. Ensure only trusted devices and users gain access to internal networks via wireless access	Transitional

UAE IAR 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 entity shall establish and enforce secure log-on and log-off procedures to control access to system, applications, services, medical devices and equipment. The entity shall: 1. Ensure that access to systems, applications, services, medical devices and equipment that process, use or store health information are authenticated. 2. Enforce automated locking of workstation/system after a predefined period of inactivity. 3. Automatically terminate inactive sessions after a predefined period of session inactivity 4. 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 Service Provider
AC 6.2	The entity shall create unique identifier (user ID) for each user who requires access to entities systems, applications, or services, and shall implement a suitable authentication technique. The entity shall: 1. Grant each user with a unique identifier 2. Ensure all user activities are logged with the associated identifier	Basic Service Provider

AC 6.3	The entity shall restrict and control the use of utility programs and tools that might be capable of overriding system and application controls. The 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 IAR Reference: T5.5.1, T5.5.2, T5.5.4

5. Communications and Operation Management

Communications and Operations management aims to establish and/or strengthen entities processes and efforts to improve and enhance control environment. Entity shall have controls in place to ensure the safe operation of information processing equipment and the security of data while it is processed, stored and transmitted across networks.

The domain addresses requirements of backup, security of network, secure electronic communication and monitoring to ensure protection against malicious code and spyware.

Objective:

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

Supporting or dependent entity policy references:

i. Change Management Policy
ii. Capacity Management Policy
iii. Patch Management Policy
iv. System Acceptance Policy
v. Backup Policy
vi. Logging and Monitoring Policy
vii. Cloud Security Policy
viii. Third Party Security Policy

CO 1	Communication and Operation Management Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 1.1	The entity shall develop, enforce and maintain a secure communication and operation management policy to ensure operational and communication activities concerning data, technology and application are controlled. The policy shall: 1. Be relevant and appropriate to the 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 management d) Baselines and minimum-security configurations e) Standard operating procedures f) Capacity management g) System acceptance h) Malware control i) Backup management j) Network Security Management k) Secure exchange of Information l) Electronic Commerce Services m) Logging and monitoring n) Patch management	Basic

UAE IAR Reference: T3.1.1, T4.1.1

CO 2	Operational Procedures and Responsibilities	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 2.1	The entity shall develop and enforce baseline and recommended configuration and system settings for hardening of information technology products, applications, virtual machines (VM), medical devices and equipment The entity shall: 1. Consider the following while developing baseline and recommended configuration setting: a) Requirements of this Standard b) Manufacturer's security recommendations c) Industry best practices d) Risk mitigation strategies e) Resilience during any unforeseen events f) Corrective and preventive actions (audit, assessment, and incident outcomes) 2. Periodically review and update baseline and configuration requirements in line with evolving vulnerabilities and threats	Transitional Service Provider
CO 2.2	The entity shall document and follow operating procedures for all administrative, support, operational and maintenance activities of information systems, applications, medical devices, equipment or Cloud based systems and solutions. The entity shall: 1. Disseminate operating procedures and ensure all relevant internal stakeholders are aware of their responsibilities as needed by their roles. 2. Ensure all the involved third-party users (if any) are well aware of the entity's operational procedures and they adhere to the same. 3. Ensure operating procedures are relevant and are updated periodically or in case of any significant change, whichever is earlier 4. Ensure system documentation includes up-to-date diagrams.	Advanced

CO 2.3	The entity shall establish, document, approve, communicate, apply, evaluate, and maintain the policies and procedures for managing the risks associated with applying changes to entity assets including information systems, software's, applications, medical devices, equipment, infrastructure and technology environment regardless of whether the assets are managed internally or externally. The entity shall: 1. Establish a Change Advisory Board to authorize changes. 2. Define and enforce a process that addresses the following elements: a) Identification and recording of significant changes. b) Planning and testing of changes in test environment c) Assessment of potential risks and impacts of changes d) Formal approval procedure e) Communication of change to all relevant stakeholders f) Identification of stakeholders responsible for the "build, test, and implement" portion of the change. g) Roll-back plan to be utilized during unsuccessful changes. h) Post implementation assessment i) Monitoring of changes j) Maintenance of change records 3. Maintenance of previous version of software, code, and configurations. Maintenance of CMDB with updated Configuration Items. 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 4. Identify and segregate roles of conflicting interests and assign responsibilities accordingly. 5. Make sure the third party notifies the entity in advance of any changes to the manner services are provided, including but not limited to: a) Relocation b) Reconfiguration	Transitional

	c) Changes in hardware or software d) Onboarding sub-contractor e) Changes to operating environment	
CO 2.4	The entity shall identify and maintain separate environment for development, testing, staging and production. The entity shall: 1. Identify the appropriate level of segregation and protection between production, 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, confidential data and/or PII and PHI is not used in test environment. 4. Restrict usage/migration of test data into operational environment. 5. Ensure to test the change in testing environment before rolling it out in production state. 6. Prepare a rollback strategy	Transitional Service Provider

UAE IAR Reference: T3.2.1, T3.2.2, T3.2.3, T3.2.4, T3.2.5, T7.6.1, T7.6.2, T7.6.3

CO 3	Planning and Acceptance	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 3.1	The entity shall identify and document current and future capacity requirements for information systems and applications. The 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. Run stress testing on systems and services to ensure system stability during peak hours. 4. Identify capacity thresholds for all information systems and applications, cloud environment and services and define advance escalation matrix to ensure capacity demands are met. 5. Establish process to: a) decommission systems that are no longer needed. b) optimize databases. c) archive data that is not accessed regularly	Advanced

CO 3.2	The entity shall establish acceptance criteria for new information systems, applications, medical devices, equipment, and for changes, upgrades and releases, in addition to satisfactory test results. The 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 (with permissions appropriate for the tasks) involved in testing are different from the ones involved in operational and development activities. 5. Ensure development tools and/or editors are not installed on operational systems. 6. Ensure test data and accounts are removed completely before the application is moved into production state	Transitional Service Provider

UAE IAR Reference: T3.3.1, T3.3.2

CO 4	Malware Protection	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 4.1	The entity shall implement security measures to prevent and detect malware in order to safeguard information assets. The 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, virtual machine, cloud environment, hard drives, USB devices etc. 3. Ensure anti-malware and anti-virus protections mechanisms are updated and current. 4. Prevent access to malicious websites or sites. 5. Enable real-time protection capabilities. 6. Establish and enforce periodic scan schedules. 7. Scan removable media for viruses and malware on all occasions when they are connected to information systems. 8. Disable auto-run features for removable media on information systems. 9. Disallow the use or installation of unauthorized software. 10. Configure anti-malware and anti-virus protection systems to alert responsible stakeholders on event, incident or anomaly detection. 11. Collect information about new threats and provide ongoing awareness for users on techniques, tactics, and procedure to avoid and minimize probabilities	Transitional Service Provider

CO 4.2	The entity shall deploy gateway level protection mechanisms for web and email traffic to detect and defend against malware and viruses. The entity shall: 1. Implement Email Authentication Solution to block harmful or fraudulent uses of email such as phishing and spam. 2. Check any attachments or downloads from email and instant messaging for malware, before use	Advanced

UAE IAR Reference: T3.4.1

CO 5	Backup and Archival	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 5.1	The entity shall maintain backup copies of essential information and software needed to support care delivery and its operations. The entity shall: 1. Establish backup management process that identifies. a) Essential and critical information systems and applications 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) Security controls to prevent compromise of backup data	Basic Service Provider

	2. Perform backup of all identified systems, applications and its critical data including the configuration 3. Establish a data restoration process and ensure data restoration requirements for continuity and recovery are adequately met. 4. Ensure data backups are tested for restoration in accordance with the entity's defined recovery plan 5. Ensure data backup of specific instances are not mixed, accidently or deliberately. 6. Ensure backups are not stored on entity live environment	
CO 5.2	The entity shall establish data archival requirements that satisfies entities retention demands. The 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 Service Provider

UAE IAR Reference: T3.5.1

CO 6	Logging and Monitoring	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 6.1	The entity shall establish and enforce Logging and monitoring procedures for information systems application, cloud services, medical devices, equipment etc. The entity shall: 1. Ensure all critical technology (servers, database, network devices, applications, medical devices equipment etc.) are capable of generating logs and/or reports that can be referred for monitoring. 2. Identify aspects system use, privilege activities, operator and user activities, logon attempts, network, system and application traffic, security events, changes, internal processing, Exemption, information exchange, integration, access, backup process etc.) to be monitored 3. Establish minimum information gathering requirements for each monitoring activities. 4. Conduct real time monitoring or in a defined periodic interval, subject to entity risk environment. 5. Define minimum frequency requirements for reviewing each type of logs. 6. Ensure procedures are in place to respond to alerts from the monitoring system, as required. 7. Define criteria for alerting and escalation. 8. Have defined criteria that quantifies specific outcomes of monitoring as incidents. 9. Establish roles for monitoring activities and assign specific responsibilities. 10. Communicate alerts to relevant stakeholders to address the issues and enhance monitoring capabilities. 11. Ensure that logs and/or reports are protected and not tampered with or modified or destroyed	Advanced Service Provider

