دائـــرة الـــصـــحـــة
DEPARTMENT OF HEALTH

# ABU DHABI HEALTHCARE INFORMATION AND CYBER SECURITY STRATEGY

# TABLE OF CONTENTS

1. Introduction 6

2. Vision & Mission 9

3. Abu Dhabi Health Sector Target State 10

4. Our Approach 12

5. Information & Cyber Security Strategy for Abu Dhabi's Healthcare Sector 14

6. The Way Forward 28

## 1.1 Background

Technological evolution has become an essential business, industry, and government enabler for global economies. This technological evolution has played a vital role within the healthcare sector, enhancing patient care effectiveness and safety. New digital trends are becoming increasingly popular, such as wearable devices enable the patients to augment their health records, as well as networked devices, allow remote monitoring and patient care.

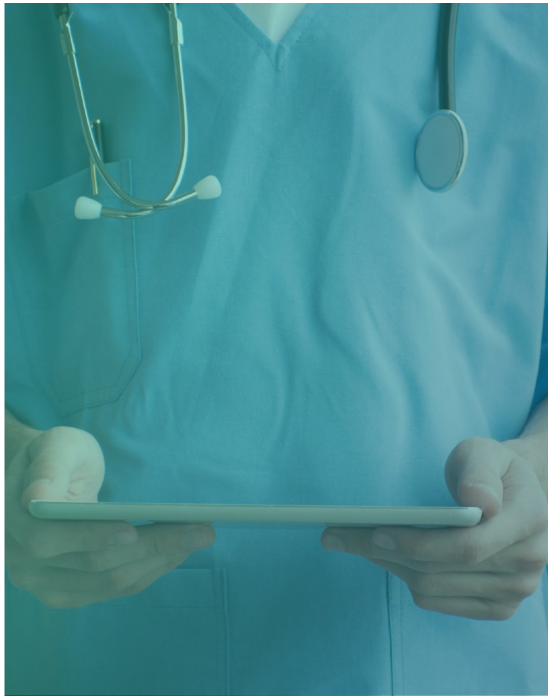
These resources and systems are open to several threat vectors, even nation-state attack. In nearly all cases, these threats are focused on capturing health-related data for vested interests or looking to monetise valuable protected health information (PHI). The healthcare industry shall prioritise information security and cybersecurity in their agenda to minimise the risk associated with data loss, reputational damage and potential financial losses.

A concerted effort and structured approach are required to manage and protect the cybersecurity posture; not only to ensure the safety of the patient but also to maintain trust in healthcare services. A structured approach to cybersecurity for establishing a range of objectives and priorities, driven by the information and cybersecurity strategy is required.

## 1.2 Purpose

The purpose of the healthcare information and cybersecurity strategy is to define a high-level top-down approach applying a consistent cybersecurity framework. The strategy supports healthcare sector objectives, priorities, and is safeguarding Abu Dhabi’s healthcare sector from cyber threats.

The healthcare information and cybersecurity strategy will provide a cohesive and proactive response to the current and future healthcare cybersecurity challenges for the Emirate of Abu Dhabi. Moreover, it supports the objective of digital transformation by enabling technology, innovation and AI adoption in Abu Dhabi healthcare sector. The strategy aligns the healthcare sector cybersecurity initiatives with UAE national cybersecurity initiatives.



## 1.3 Scope

The strategy asserts a series of recommended actions. Department of Health (DOH) will ensure that the Abu Dhabi healthcare information and cybersecurity strategy is uniformly implemented across the healthcare sector in Abu Dhabi.

The scope of this strategy covers:

- All information and cybersecurity aspects of the healthcare sector and healthcare services within the Emirate of Abu Dhabi.
- Healthcare professionals, healthcare facilities, insurance providers, service providers, vendors and third parties who have access and handling/ processing/ accessing/managing/storing patient information and operating within the emirate of Abu Dhabi.

Each health sector facility is responsible for its information and cybersecurity posture. DOH, as the owner of this strategy, will align the Abu Dhabi health sector to the national mandate of enhancing the overall security posture. With the vision for the next five years, DOH will drive the successful implementation of various initiatives for the Abu Dhabi healthcare sector.