CO 6.2	The entity shall preserve logs in a centralized log management system. The 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 maintaining information systems or application. 3. Ensure logs are correlated to identify any security threats or malicious activity. 4. Retain logs for a period commensurate with legal, regulatory and entity demands. 5. Define use cases and dashboards based on the entity's needs and industry recommendations, and shall consider: a) System utilization 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
CO 6.3	The entity shall synchronize clock of all information systems and devices with an agreed time source. The 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 synchronized with the connected systems. 3. Regularly check that the clocks of all relevant information processing systems are synchronized.	Basic
CO 6.4	The entity shall implement solutions to prevent data leakage from systems, networks and any other devices that process, store or transmit health information. 1. The entity shall implement Data Leakage Prevention measures to control loss of entity data	Transitional Service Provider

UAE IAR Reference: T3.6.1, T3.6.2, T3.6.3, T3.6.4, T3.6.5, T3.6.6, T3.6.7, T7.6.

CO 7	Security Assessment and Vulnerability Management	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 7.1	The entity shall conduct periodic independent (Internal/External) technical assessment to ensure critical information assets are secure and always protected. The entity shall: 1. Establish yearly schedules and conduct vulnerability assessment and penetration testing of: a) Entity's system, network, infrastructures and environment b) Web and mobile applications accessible over internet c) Connected medical devices. 2. Establish processes to conduct security testing and authorization by authorized business and security stakeholders for all new deployment and changes to information assets prior to production roll-out and/or use Co-operate with DoH during DoH vulnerability assessment activity and ensure to provide all required information. 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 entity's management 5. Define timelines for tracking remediation of the identified technical vulnerabilities 6. Periodically follow up on the progress and status of mitigation measures with the appropriate stakeholders 7. Verify effectiveness and efficiency of mitigation measures by performing revalidation assessment	Advanced Service Provider

CO 7.2	The entity shall ensure that assessment data is not available with third parties engaged to conduct assessments beyond the time of engagement The entity shall: 1. Ensure that system, network, applications, devices, equipment 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, devices, equipment 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 all shared reports are suitably protected and controlled	Advanced Service Provider

UAE IAR Reference: T7.7.1

CO 8 Patch Management

	Control Demands	Control Criteria Basic/Transitional/Advanced
CO 8.1	The entity shall define and establish formal procedures for updating and patching of information system and application, medical devices and equipment The entity shall: 1. Restrict the usage of obsolete software/technology/medical devices/ equipment 2. Ensure all systems and devices that process or communicate information are timely patched and protected 3. Define criteria and process for application of standard, urgent and critical patches 4. Ensure all critical security patches are applied as soon as practicable from the date of release. 5. Ensure patches are deployed to a subset of systems or devices to allow testing before deployment to all. 6. Ensure firmware on devices are kept updated 7. Ensure security patches and updates are obtained from trusted sources and are periodically implemented 8. Ensure third parties provide advance notification to entity prior to the release of any patches or updates to the offered product or service 9. Periodically validate patch status of systems and devices in use	Basic Service Provider
CO 8.2	The entity shall have mechanisms in place to keep track of the patches and updates	Advanced

CO 9	Information Exchange	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 9 .1	The entity shall develop, enforce and maintain formal procedures on information exchange and transfer incorporating control measures that protect information during information exchange and transfer and ensure that such exchange/transfer is carried out in compliance with relevant legislation and agreements. The procedures shall: 1. Include control measures to protect information from interception, unauthorized access, copying, modification, misrouting, destruction and reduce probabilities of compromise during exchange and transfer taking into account: a) Classification and criticality of information b) Information exchange and processing environment c) Stakeholders involved d) Need for the exchange/transfer 2. Identify minimum technical standards for secure 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

CO 9.2	The entity shall follow secure practices and capabilities for health information exchange. The entity shall: 1. Ensure health information is not transacted through medium of mails., unless it is being shared with the data subject. 2. Maintain chain of custody for information while in transit. 3. Connectivity with DoH (AD Healthcare Net) and provide all required information. 4. Ensure secure integration of Electronic Medical Records (EMR) platform to Abu Dhabi Health information Exchange Platform (Malaffi) 5. Ensure that entity resources are given access to Malaffi with the proper authorization and based established need to provide healthcare services 6. Ensure health information (in any form) PII and PHI or its copy is not stored, shared, processed, disseminated and/or transferred outside UAE, except in cases where a valid and specific exemption is issued by DoH is in place 7. Ensure that employees of the entity and third-party involved in service delivery of any kind, fulfill their responsibilities and provide assistance from within the Health Sector Stakeholder premise, and from within UAE, unless a valid exemption has been issued by the Department of Health (DoH) 8. Not share identified or de-identified health information with third parties, data processors inclusive of counterparts and partners, unless authorized by Department of Health 9. Ensure that information exchanged between entities, and information sharing communities are protected 10. Ensure that username and password are communicated using two different communication channels (email and SMS-text, or email and phone, etc.) 11. Encrypt critical information before transferring and ensure sharing decryption key using a different communication channel	Basic Service Provider

	12. Ensure usage of appropriate interoperability standards for the exchange or transfer of information between systems and custom-developed applications 13. Identify and implement security requirements for exchanging information and software with third parties	
CO 9.3	The entity shall establish agreements between the entity and the external parties for the exchange of information and software The 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 with regards to the criticality and classification of the information to be exchanged 2. Agree on the process of notifying sender of transmission, dispatch and receipt 3. Clearly define roles and responsibilities of each party to the agreement 4. Establish non-disclosure agreements for all disclosures 5. Agree on the expiration date of the agreement 6. Include in the agreements: a) Definitions of information to be protected b) Classification of information to be shared c) Security requirements to be considered for information protection d) Duration of agreement e) Process for notification of leakage or incident f) Ownership for data protection g) Right to audit and monitor activities that involve health information and personally identifiable information h) Control requirements in handling the information in line with the defined asset handling policy	Basic Service Provider

CO 9.4	The entity shall protect physical media containing information during transit The entity shall: 1. Identify and ensure that physical media containing sensitive information is classified and labelled 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. Ensure information in removable media is encrypted before transit 5. Utilize trusted entity staff or courier service for transporting media 6. Ensure that media is controlled and disposed as per the relevant policy	Basic Service Provider
CO 9.5	The entity shall restrict the usage of public domain email address for any official purposes and ensure email IDs possess email domains within the UAE	Basic Service Provider

CO 9.6	The entity shall protect information involved in electronic messaging The 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 restrictions are implemented regarding forwarding of communications (e.g., automatic forwarding of electronic mail to external mail addresses), as applicable 5. Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging 6. Educate employees about the best practices to be followed for electronic messaging	Transitional
CO 9.7	The entity shall develop, enforce and maintain procedures to secure information transferred across business information systems, EMR and medical devices, equipment etc. The entity shall: 1. Identify all points of interconnections and integrations between business information systems and identify the information to be protected 2. Identify adequate measures to be applied to protect each type of information 3. Implement strong encryption capabilities for secure data exchange between medical devices and equipment, as applicable 4. Ensure integration of any device, solution and technology with EMR system and/or any critical infrastructure is protected by adequate measures such as encryption, secure protocols, dedicated physical connection etc.	Advanced Service Provider

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

CO 10	Electronic Commerce	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 10.1	The 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 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 and regularly monitor the same	Transitional Service Provider
CO 10.2	The entity shall protect information involved in online transactions against incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure and unauthorized message duplication or replay The 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 Service Provider

CO 10.3	The entity shall protect information available through the publicly accessible system The 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. Ensure that information available through the publicly accessible system is always available and is protected against unauthorized modification 6. Ensure non-public information is not available on publicly accessible information systems and systems are hosted in compliance with the applicable laws and regulations	Advanced

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

CM 11	Information Sharing Platforms

Control Demands		Control Criteria Basic/Transitional/Advanced
CO 11.1	The entity shall ensure that connectivity to information sharing platforms is secure and controlled The 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

UAE IAR Reference: T4.4.1, T4.4.2.

CO 12	Network Security Management	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
CO 12.1	The entity shall ensure that all networks and supporting infrastructures are adequately managed, controlled and protected The entity shall: 1. Ensure that all network components and interconnections are identified and sufficiently documented, including documentation of updates and changes incorporated via the change management process 2. Ensure that network documentation includes up to date network architecture diagrams and configuration files of devices (e.g., routers, switches) 3. Prohibit the use of insecure protocols like FTP, Telnet and use only secure protocols such as HTTPS, SFTP 4. Ensure information assets operate with only minimum needed TCP/UDP ports and disable all unused/vulnerable ports, services and protocols 5. Identify threats and vulnerabilities affecting network components and network as a whole 6. Implement specific security controls to mitigate identified vulnerabilities 7. Continually monitor implemented controls for their efficiency and effectiveness	**Basic** **Service Provider**

CO 12.2	The entity shall segregate physical, logical and wireless networks based on criticality, nature of services and user information systems The entity shall: 1. Establish criteria for network segregation. 2. Establish and maintain appropriate network security zones, allowing data flow through controlled path 3. Establish minimum and specific security requirements for each of the segregated networks, zones and resources 4. Ensure medical device and equipment network and Remote Patient Monitoring network is segregated from corporate network 5. Implement network segmentation and access control policy to allow permitted traffic to selected network devices. 6. Periodically evaluate the adequacy of implemented segregation strategy and identify areas of improvement	Transitional
CO 12.3	The entity shall ensure that all wireless networks are adequately protected The 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 public and guest access are segregated and isolated from the entity's internal network	Basic

UAE IAR Reference: T4.5.1, T4.5.3, T4.5.4

6. Data Privacy and Protection

Entities generate and utilize Personally Identifiable Information (PII) and/or Protected Health Information (PHI) and establish relations with individuals to give the information a persistent value during its lifecycle of usage and references. It is imperative that, entity implements controls to prevent the inappropriate, unintentional, unauthorized or illegal disclosure of any PII and PHI/PHI and to ensure that this standard is being followed.

PII and PHI are comprised of diverse range of data, including but not limited to:

a) Patient demographic data and general identifiers such as name, address, birth date, mobile number, Emirates ID, Email Address, Image, Vehicle number/License plate, Biometric data, IP Address etc.

b) Information on past, present or future physical or mental health condition and the provision of health care to the patient, or details of medical insurance

c) Financial Information i.e., Account number, Card details etc.

d) Medical record number, Medical reports / records (Imaging/radiology and Lab reports, Prescriptions, Vaccinations record, Diagnostic reports) whether it is in electronic or paper format

e) Information about any organ donation to/by patient, any body part or any bodily substance of that patient, or derived from testing or examination of body part

f) Genetic, biological or sexual information or condition

g) Family medical history

h) Employee's compensation details, family members details, performance reviews, passport, and National identifier details

i) Employment details, employee bank information, verification documents

Objective:

To maintain privacy and ensure the security of PII and PHI in order to retain public confidence in the government's interests and values and to maintain entity reputation while providing healthcare services.

Supporting or dependent entity policy references:

i. Information Security Policy
ii. Acceptable Usage Policy
iii. Compliance Policy
iv. Disciplinary Actions Policy

DP 1	Privacy and Protection Practices	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
DP 1.1	The entity shall develop, enforce and maintain a data privacy policy that ensures management's commitment to protect privacy of PII and PHI generated, collected and processed by the entity The policy shall: 1. Define requirements on; a) Data Generation b) Data Collection c) Data Processing d) Data Security e) Data Localization f) Data Disclosure g) Data Retention h) Data management i) Data Subject 2. Identify and define government sanctions and legal obligations. 3. Include reference to organizational disciplinary process. 4. Include references to other policies and procedures, as applicable	**Basic** **Service Provider**

DP 1.2	The entity shall implement measures to take consent from data subjects in the decision-making process while processing their PII and PHI The entity shall: 1. Restrict from processing PII and PHI without the consent of the data subject, except for: a) Processing shall be necessary to protect public interest. b) Processing shall be related to PII and PHI which became available and known by all by the act of the data subject. c) Processing shall be necessary to establish or defend any of the procedures for claiming or defending rights and legal claims or related to judicial or security procedures. d) Processing shall be necessary for the purposes of medical diagnosis, provide health treatment, health insurance services, manage health systems and services in accordance with the applicable legislation. e) Processing shall be necessary to protect public health and include protection from communicable diseases and epidemics or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices in accordance with the applicable legislation. f) At the written request of the patient (UAE national or non-national) not residing in UAE and getting non-emergency medical services as a medical tourist in a healthcare facility licensed by Department of Health, Abu Dhabi	Basic Service Provider

	g) At the request of the regulatory body(ies) for the purposes of inspection, supervision and protection of public health. h) Information exchange with Malaffi i) Processing shall be necessary to protect the data subject interests. j) Processing shall be necessary to implement specific obligations in line with applicable legislation. k) Processing shall be necessary for the completion of employment related activities. 2. Collect and store informed consent by the data subject or his/her designated representative. 3. Ensure the consent is prepared in clear, simple, and unambiguous way and is easily accessible (written or electronic) 4. Include right of data subject to withdraw or modify the consent to stop further processing of data	
DP 1.3	The entity shall ensure Lawful, Fair and Transparent Processing of PII and PHI The entity shall: 1. Ensure to have an appropriate lawful basis (or bases if more than one purpose) for processing personal data. 2. Collect sufficient and limited PII and PHI, necessary in accordance with the purpose for which the processing has to be carried out. 3. Implement measures to ensure that PII and PHI is not issued in a manner incompatible with the purpose. 4. Implement controls to ensure accuracy of PII and PHI throughout lifecycle with measures for updating it, as requested by data subject. 5. Implement controls for deletion of PII and PHI after the purpose of processing has been exhausted or in line with entity retention policy 6. Ensure compliance with requirements of applicable privacy laws and regulations	Transitional Service Provider

DP 1.4	The entity shall implement appropriate technical and organizational measures for maintaining security and privacy of PII and PHI throughout its lifecycle. The entity shall: 1. Implement information security policies, procedures, and technical controls in accordance with the requirements of this standard and the risks associated with processing PII and PHI. These include but not limited to: a) System controls: User access measures (E.g.: Physical and Logical Access Controls), Network Security, Data Security, Data concealment etc.). b) Process controls: Data classification policies, data backup and retention policy, compliance audits etc. c) People controls: Signing of Non-Disclosure Agreements (NDAs) and Data Processing Agreements (DPAs), Trainings, awareness, Employee background checks, and / or any other project specific requirements. 2. Ensure printing of PII and PHI is limited to local printers and avoid printing through uncontrolled printers 3. Ensure that only people who are physically present in the UAE or who have a valid license issued by DoH to practice their profession there, have access to systems and applications that contain PII and/or PHI. Any exemptions must be approved by entity management and then submitted to the DoH for approval. 4. Ensure health information and its copies in any form, whether encrypted, anonymized, deidentified, pseudonymized, etc., are not stored, processed, or transferred outside the UAE. Any exemptions must be approved by entity management and then submitted to the Department of Health (DoH) for further approval. 5. Access to health data shall be limited to healthcare professionals, insurance processing individuals and/or breach/compromise investigating individuals. 6. Access to health information, inclusive of personal health information and personally identifiable information, by healthcare professionals shall be based on established need (e.g., Encounter with a patient) and for the purpose of healthcare service delivery only.	Basic Service Provider

DP 1.5	The entity shall prepare Data Processing Inventory to keep track of PII and PHI stored, processed and managed and conduct Data Privacy Impact Assessment (DPIA) before implementing or acquiring information technology that stores, process, or transfers PII and PHI and/or before initiating any processing activity if it is likely to result in high risks The entity shall: 1. Ensure that the Data Processing Inventory captures information including but not limited to: a) Description of the categories of PII and PHI b) Details about the data subject c) Individuals authorized to access personal healthcare d) Period, purpose, limitation and scope e) Details about data exchange/transfer f) Mechanism of transfer, deletion, modifying or processing g) Data related to the cross-border movement, if any h) Technical and organizational measures related to information security and processing operations 2. Ensure DPIA template includes at a minimum of the following: a) Documented necessity, suitability and purpose of proposed processing operations b) Assessment of potential risks and impacts on the security of PII and/or PHI c) Documented plan of action to mitigate the risks and ensure security of PII and/or PHI d) Keep the Data Processing Inventory updated and periodically review DPIA output to assess the processing operations 3. Conduct a DPIA reassessment in response to changes in the risks associated with the processing activity	Advanced

DP 1.6	The entity shall implement measures to ensure that the involved third parties and/or data processors have controls in place for PII and PHI The entity shall: 1. Only appoint a third party and data processor that has sufficient technical and organizational measures that fulfil the secure processing requirements 2. Document security requirements within the third-party service level agreements 3. Address requirements in case of sub-contracting through contracts and service agreements 4. Ensure the third party / data processor processes data only for agreed purpose and duration and deletes the data once purpose is accomplished 5. Ensure the third parties and data processor notify the entity in case of: a) Appointment of sub-contractors b) Security incident and data breach c) Processing PII and/or PHI beyond agreed time-period	Basic Service Provider