# 2 VISION & MISSION

The vision is an important element of the strategy. It seeks to outline the purpose, direction, and guiding values for the journey. The vision and mission are developed in alignment with and prioritized from superior vision and mission statements, especially considered (i) Abu Dhabi Department of Health, (ii) Abu Dhabi Digital Authority and the (iii) UAE-wide cybersecurity strategy.

The Abu Dhabi Healthcare Information and Cyber Security Vision is:

> To enable the cyber-secure digital transformation of the healthcare services and to provide adequate assurance on information security, while enhancing the consumer experience in healthcare delivery.

Additionally, a mission provides general statements on how the sector will achieve the outlined vision in terms that are more practical and combines forward-thinking with present goals.

The Abu Dhabi Healthcare Information and Cyber Security mission is to enable safe, secure and sustainable digital healthcare services by:

- Establishing a leadership oversight of the health sector.
- Enabling resilient infrastructure for quick response and recovery.
- Developing and enabling an efficient cybersecurity workforce.
- Establishing a sector-wide risk management methodology.
- Enhancing healthcare policies and standards.
- Establishing an environment to nurture cybersecurity partnership and innovation.

In terms of next steps, the defined high-level top-down approach via Vision & Mission enables us to define an appropriate target state and follow-up on sector objectives and priorities that shall be achieved in a specific timeframe.

# 3 ABU DHABI HEALTH SECTOR TARGET STATE

The objective of Abu Dhabi information and healthcare cybersecurity strategy is to provide a strong, cohesive and proactive response to the current as well as future healthcare cybersecurity challenges for the Emirate of Abu Dhabi.

Based on analysis and comparison with global cybersecurity maturity models, the target state maturity for the healthcare sector cybersecurity can be defined as follows:

- Sustainable cybersecurity governance, established strategy and associated processes with appropriate oversight.
- Role-based sustainable cybersecurity awareness resulting in greater focus on security initiatives.
- Readiness for handling cybersecurity related incidents with prompt response and recovery capabilities.
- Skilled resources and cybersecurity related processes to ensure the success of security initiatives.
- Cohesive practices between vendors, partners within the healthcare sector for collaborative mitigation of sector-related cybersecurity threats and vulnerabilities.
- Adoption of global technology trends in Abu Dhabi healthcare sector within acceptable risk limits.

Key considerations for achieving the target state should be to mitigate the current healthcare sector challenges and the future potential risk areas.

# 4 OUR APPROACH

To enable the vision for the healthcare information and cybersecurity strategy, the Department of Health (DOH) has taken the initiative of defining the Abu Dhabi healthcare information and cybersecurity strategy.

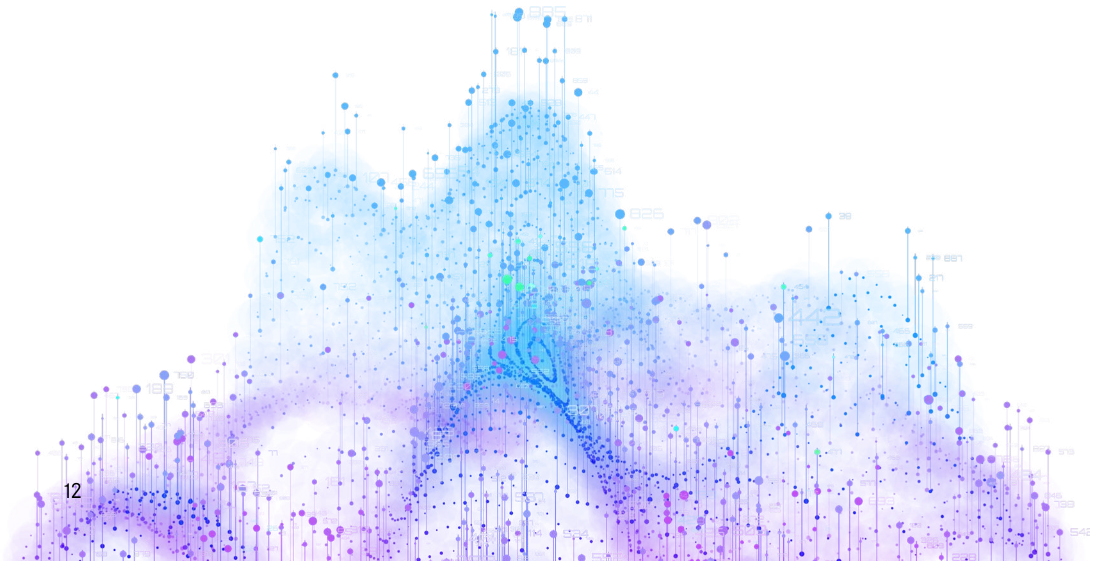
Developing the strategy requires a clear understanding of what the global leaders have done in healthcare cybersecurity space. DOH worked in a collaborative approach with various stakeholders to define and develop this strategy.

The benchmarking exercise started with the identification of countries that currently demonstrate a high cybersecurity maturity and ranking in healthcare. During the benchmarking exercise, inputs were collected from various resources, including the Global Cybersecurity Index (GCI), geography-specific peers, headline makers, early adopters and countries identified as being leaders in cybersecurity policy.

Comprehensive maturity assessment of Abu Dhabi healthcare sector was conducted against the best practices and compliance regulations of information security and privacy standards. Key focus areas and objectives were identified for internal and external stakeholders.

Alignment with overall DOH strategy and other digital transformation initiatives was conducted to identify the healthcare cybersecurity vision, mission and directives.

To achieve the target state for the Abu Dhabi healthcare sector, DOH has defined an Abu Dhabi healthcare information and cybersecurity strategy with six pillars.



### CYBER SECURITY GOVERNANCE

Enhance leadership oversight by establishing a dedicated cyber security governance frame work

### CYBER SECURITY RESILIENCE

Ensure the capabilities for response and recovery from cyber threats

### CYBER SECURITY CAPABILITIES

Develop relevant knowledge, and abilities to secure the cyber environment

### CYBER SECURITY PARTNERSHIPS

Enhance effective collaboration with multi-lateral partners to enhance the cyber space

### CYBER SECURITY MATURITY

Ensure the cyber security awareness and frameworks for adequate management of cyber threats

### CYBER SECURITY INNOVATION

Establish sustainable innovation as cyber security enabler

**Objectives**

**Initiatives**

**Outcome**

The objectives, key initiatives and action plans for each of the pillars are identified based on the inputs from healthcare entities and stakeholders.

5

# INFORMATION & CYBER SECURITY STRATEGY FOR ABU DHABI'S HEALTHCARE SECTOR

## 5.1 Pillar one: Cyber Security Governance

This pillar establishes a governance framework for information security and cybersecurity. The sector governance framework will establish not only a dedicated leadership and an adequate organizational structure but also comprehensive processes to achieve and sustain strategic objectives.

### 5.1.1 Strategic objectives and initiatives

**Objective One**

Establish a robust information and cybersecurity governance framework with a clear set of accountabilities and responsibilities.

**Initiatives**

- Establish adequate internal structures for efficient operations and delivery of entrusted responsibilities.
- Establish necessary committees and forums to manage internal and external communications, operations and compliance as well as discuss issues and enhancements.
- Establish adequate tools & technologies for the effective implementation of the information and cyber security governance framework.

### 5.1.2 Desired outcome

- Sector-wide participation in governance meetings, on defined frequency, to review cybersecurity performance.
- Term of reference along with accountabilities and responsibilities defined and established to enable adequate sector and internal governance.
- Sector-wide monitoring tools and technologies implemented and operated to support the cybersecurity governance framework.
- Defined and established sector-wide cybersecurity monitoring and reporting parameters for leadership oversight and improvements.

## 5.2 Pillar two: Cyber Security Resilience

This pillar focuses on ensuring a robust environment for Abu Dhabi's healthcare sector when faced with cyber threats. This includes the ability to withstand all types of attacks, rapidly recover from adverse effects, and limit the damage of attacks on business, people and society. Equally important is the focus on preparing for and adapting to changing conditions.

### 5.2.1 Strategic objectives and initiatives

#### Objective One

Establish a cyber-response framework for the healthcare sector with the management of cybersecurity incidents threats and risks.