DP 1.7	The entity shall ensure that PII and PHI breaches are detected, reported, prioritized and handled effectively The entity shall: 1. Inform DoH about breach at the entity and/or the relevant third party/data processor within predetermined timelines. Refer: Guidelines for the Implementation of the Abu Dhabi Health information and Cyber Security Standard – IM 2 - Information Security Incident Reporting matrix 2. Ensure the breach notification and further updates to DoH include all information, as requested by DoH 3. Complete and submit the "Data Breach Form" in addition to submitting incident notifications and updates. This form shall be shared with the DoH within 72 hours of acknowledging the incident. Refer: Guidelines for the Implementation of the ADHICS – Section 5- Data Breach Form 4. Document all evidence pertaining to data breaches investigation and resolution and provide DoH with the requested information within 30 working days after the initial reporting 5. Inform the affected data subject about the breach including the level of impact/damage and the measures undertaken for correction and prevention, in case of a breach that is likely to result in high risk to the data subjects 6. Entity Management shall establish process and controls to minimize probabilities of data breaches, and are accountable for any data breach involving their entity	Basic Service Provider

UAE IAR Reference: M5.2.4

DP 2	Appointment of Data Protection Officer	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
DP 2.1	The entity and the involved data processor shall appoint a Data Protection Officer (DPO) with sufficient skills and knowledge to protect protected health information if: a) Entity is processing large volumes of PII and PHI b) There is high risk due to automated and processing through technologies. c) Entity is performing profiling and comprehensive assessment of PII and PHI The entity shall: 1. Ensure there is no conflict of interest between the DPO's role, and the tasks assigned 2. Ensure contact address of the data protection DPO is well communicated to all Data Subject	Advanced

DP 3	Data Subject Rights	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
DP 3.1	The entity shall ensure protection of data subject rights while processing their PII and PHI The entity shall: 1. Fulfil data subject's request for: a) Obtaining information about their PII and PHI i.e., Type of processing, purpose of processing, sharing of data, security controls, breach management process etc. b) Transferring of their PII and PHI (to the data subject / another data controller) c) Correction and deletion of their PII and PHI d) Restriction on further processing of their PII and PHI or retaining the data for defending rights and lawsuits e) Objection to results of automated data processing and profiling 2. Keep records of PII and PHI information sharing and disclosures 3. Based on request from the data subject, Transfer the PII and/or PHI to the data subject in machine-readable format 4. Reject data subject's request to exercise its rights, if the following becomes evident: a) Request is inconsistent with the judicial procedures or investigations or matters of public interest b) Deletion of data request conflicts with any applicable legislation to which the entity is subjected to c) Request may negatively affect the efforts of the controller to protect information security d) Restriction request conflicts with consent Exemption conditions e) Request violates the privacy and confidentiality of others personal data f) Prior contract or consent is available for automated processing	Transitional Service Provider

UAE IAR Reference: M5.2.4

7. Cloud Security

Cloud services and resources provide entities with options for quick adaptation and scalability. Its critical, that foundational and essential aspect of security control are considered from the concept stage to better handle threats, technological risks, and protections of cloud environments

Entity shall implement procedures, personnel, physical and technical controls through their cloud journey, to ensure security of cloud-based data, applications, infrastructure.

Objective:

To ensure security while using cloud resources, and minimize probabilities of data compromises

Supporting or dependent entity policy references:

i. Access Control Policy
ii. Communications and Operations Management Policy
iii. Incident Management Policy
iv. Compliance Policy
v. Third Party Security Policy
vi. Data Health information Privacy Policy

CS 1	Cloud Security Policy	
	Control Demands	**Control Criteria** Basic/Transitional/Advanced
CS 1.1	The entity shall develop, enforce, and maintain a Cloud Security Policy to protect the confidentiality, integrity and availability of all IT applications, data, systems and network resources implemented in a cloud environment and ensure cloud services are acquired, used, managed, and terminated in conformity with all applicable laws and regulations. The policy shall: 1. Be relevant and appropriate to the entity's cloud security demands and applicable legal and regulatory compliance requirements 2. Demonstrate management commitment, objectives and directions 3. Establish a process that facilitates: a) Selection of suitable cloud service provider and scope of cloud services usage b) Identification of suitable information security requirements c) Signing of Service Level Agreements (SLAs) and Non-Disclosure Agreements (NDAs) d) Assignment of roles and responsibilities related to use and management of cloud services e) Agreement on data retention, portability and destruction requirements	Basic

CS 1.2	The entity shall identify and ensure implementation of information security controls to protect their cloud environment against evolving threats and risks: The entity shall: 1. Implement the Shared responsibility model for information security of the cloud and ensure that the duties for managing information security in the cloud are assigned to recognized parties, effectively communicated, and executed 2. Ensure cloud environment is physically hosted within UAE without any of the environments, infrastructures, or systems outside the country including backup and disaster recovery 3. Ensure data/health information stored in cloud is not extended for access, use or support by; a) Any other entity/party in a multi-tenant environment. b) Any entity/party that provides analytical services, where the data or copy of data is transferred/sent outside country c) Any entity/party that provides remote support from outside UAE 4. Ensure data-at-rest, data-in-transit/motion is always encrypted 5. Ensure the key used to encrypt data-at-rest and data-in-transit/motion is not provided by the cloud service provider who provides the application, infrastructure and data hosting services 6. Protect data during processing in a cloud environment 7. Procure cloud service that provides feature to generate or configure entity's own cryptographic keys to be used for applications and services in cloud 8. Ensure the cloud service provider does not store and control the entity's cryptographic keys 9. Ensure role-based security training and awareness is provided to the resources handling cloud environment 10. Engage independent external party to conduct testing of service design, service components and implemented security controls in the cloud 11. Ensure procedures are in place for ease of migration/portability for on-prem to cloud and cloud-to-cloud infrastructure, as required	Transitional Service Provider

	12. Procure cloud service that provides feature to generate or configure entity's own cryptographic keys to be used for applications and services in cloud 13. Identify security requirements and ensure implementation of controls including but not limited to: a) Secure protocols, industry standard encryption for protection of data at rest, transit & processing b) Logical segregation, access control and logging and monitoring of activities c) Controls for change management assuring adherence to the entity's change management policy d) Physical security and environmental controls for natural disasters, malicious attack or accidents e) Identification of misconfigurations and vulnerabilities on periodic basis f) Data Backup, redundancy and recovery, based on business criticality and impact assessment g) Ongoing maintenance, patching and upgrades, as required h) Incident management and Forensics requirements	

UAE IAR Reference: T6.3.1, T6.3.2

8. Third Party Security

Third Party security is critical to ensure all external stakeholders comply with entity and regulatory demands on information security, and have implemented and maintaining essential security requirements to aid in secure delivery of services, and to ensure information stored, processed, and retrieved are secure and protected always

Entity shall ensure adequate due diligence is applied to all contractual activities and services, as well as proactive identification and definition of control environment to secure entity's information assets

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

a) Reduce probabilities of information compromise

b) Secure information assets

c) Minimize unauthorized access and usage

d) Uphold organizational and governmental reputation

e) Ensure service continuity

Objective:

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

Supporting or dependent entity policy references:

i. Information Security Policy

ii. Access Control Policy

iii. Communications and Operations Management Policy

iv. Compliance Policy

v. Cloud Security Policy

vi. Data Privacy Policy

TP 1	Third Party Security Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
TP 1.1	The 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. Outline roles and responsibilities for managing the third party 3. Establish a process that facilitates: a) Security due diligence of third-party services before appointment b) Secure management of third-party services and their role in healthcare and/or related services c) Defining and including information security objectives in line with applicable mandates and/or requirements of entity d) Third party briefing of security requirements e) Security requirements for sub-contracting f) Signing service delivery agreements & non-disclosure agreements (NDAs) with third parties SLA definition and Performance monitoring 4. Demonstrate management's commitment, objectives and directions	**Basic**

UAE IAR Reference: T6.1.1

TP 2	Third Party Service Delivery and Monitoring	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
TP 2.1	The entity shall identify and enforce information security requirements, service levels and management requirements as part of relevant third-party service agreements In case the agreements are non-negotiable, the entity shall ensure that the risks are clearly identified and accepted by the management. The entity shall: 1. Define and document the type of information that third-party/service provider needs or will have access to 2. Identify security requirements to address the perceived risk associated with the services and mandates of this standard 3. Ensure that specific security requirements are included in the service delivery agreement 4. Ensure third party does not seek to use the entity's data for their own advantages or requirements 5. Include third party data center security requirements as part of the agreement, as applicable 6. Ensure the agreements cover technical support required from third parties throughout tenure of service and beyond till data is to be retained 7. Promptly notify DoH within defined timelines, in the event of any information security incident involving the third party or the service they deliver/support 8. Ensure the third party provides required support in the event of any information security incident within the scope and duration of the third-party service entity	**Basic** **Service Provider**

	9. Identify and include Right-to-Audit terms specific to the provisions and environment of service management to manage information security risks 10. 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 11. Ensure agreement includes termination clauses and transition support required from the third-party during entity decision to exit agreement and/or use another service/solution 12. These clauses shall cover at minimum below requirements: a) Data conversion to a standardized format by the third party, based on industry standard and agreement with healthcare entity b) Removal of data from all third party's environment, after an agreed period of time c) Migration of data to entity's environment d) Handover of all backup copies of data to the healthcare entity e) Disconnecting all existing integration on behalf of the healthcare entity f) Cooperation with the new onboarded third party (if any) for the required integration and data migration g) Knowledge handover to the new third party or the healthcare entity's stakeholders, based on an agreed approach	Basic Service Provider

TP 2.2	The entity shall monitor, and review services provided, reports and records submitted by third parties The entity shall; 1. Monitor compliance of security requirements identified in agreements with third parties 2. Conduct security assessments and audits in accordance with this standard's applicable mandates and the entity's information security needs 3. Implement controls for authenticating and monitoring the exchange of information between various parties to ensure security compliance 4. Assess and manage business, commercial, financial and legal risk associated with third party services	Advanced
TP 2.3	The entity shall regulate/control changes to the provisions of the signed third-party agreement through a formal management process The entity shall: 1. Ensure that changes to activities and provisions in the agreement are in compliance with security requirements 2. Include as part of the agreement, formal processes to manage changes in the agreement 3. Define parameters of change that shall be communicated and agreed between the entity and the third party	Transitional

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

9. Information Systems Acquisition, Development, and Maintenance

Entity management shall implement appropriate information systems acquisition, development, and maintenance process to avoid unauthorized alteration or misuse of information/configurations in applications, to maintain security during the in-house and outsourced development lifecycle and support procedures, and to assure protection of data used for testing. Based on detailed assessment and entity risk appetite, the entity's management shall choose from one of the below options:

a) In-house development, maintenance and support of application and systems

b) Outsource the development, maintenance and support of application and systems

c) Out-of-shelf product deployment, maintained and supported by the vendor

d) Cloud-based application utilization

e) Hybrid approach for the development, maintenance, and support requirements

Objective:

To emphasis the need for adoption of 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:

i. Access Control Policy

ii. Communications and Operations Management Policy

iii. Third Party Security Policy

iv. Compliance Policy

v. Data Privacy Policy

SA 1	Information Systems Acquisition, Development, and Maintenance Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SA 1.1	The entity shall develop, enforce and maintain an information systems acquisition, development and maintenance policy to facilitate implementation of secure system development and maintenance practices The policy shall: 1. Be relevant and appropriate to the model and relationship of the entity and involve internal and external stakeholders 2. Demonstrate management's commitment, objectives and directions 3. Establish a process that facilitates: a) Defining and including information security objectives b) Identification and mitigation of risks in involved business and application processes c) Selection of the right model and approach 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	**Basic**

UAE IAR 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 entity shall apply security engineering principles in the specification, design and development of new information systems, medical devices and equipment , applications or enhancements to existing systems, devices and applications The security requirement shall: 1. Be relevant to be used for new information assets or enhancements to existing information assets 2. Be approved by individuals authorized to do so on behalf of business and information security 3. Address all risk elements identified during risk assessments throughout the system development lifecycle 4. Address risks from all software components, medical device and equipment 5. Consider additional/compensating controls if design level risk mitigations are not possible 6. Be compliant with the requirements of this standard and secure coding practices 7. Outline validation criteria to verify security control efficiency and effectiveness. 8. Ensure no activity in development lifecycle is carried out outside the boundaries of UAE 9. Define system acceptance criteria. 10. Ensure maintenance of High-Level Design and low-level design of the System Architecture with descriptive details of every component in the architecture along with their interconnectivities	Transitional Service Provider

SA 2.2	The 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 entity shall: 1. Identify baseline training requirements that are essential for 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	Advanced

UAE IAR Reference: T7.2.1, T7.2.2

	Control Demands	Control Criteria Basic/Transitional/Advanced
SA 2.3	The entity shall incorporate validation checks into applications to detect any corruption and to ensure data is correct and appropriate The entity shall: 1. Define criteria, rules and validation parameters to validate data input into applications 2. Develop or configure applications to reject input data that is identified as incorrect or inappropriate 3. Establish minimum requirements for validation checks on internal processing of application under development to ensure correct processing of data a) Ensure application developers to provide evidence of compliance with minimum requirements b) Ensure that the incorporated validation checks are valid and relevant over a period of time and meet minimum requirements through the applications' lifecycles 4. Identify and enforce requirements to ensure authenticity and integrity of messages transmitted between systems and applications 5. Define criteria, rules and validation parameters to validate data output from applications	Transitional Service Provider
SA2.4	The 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 Service Provider

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

SA 3	Cryptographic Controls	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SA 3.1	The entity shall ensure cryptographic controls are used effectively to protect health information based on the needs of regulatory requirements and risk environment. The entity shall: 1. Use encryption for the protection of information stored and transmitted within and outside entity. 2. Establish key management process to: a) Securely generate and use cryptographic keys for applicable systems and applications. b) Securely share keys with authorized users c) Protect keys against modification, loss and destruction d) Set date of activation and deactivation for keys e) Revoke/block keys, as needed f) Backing up or archiving keys g) Recover keys that are lost or corrupted h) Replace keys when they are weakened or compromised i) Monitoring of key management related activities 3. Define standards for: a) Key strength for various environments b) Key storage	**Transitional** **Service Provider**

UAE IAR Reference: T7.4.1, T7.4.2

SA 4	Security of System Files	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SA 4.1	The entity shall control the installation of software on operational systems The entity shall: 1. Ensure software installations are carried out only by authorized resources and for justified business need 2. Keep a copy of all software installed, including any previous versions 3. Adhere to software standards and ensure only licensed software is installed on an entity system 4. Ensure that no unauthorized software is installed on entity system and maintain an up-to-date inventory of authorized software that is necessary for the entity's business needs 5. Ensure software installed in production systems are subject to entity change management process and approval	Transitional Service Provider
SA 4.2	The entity shall protect system test data and restrict access to program source code The 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, 3. Ensure health information is anonymized before being made available for testing and training purpose. 4. Maintain records of copying, using and erasing of operational information in test environment 5. Ensure that personally identifiable information is not used as test data 6. Erase any data from test applications immediately after completion of the test 7. Ensure that access to program source code is strictly based on need and is in compliance with entity access control policy	Transitional Service Provider

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

SA 5	Outsourced Software Development	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SA 5.1	The entity shall supervise and have control over outsourced software development The entity shall: 1. Ensure that the outsourced development adheres to secure engineering principles and the entity holds sole custody of the source code and source code backups. 2. Define acceptance and quality assurance processes 3. Include in the outsourced software development agreement the requirement to comply with: a) All relevant 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 4. Include in the agreement the right to audit clause 5. Conduct source code review, security assessments 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 c) Information compromise	Transitional Service Provider

UAE IAR Reference: T7.6.5

SA 6	Supply Chain Management	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SA 6.1	Prior to procurement, it is imperative for the entity to ensure that all highly critical third-party products and services conform to the information security requirements as well as comply with relevant laws, regulations, circulars, and standards	Basic Service Provider
SA 6.2	The entity shall develop a comprehensive information security strategy against supply chain threats to the information systems and application, medical devices and equipment The entity shall: 1. Define an evaluation process for suppliers of information systems, system components, medical devices and services 2. Agree with suppliers of systems, applications, medical devices equipment, related products/services on control measures and include them in the supplier contract 3. Limit sharing of configuration and architecture with suppliers 4. Limit the amount of information you share with suppliers; only share essential and relevant information on need-to-know basis through a secure channel. 5. Define acceptance criteria for all new systems and device purchases and ensure information systems, system components, and medical devices are genuine and are satisfying system acceptance requirements 6. Ensure software delivered has not been altered or modified 7. Procure and use medical devices/equipment that incorporates security features to strengthen the protection and integrity of the devices/equipment e.g., specialized security chips/coprocessors that integrate security into the devices 8. Include in the supplier contract: a) Right-to-Audit clause	Advanced Service Provider

	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	
SA 6.3	The entity shall establish processes to address weakness or deficiencies in supply chain elements The 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	Advanced Service Provider
SA 6.4	The entity shall ensure adequate supplies of critical information systems, medical devices and system/devices components The entity shall: 1. Engage with more than one supplier for critical products and systems 2. Establish contingency plans for the supply of any critical information systems, medical devices and system/device components 3. Consider stockpiling of essential and critical spare components	Advanced

UAE IAR 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

Entity's management shall be aware that information security incidents may not always be preventable, the frequency, severity, and impact on an entity's assets, reputation, financial situation, and legal standing can all be reduced with the implementation of suitable policies, processes, and technology for detection, reporting, and handling, together with education, awareness, and training.