#### Initiatives

- Setup best practices, guidelines and playbooks, with the aspect on how the healthcare sector needs to manage cybersecurity incidents and vulnerabilities.
- Establish an advanced incident management team with appropriate skillset to handle cybersecurity incidents.
- Enhance situational awareness for incident detection and tactical response by enabling real-time threat information sharing between the healthcare sector entities.
- Enhance information exchange between Abu Dhabi cyber threat intelligence centre (CTIC) and Abu Dhabi healthcare sector CERT on healthcare-specific threat information.

#### Objective Two

Mitigate identified issues and vulnerabilities in systems, application and infrastructure with a risk-based approach.

#### Initiatives

- Enhance standards and best practices for risk management for medical devices and healthcare services.
- Collaborate with authorities and stakeholders to setup adequate hardening regulations & processes to ensure healthcare sectors secure environment for IT infrastructure, IT network and medical devices.
- Define a systematic approach for legacy and new systems, application and infrastructure in terms of their cybersecurity life cycle (e.g. patching, implementation of compensation controls, segmentation, replacements).

### Objective Three

Establish a sector-wide continuity plan for cybersecurity.

### Initiatives

- Establish continuity policies for the healthcare sector as per business continuity management (BCM) standard guidelines (NCEMA 7000).
- Ensure continuity plans are validated by identifying and testing of critical IT systems failover and are exercised frequently.

## 5.2.2 Desired outcome

- Sector-wide adherence to cyber response framework to manage cybersecurity incidents.
- Established incident management team with adequate skills, defined best practices, measurements and guidelines for cybersecurity incident handling.
- Dissemination of real-time and situation based threat information to health sector stakeholders.
- Established communication and collaboration with other federal entities for threat information sharing.
- Enhanced standards and frameworks enforced to the healthcare sector.
- Proof of progressive existence of hardening regulations.
- Developed and established systematic approach for legacy and new systems, application and infrastructure in terms of their cybersecurity life cycle.
- Defined continuity policies and plans are established for cybersecurity with assigned roles and responsibilities.
- Periodic plan and testing of cybersecurity BCP and DR plans.

# 5.3 Pillar three: Cyber Security Capabilities

This pillar focuses on the development of relevant knowledge, skills and abilities to enhance the ability to address cybersecurity risks and threats. This includes the development of functionalities and capabilities to facilitate technology innovation in care delivery and patient health.

## 5.3.1 Strategic objectives and initiatives

### Objective One

Establish a technology environment to nurture and enable secure enterprise technology platforms and digital transformation.

### Initiatives

- Promote cybersecurity as a core feature of service design and use design thinking to build secure and convenient customer experiences.
- Promote automation and orchestration technology to reduce time lags and delays in security processes and interactions to improve identification and response for cyber threats.
- Enable secure and relevant healthcare information exchange of patient information between healthcare service providers, insurance agencies and patients.

## Objective Two

Improve healthcare information and cybersecurity awareness within the sector by establishing the understanding of implications for people, process, and technology.

## Initiatives

- Build executive education and awareness programs targeting all healthcare sector leadership and staff to ensure adequate awareness and a greater focus on security initiatives.
- Develop and conduct role-based cybersecurity awareness workshops and awareness campaigns for all relevant stakeholders, including patients and staff.
- Promote skill enhancement for all healthcare workforce through multiple avenues for learning cybersecurity through industry-academia collaboration.

## 5.3.2 Desired outcome

- Standardized security practices and guidelines through the life cycle process of software/application/system development and usage.
- Enhanced capabilities to identify and recover from cyber threats due to automation and orchestration technologies.
- Established guidelines and enhanced secure information exchange platform for secure and relevant healthcare information exchange between healthcare service providers, insurance agencies and patients.
- Enhanced awareness and focus of healthcare business leadership on cyber security to improve management buy-in for critical cybersecurity initiatives.
- Enhanced role-based awareness of all stakeholders about the cyber threats and cyber hygiene, improving the identification, response and recovery time for cybersecurity incidents.
- Organize seminars and training sessions for healthcare workforce to promote cybersecurity skill enhancement.