Information security incidents shall be reported, and evidence of security incidents shall be collected and analyzed to ensure that information security events and weaknesses are properly communicated and security incidents adequately managed.

Objective:

To ensure that entity define and utilize suitable processes and resources to identify and respond to information security and privacy 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:

i. Access Control Policy
ii. Communications and Operations Management Policy
iii. Third Party Security Policy
iv. Compliance Policy
v. Data Privacy Policy

IM 1 Information Security Incident Management Policy

	Control Demands	Control Criteria Basic/Transitional/Advanced
IM 1.1	The entity shall create, implement, and uphold an incident management policy to ensure that information security and privacy incidents are addressed and managed properly, enabling prompt corrective and preventive actions. The policy shall: 1. Be relevant and appropriate to the entity's operation and risk environments. 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 and privacy incidents. 5. Establish management demands on: a) Incident identification b) Incident response c) Incident notification/communication d) Containment & Eradication e) Learning from incident	Basic

UAE IAR Reference: T8.1.1

IM 2	Incident Management and Improvements	
	Control Demands	**Control Criteria** Basic/Transitional/Advanced
IM 2.1	The entity shall establish incident management procedure to guide information security and cybersecurity response activities The entity shall: 1. Have procedures to handle incident during preparation, detection, analysis, containment, eradication, and recovery 2. Clearly document roles and responsibilities of the relevant stakeholders and management 3. Establish a formal channel for entity and external stakeholders to report information and privacy events and weakness in any information asset as soon as they are identified 4. Assess information security events and/or alerts and determine if they are to be categorized as incident 5. Inform Abu Dhabi Health SOC of the information security and privacy incidents within predetermined timeframes Refer: Guidelines for the implementation of the ADHICS – IM 2 - Information Security Incident Reporting Matrix 6. Escalate internally within the entity and externally to Abu Dhabi Health SOC, if the incident is not resolved timely 7. Ensure the incident notification includes all the information as requested by DoH. 8. Connect incident handling activities with contingency planning activities	**Basic** **Service Provider**

IM 2.2	The entity shall establish a Computer Security Incident Response Team (CSIRT) or equivalent responsible for incident management and response efforts The 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. Ensure CSIRT coordinates with its counterparts and DoH for incidents which have significant impact on the entity's assets or operations. 6. Conduct information security forensic analysis, as required 7. Participate in forensics and the national incident response effort, as required 8. Identify impactful reoccurring incidents and implement controls to reduce the recurrence 9. 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 10. Build knowledge database on information security incident diagnosis and response. 11. 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 entity shall assess and classify information security incidents The entity shall: 1. Establish an incident classification scheme which captures the requirements of matrix recommended by DoH. Refer: Guidelines for the implementation of the Abu Dhabi Health information and Cyber security Standard – IM 2 - Information Security Incident Classification 2. Define workflows to handle incidents of various classifications/severity	Transitional
IM 2.4	The entity shall test its Computer Security incident response capabilities The entity shall: 1. Develop test procedures to validate the effectiveness of its incident response capabilities periodically 2. Establish the expected outcome of test and compare test results to identify gaps 3. Modify process and procedures to address gaps identified 4. Share test results with the management	Transitional

IM 2.5	The entity shall document and preserve records on all information security incidents. The 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 considering 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. Prepare a damage assessment report 4. Conduct a post incident analysis and implement controls identified as recommendations 5. Preserve documents, records, reports and evidences in compliance with the entity's retention policy	Transitional

UAE IAR Reference: T8.2.1, T8.2.2, T8.2.3, T8.2.4, T8.2.5, T8.2.6, T8.2.7, T8.2.8, T8.2.9, T8.3.2, T8.3.3

IM 3	Information Security Events and Weakness Reporting	
	Control Demands	**Control Criteria** Basic/Transitional/Advanced
IM 3.1	The entity shall develop a situational awareness culture by participating in the information sharing community and obtaining cybersecurity information from various sources The 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

UAE IAR Reference: T8.3.1

11. Information Systems Continuity Management

Entity shall have proactive strategies and plans in place to counteract interruptions to entity operations and to protect critical business operations and processes from the consequences of significant information system, medical device and/or equipment failures to enable timely resumption of affected processes.

Objective:

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

Supporting or dependent entity policy references

i. Incident Management Policy

ii. Business Continuity Policy

iii. Business Continuity and Recovery Plan

iv. Communications and Operations Management Policy

v. Compliance Policy

vi. Backup Policy

SC 1	Information Systems Continuity Management Policy	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SC 1.1	The entity shall develop, enforce and maintain an information systems 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, medical device, equipment and application continuity during adverse situations b) Ensuring Information security during business continuity and disaster recovery c) Compliance with organizational business continuity plans d) Testing of continuity and restoration plans	Advanced

UAE IAR Reference: T9.1.1

SC 2	Information Systems Continuity Planning	
	Control Demands	**Control Criteria** **Basic/Transitional/Advanced**
SC 2.1	The entity shall conduct Business Impact Analysis (BIA) to capture information necessary to predict the impact of a critical information systems medical devices, equipment and application failure and gather information to define the strategies to mitigate or minimize the risk The entity shall: 1. Perform Risk Assessment to identify points of failure and understand likelihood, impact in time for identification and prioritization of critical Information systems 2. Determine the criticality of information systems and their need for recovery 3. Establish Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to resume activities timely and effectively 4. Identify dependencies between services and supporting resources (facilities, personnel, equipment, software, data files, system components, and vital records)	Advanced Service Provider

SC 2.2	The entity shall develop Information Systems Continuity and Recovery plans that shall prevent or minimize interruptions and support in recovery of critical information assets and services during adverse situations The plan shall: 1. Enlist information systems, medical devices, equipment and applications in scope of continuity plan 2. Identify continuity requirements for recovering from events that affect availability of critical information assets and services Have recovery strategies for critical information assets to minimize the period and impact of disruption 3. Be harmonized and support organizational business continuity planning and/or disaster recovery demands 4. Identify individuals with assigned roles and responsibilities, along with necessary contact information 5. Define call tree matrix and escalation matrix 6. Defined criteria and conditions for plan activation 7. Have provisions to address information security incident-based scenarios and provide guidance to operate and support critical business services during such scenarios 8. Ensure required level of continuity for information security during disruption 9. Consider redundant system, components or architectures for critical business services, processes and technology, wherever availability cannot be guaranteed using the existing systems architecture	Advanced Service Provider

SC 2.3	The entity shall test, reassess, and maintain its information systems' continuity plans at planned intervals or in case of any significant change, to ensure that they are up to date and effective. The entity shall: 1. Define schedules and test information system, medical devices, equipment's and application continuity plans to ensure: a) Adequacy and effectiveness of the plans b) Entity and resource readiness to execute the plans 2. Conduct fail over testing to check the efficiency of redundant information systems 3. Document test outcomes and lessons learned 4. Assess plan adequacy during changes to business services, systems and applications 5. Update and maintain information system and application continuity plans based on lessons learned and assessment outcome	Advanced

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

4.Key stakeholder Roles and Responsibilities

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

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

Stakeholder	Responsibility
Department of Health	a) Establish ADHICS. b) Enforce ADHICS Standard for Abu Dhabi Healthcare sector, covering all in scope entities, healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information. c) Maintain ADHICS Standard, based on learning and industry evolution. d) Review entity's mandatory self-assessment reports (shared by entity) and recommend improvements towards achieving compliance, and escalations where relevant Conduct review meetings with entities to enhance cybersecurity and maintain compliance. e) Develop the sector risk profiles and sector level improvement plans derived from the risk mitigation/treatment actions and report to relevant Local and Federal authorities. f) Conduct information security audits of entities periodically in line with requirements of this standard. g) Provide sector specific inputs to the National cyber threat intelligence initiatives and work in collaboration with National Authorities. h) Establish and maintain sector HIIP.
Entity Management	a) Overall accountability for complying with ADHICS Standard within respective entities. b) Fund and manage program implementation. c) Approve entity program plan, strategies, initiatives, and policies. d) Manage information security risks in accordance with the entity's risk acceptance criteria. e) Ensure periodic monitoring and review for continual improvement.
Entity - InfoSec Stakeholders	a) Ensure internal coordination and implementation of ADHICS Standard. b) Conduct periodic risk assessment exercises to identify the most critical risks and enhance/modify/amend entity's priorities, initiatives and investment accordingly. c) Monitor and report/escalate the entity's information security program

	progress to entity management and Abu Dhabi Healthcare sector – HIIP Chairperson. d) Educate business users and conduct periodic Information Security and data privacy awareness trainings/sessions. e) Ensure security requirements are adequately addressed during the design, development, implementation, and maintenance of any existing or new information systems. f) Maintain system accreditation and compliance as per policy.
Entity- External Stakeholders	a) Sign service delivery agreement and non-disclosure agreement. b) Ensure service delivery as per the agreement with entity. c) Implement all necessary information security controls as agreed with the entity. d) Maintain confidentiality of entity's data. e) Submit periodic records and reports as agreed with the entity. f) Agree to the Right to Audit clause and co-operate with entity during third-party security assessment. g) Support entity in ADHICS audit and address audit findings (if any) within the services scope. h) Ensure information security assurance in line with requirements of this standard in case of sub-contracting.
Entity Business / End User	a) Adhere to and comply with ADHICS Standard, and Entity policies and demands. b) Align business processes as per information security demands of the entity. c) Participate in all applicable information security training and other awareness programs organized by the entity.

5.Monitoring and Evaluation

The entity shall establish robust monitoring to track and evaluate compliance with the standard. Reliable metrics and measurements to be utilized to assess the effectiveness of compliance with required controls. The entity will periodically report compliance status, deviations, and risks to DoH. Risk(s) related to non-compliance shall be recorded and managed appropriately. Regular internal audits and assessments shall be conducted to validate and verify compliance with the requirements of standard. Based on the outcomes of monitoring and evaluation activities, the entity shall establish a continuous improvement process, adapting to emerging threats, technology changes and evolving compliance requirements.

DoH shall conduct periodic audits and technical assessments on all regulated entities, as relevant and applicable, to validate compliance with the requirements of standard.

6.Enforcement and Sanctions

In the event of non-compliance with the application of the terms of the standard, DoH can impose sanctions in relation to any breach of requirements under this standard in accordance with the Audit Outcomes, Complaints, Investigations, Regulatory Action and Specified Sanctions shall be applied as per the disciplinary regulation for the healthcare sector of the Emirate of Abu Dhabi.

7. Relevant Reference Documents

No.	Reference Date	Reference Name	Relation Explanation / Coding / Publication Links
1	2019	Abu Dhabi Healthcare Information and Cyber Security Standard	AAMEN | Department of Health Abu Dhabi (doh.gov.ae)
2	2019	Federal Law No. (2) of 2019 on the Use of Information and Communications Technology (ICT) in healthcare	https://mohap.gov.ae/app_content/legislations/php-law-en-77/mobile/index.html#p=1
3	2021	Federal Decree-Law no. (45) of 2021 On Data Privacy	https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws
4	2023	GP Program_National IoT Security Policy	Policies (csc.gov.ae)
5	2023	GP Program_National Cloud Security Policy	Policies (csc.gov.ae)
6	2020	Department of Health Publications: Data Privacy & Internet Of Medical Things Standard, Circulars	AAMEN | Department of Health Abu Dhabi (doh.gov.ae)
7	2020	UAE Information Assurance Regulation	https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation
8	2017	Abu Dhabi Government Data Management Standards V2.0	https://data.abudhabi/opendata/sites/default/files/AD-Gov-Data-Management-Standards-EN-v1.0.pdf
9	Draft	DOH Standard on Telemedicine	Yet to be released
10	2022	ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

11	**2015**	ISO/IEC 27017:2015	https://www.iso.org/standard/43757.html
12	**2023**	HITRUST	HITRUST Alliance | HITRUST CSF | Information Risk Management
13	**2009**	Information Security Governance – A Practical Development and Implementation Approach, by Krag Brotby	[PDF] Information Security Governance by Krag Brotby eBook | Perlego
14	**2021**	NCEMA	Publication-en.pdf.aspx (ncema.gov.ae)
15	**2019**	ISO22301:2019	ISO 22301:2019 - Security and resilience —
16	**2016**	ISO 27799:2016	ISO 27799:2016 - Health informatics —

8. Appendices

Appendix 1 - Distribution of Control

Sr. No.	Control Criteria	Number of Controls	Number of Sub-Controls	Total
1	Basic	58	274	332
2	Transitional	40	171	211
3	Advanced	33	132	165

Appendix 2 - Summary of Controls

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
Domain 1 - Human Resource Security				
HR 1 - Human Resources Security Policy				
HR 1.1 Human Resources Security Policy	3	Basic		M3.1.1, M4.1.1
HR 2 - Prior to Employment				
HR 2.1 Background Verification	6	Basic		M4.2.1
HR 2.2 Terms and Conditions of Employment	9	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 Program	5	Basic		M3.2.1, M3.3.3, M3.3.4, M3.3.5
HR 3.3 Awareness and Training	6	Transitional		M3.2.1, M3.3.3, M3.3.4, M3.3.5
HR 3.4 Role based training	2	Advanced		
HR 3.5 Disciplinary Process	2	Transitional	Service Provider	M4.3.2
HR 4 - Termination or Change of Employment and Role				
HR 4.1 Termination Responsibility	4	Basic		M4.4.1
HR 4.2 Return of Assets	3	Basic		M4.4.2
HR 4.3 Removal of Access Rights	2	Basic	Service Provider	M4.4.3

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
HR 4.4 Internal Transfers and Change of Role	3	Basic		M4.4.3
Domain 2 - Asset Management				
AM 1 Asset Management Policy				
AM 1.1. Asset Management Policy	5	Basic		T1.1.1
AM 1.2 Allocation of Medical Assets	6	Basic	Service Provider	
AM 2 Management of Asset				
AM 2.1 Asset Inventory	3	Basic	Service Provider	T1.2.1
AM 2.2 Asset Relationship	NA	Advanced		T1.2.1
AM 2.3 Asset Ownership	5	Basic		T1.2.2
AM 2.4 Acceptable Use of Assets	2	Basic	Service Provider	T1.2.3
AM 2.5 Acceptable Bring Your Own Device Arrangements	5	Basic	Service Provider	T1.2.4
AM 3 Asset Classification & Labelling				
AM 3.1 Information Classification	4	Basic	Service Provider	T1.3.1, T1.3.2
AM 3.2 Interpretation of External Entities Classification Scheme	NA	Transitional		T1.3.1
AM 3.3 Asset Tagging	NA	Transitional		
AM 4 Asset Handling				
AM 4.1 Handling Procedures	2	Basic		T1.3.3
AM 4.2 Management of Removable Media	3	Basic	Service Provider	T1.4.1
AM 4.3 Access Allocation for Medical Devices	1	Basic	Service Provider	-
AM 4.4 Security of Information within Medical Devices	4	Transitional	Service Provider	-
AM 4.5 Communication Facility for Medical Devices	NA	Transitional		-
AM 4.6 Removable Media Security	NA	Advanced		T1.4.1
AM 4.7 Removal and Movement of Information Assets	2	Transitional	Service Provider	T2.3.7
AM 5 Asset Disposal				

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
AM 5.1 Information Asset Secure Disposal	6	Basic	Service Provider	T2.3.6
AM 5.2 Records on Disposal	NA	Transitional		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	5	Basic		T2.1.1, T2.3.5
PE 2 Secure Areas				
PE 2.1 Physical Security Perimeter	5	Basic	Service Provider	T2.2.1
PE 2.2 Private Areas	NA	Advanced		
PE 2.3 Secure Areas Control Measures	9	Basic		T2.2.2, T2.2.5
PE 2.4 Ownership of Secure Areas	4	Transitional		
PE 2.5 Protection against External & Environmental Threats	5	Basic	Service Provider	T2.2.4
PE 2.6 Deliver and Loading Areas	3	Basic		T2.2.6
PE 3 Equipment Security				
PE 3.1 Equipment Siting and Protection	3	Basic	Service Provider	T2.3.1, T2.3.8
PE 3.2 Standard operating procedure for equipment's	2	Advanced	Service Provider	
PE 3.3 Cabling Security	2	Basic		T2.3.3
PE 3.4 Security of Equipment Off Site	4	Transitional	Service Provider	T2.3.5, T2.3.7
PE 3.5 Clear Desk & Clear Screen Policy	4	Basic		T2.3.9
Domain 4 - Access Control				
AC 1 Access Control Policy				
AC 1.1 Access Control Policy	9	Basic		T5.1.1
AC 2 User Access Management				
AC 2.1 User Registration and De-Registration	7	Basic	Service Provider	T5.2.1
AC 2.2 Privilege Management	7	Basic	Service Provider	T5.2.2