## 5.4 Pillar four: Cyber Security Partnerships

The focus of this pillar is to ensure effective collaboration with multi-lateral partners to enhance the security of the healthcare cyberspace. The intent is to guard against cyber threats, increase information sharing of threat vectors and take actions on cyber actors across multiple states entities and boundaries.

### 5.4.1 Strategic objectives and initiatives

#### Objective One

Develop local and international consortiums to improve collaboration among the cybersecurity community.

#### Initiatives

- Establish regional and international consortiums to share, discuss and manage healthcare cybersecurity issues and risks with other sectors.
- Collaborate with biomedical teams to establish cybersecurity hygiene practices and quality checklists for biomedical devices.
- Collaborate with vendor, partners and stakeholders to promote secure by design principles into the product development.

#### Objective Two

Promote cyber threat intelligence platforms and forums for sharing healthcare-specific threat information.

#### Initiatives

- Increase outreach and engagement for cybersecurity across healthcare and other sectors for knowledge and information exchange.
- Setup, maintain and promote a central body of knowledge for medical IT/medical devices, to collect identified vulnerabilities, patches, common issues and how to resolve them.

### 5.4.2 Desired outcome

- Abu Dhabi promoted as a global leader in cyber-secure healthcare sector by establishing consortiums, cohesive partnerships and collaboration on mitigating healthcare cybersecurity threats and risks.
- Develop a checklist and guidelines for biomedical teams for quality checks and cybersecurity assessment of medical devices.
- Established cohesive partnership with vendors and partners to establish cybersecurity as a shared responsibility.
- Established threat intelligence information and knowledge sharing platforms for various stakeholders and sector.
- Published body of knowledge for identified vulnerabilities and patches for the devices and common issues.

## 5.5 Pillar five: Cyber Security Maturity

This pillar focuses on enhancing the maturity of cybersecurity-related practices and processes. A continuous process of evaluating the effectiveness of controls and security framework is essential. With an evolving threat landscape, establishing a mature and evolving cybersecurity framework for enhancing the capabilities should be mandated.

### 5.5.1 Strategic objectives and initiatives

#### Objective One

Enhance the healthcare information and cybersecurity framework with required legislation and industry demands on people, process and technology, and introduce measurements of their adherence.

#### Initiatives

- Establish an audit and monitoring program for the healthcare sector to evaluate the implementation status and adherence of the healthcare standards and required policies.
- Establish a process to conduct annual assessments for evaluation of current information and cybersecurity standards against global best practices and emerging technology trends.
- Complement the healthcare information and cybersecurity framework with required policies, standards and guidelines as well as checklists on people, process and technology.

#### Objective Two

Strengthen the protection of healthcare information against unauthorized access by introducing necessary security mechanism for digital infrastructure.

#### Initiatives

- Set up internal structures and controls to manage data privacy in line with applicable legislation and regulations.
- Work with authorities to establish a certification/accreditation process for systems handling healthcare data and connected medical devices.
- Develop and establish specific practices, protocols as well as technical specifications for secure exchange and management of patient records.

### 5.5.2 Desired outcome

- Sector wide compliance status with legislations, cyber security standards and risk management framework.
- Updated information and cyber security standards based on review findings, addressing industry demands and legislative requirements on a yearly cycle.
- Established process for development and maintenance of supporting policies, standards, guidelines etc.
- Defined roles and responsibilities within healthcare sector to manage and address the requirements of the data privacy legislation and standards.
- Sector wide compliance of healthcare systems and connected medical devices with Abu Dhabi cyber security and data privacy and other legal and regulatory requirements.
- Established secure healthcare information exchange mechanism towards achieving DOH vision of ‘healthy and safe Abu Dhabi’.

## 5.6 Pillar six: Cyber Security Innovation

This pillar focuses on to bringing sustainable innovation as an enabler for cyber security, by adopting the trends in healthcare technology to anticipate better care delivery for future with minimum threat landscape. This includes not just the technology domain, but also people and process aspects.

### 5.6.1 Strategic objectives and initiatives

#### Objective One

Regulate and enable the healthcare innovation eco-system for cyber secure transformation.