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
AC 2.3 Use and Management of Security Credential	10	Basic	Service Provider	T5.2.3, T5.3.1, T5.5.3
AC 3 Equipment and Devices Access Control				
AC 3.1 Access Control for Portable and Medical Devices	3	Transitional	Service Provider	T5.7.1
AC 3.2 Access Control for Assets and Equipment in Teleworking Sites	3	Transitional	Service Provider	T5.7.2
AC 3.3 Telehealth Security	NA	Basic	Service Provider	
AC 4 Access Reviews				
Ac 4.1 Review of User Access Rights	4	Basic	Service Provider	T5.2.4
AC 5 Network Access Control				
AC 5.1 Access to Network and Network Services	4	Basic	Service Provider	T5.4.1, T5.4.2, T5.4.5
AC 5.2 Equipment Identification in Network	NA	Advanced		T5.4.3
AC 5.3 Remote Diagnostic and Configuration Protection	3	Advanced		T5.4.4
AC 5.4 Network Routing Control	8	Transitional	Service Provider	T5.4.6
AC 5.5 Wireless Access	3	Transitional		T5.4.7
AC 6 Operating System Access Control				
AC 6.1 Secure Log-On Procedures	4	Basic	Service Provider	T5.5.1
AC 6.2 User Identification and Authentication	2	Basic	Service Provider	T5.5.2
AC 6.3 Use of System Utilities	4	Advanced		T5.5.4
Domain 5 - Communications and Operations Management				
CO 1 Communications and Operations Management Policy				
CO 1.1 Communication and Operation Management Policy	2	Basic		T4.1.1
CO 2 Operational Procedures and Responsibilities				
CO 2.1 Baseline Configuration	2	Transitional	Service Provider	T3.2.1
CO 2.2 Documented Operating Procedure	4	Advanced		T3.2.2
CO 2.3 Change Management	5	Transitional		T3.2.3, T.7.6.1, T7.6.3, T7.6.2

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
CO 2.4 Separation of Test, Development and Operational Environment	6	Transitional	Service Provider	T3.2.5
CO 3 Planning and Acceptance				
CO 3.1 Capacity Management	5	Advanced		T3.3.1
CO 3.2 System Acceptance and Testing	6	Transitional	Service Provider	T3.3.2
CO 4 Malware Protection				
CO 4.1 Controls Against Malware	11	Transitional	Service Provider	T3.4.1
CO 4.2 Gateway Level Protection for Malware	2	Advanced		T3.4.1
CO 5 Backup and Archival				
CO 5.1 Backup Management	6	Basic	Service Provider	T3.5.1
CO 5.2 Archival Requirements	6	Advanced	Service Provider	T3.5.1
CO 6 Logging and Monitoring				
CO 6.1 Logging and Monitoring Procedures	11	Advanced	Service Provider	T3.6.1, T3.6.2
CO 6.2 Preservation of Log Information	5	Advanced		T3.6.4
CO 6.3 Clock Synchronization	3	Basic		T3.6.7
CO 6.4 Information Leakage	1	Transitional	Service Provider	T7.6.4
CO 7 Security Assessment and Vulnerability Management				
CO 7.1 Technical Vulnerability Assessment and Penetration Testing	7	Advanced	Service Provider	T7.7.1
CO 7.2 Security of Assessment Data	3	Advanced	Service Provider	T7.7.1
CO 8 Patch Management				
CO 8.1 Patch Management Procedure	9	Basic	Service Provider	
CO 8.2 Tracking of Patches	NA	Advanced		
CO 9 Information Exchange				
CO 9.1 Information Exchange Procedures	4	Transitional		T4.2.1
CO 9.2 Secure Practices for Information Exchange	13	Basic	Service Provider	T4.2.2

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
CO 9.3 Information Exchange Agreements	6	Basic	Service Provider	T4.2.2
CO 9.4 Physical Media in Transit	6	Basic	Service Provider	T4.2.3
CO 9.5 Restrict usage of Public Domain Email	NA	Basic	Service Provider	
CO 9.6 Electronic Messaging Protection	6	Transitional		T4.2.4
CO 9.7 Secure Transfer across Business Information System	4	Advanced	Service Provider	T4.2.5
CO 10 Electronic Commerce				
CO 10.1 Security of Electronic Commerce Services	3	Transitional	Service Provider	T4.3.1
CO 10.2 Online Transaction	3	Transitional	Service Provider	T4.3.2
CO 10.3 Publicly Available Information	6	Advanced		T4.3.3
CO 11 Information Sharing Platforms				
CO 11.1 Connectivity to Information Sharing Platforms	4	Advanced		T4.4.1, T4.4.2
CO 12 Network Security Management				
CO `12.1 Network Controls	7	Basic	Service Provider	T4.5.1
CO 12.2 Segregation in Networks	6	Transitional		T4.5.3
CO 12.3 Security of Wireless Networks	3	Basic		T4.5.4
Domain 6 - Data Privacy and Protection				
DP1 Privacy and Protection Practices				
DP 1.1 Data Privacy Policy	4	Basic	Service Provider	NA
DP 1.2 Consent Collection	4	Basic	Service Provider	NA
DP 1.3 Lawful, Fair and Transparent Processing Procedures	6	Transitional	Service Provider	NA
DP 1.4 Technical and organizational measures	6	Basic	Service Provider	M5.2.4
DP 1.5 Data Processing Inventory and Data Privacy Impact Assessment (DPIA)	3	Advanced		NA
DP 1.6 Data Processors security	5	Basic	Service Provider	NA
DP 1.7 Data Breach Management	6	Basic	Service Provider	NA

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
DP2 Appointment of Data Protection Officer				
DP 2.1 Requirement for Appointing Data Protection Officer	2	Advanced		
DP3 Data Subject Rights				
DP 3.1 Protection of data subject rights	4	Transitional	Service Provider	
Domain 7 - Cloud Security				
CS 1 Cloud Security Policy				
CS 1.1 Cloud Security Policy	3	Basic		T6.3.1
CS 1.2 Cloud Security Controls	13	Transitional	Service Provider	T6.3.2
Domain 8 - Third Party Security				
TP 1 Third Party Security Policy				
TP 1.1 Third Party Security Policy	4	Basic	Service Provider	T6.1.1
TP 2 Third Party Service Delivery and Monitoring				
TP 2.1 Third-Party Service Delivery Agreements	12	Basic	Service Provider	T6.2.1
TP 2.2 Monitoring and Review of Third-Party Services	4	Advanced		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	4	Basic		T7.1.1, T7.4.1
SA 2 Security Requirement of Information Systems and Applications				
SA 2.1 Security Requirements Analysis and Specification	10	Transitional	Service Provider	T7.2.1
SA 2.2 Developer Training	5	Advanced		T7.2.2
SA 2.3 Correct Processing in Applications	5	Transitional	Service Provider	T7.3.1, T7.3.2, T7.3.3, T7.3.4
SA 2.4 Off-line Processing Capabilities	1	Transitional	Service Provider	T7.3.2
SA 3 Cryptographic Controls				

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
SA 3.1 Cryptography and Key Management	3	Transitional	Service Provider	T7.4.1, T7.4.2
SA 4 Security of System Files				
SA 4.1 Control of Operational Software	5	Transitional	Service Provider	T7.5.1
SA 4.2 Protection of System Test Data and Source Code	7	Transitional	Service Provider	T7.5.3
SA 5 Outsourced Software Development				
SA 5.1 Outsourced Software Development	6	Transitional	Service Provider	T7.6.5
SA 6 Supply Chain Management				
SA 6.1 Secure Acquisition	NA	Basic	Service Provider	
SA 6.2 Supply Chain Protection Strategy	8	Advanced	Service Provider	T7.8.1, T7.8.2, T7.8.3, T7.8.4, T7.8.5
SA 6.3 Process to Address Weakness or deficiency	3	Advanced	Service Provider	T7.8.6
SA 6.4 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	5	Basic		T8.1.1
IM 2 Incident Management and Improvements				
IM 2.1 Incident Response Procedure	8	Basic	Service Provider	T8.2.1, T8.3.3
IM 2.2 Computer Security Incident Response Team	11	Advanced		T8.2.2
IM 2.3 Incident Classification	2	Transitional		T8.2.3
IM 2.4 Incident Response Testing	4	Transitional		T8.2.5
IM 2.5 Incident Records	5	Transitional		T8.2.7
IM 3 Information Security Events and Weakness Reporting				
IM 3.1 Situational Awareness	3	Advanced		T8.3.1
Domain 11 - Information Systems Continuity Management				
SC 1 Information Systems Continuity Management Policy				

Control Number & Control Name	Number of Sub-Control	Control Criteria	Service Provider Controls	UAE IAR Reference
SC 1.1 Information Systems Continuity Management Policy	4	Advanced		T9.1.1
SC 2 Information Systems Continuity Planning				
SC 2.1 Business Impact Analysis	4	Advanced	Service Provider	
SC 2.2 Developing Information Systems Continuity Plans	9	Advanced	Service Provider	T9.2.1
SC 2.3 Testing, Maintaining and Reassessing Plans	5	Advanced		T9.3.1