#### Initiatives

- Establish regulations, standards and policies to support innovation by secure adoption.
- Enhanced change management process through innovation for secure adoption during changes.

#### Objective Two

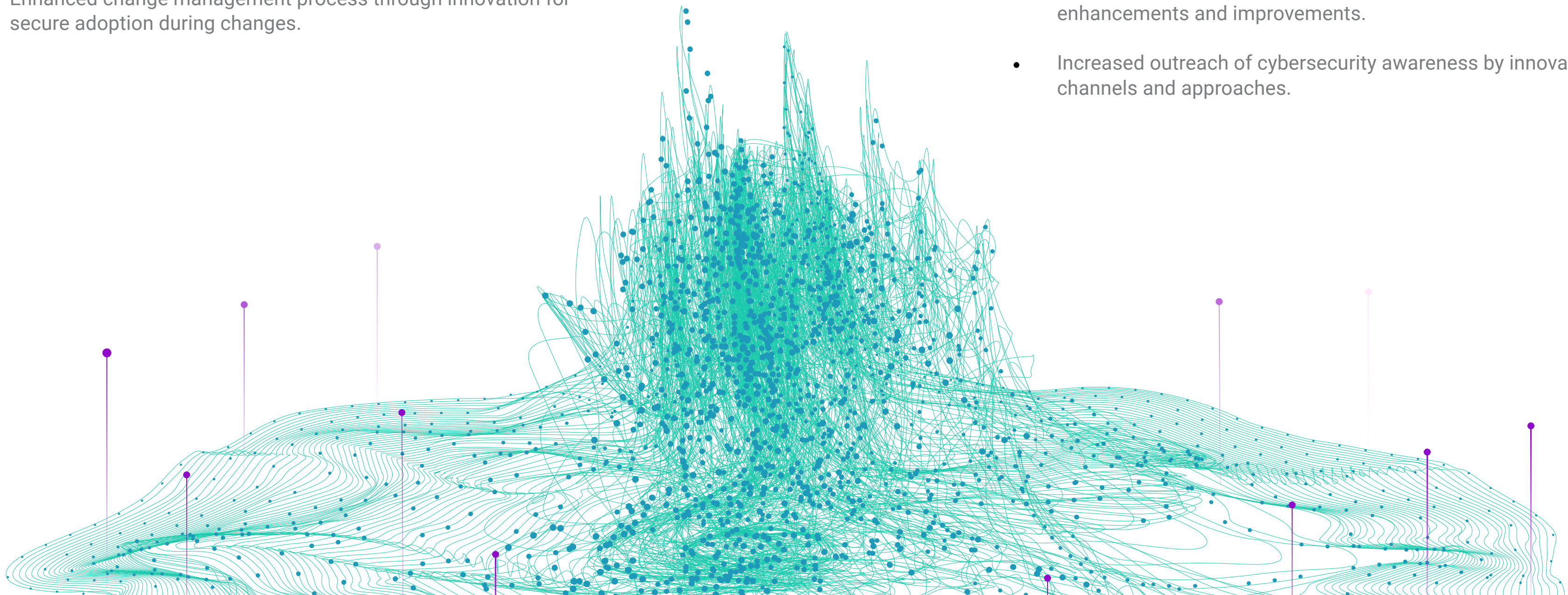
Promote the adoption of secure innovation while enhancing/improving care delivery and cybersecurity maturity of the healthcare sector.

#### Initiatives

- Identify, promote and adopt emerging technologies from across the sectors and global peers to improve the security posture of the healthcare sector.
- Promote and encourage innovation in raising the awareness about healthcare cybersecurity threats, risks and required precautions.

### 5.6.2 Desired outcome

- Established secure practices for adopting innovations with required regulations, standards/policies and guidelines.
- Enhanced and enforced IT change control for secure deployment.
- Adopted innovative technologies for care delivery and cybersecurity enhancements and improvements.
- Increased outreach of cybersecurity awareness by innovative channels and approaches.



# 6 THE WAY FORWARD

The vision of the national leadership is to guarantee cybersecurity initiatives as the enabler for growth and provides public safety, confidence and trust. In healthcare management, the most vital tenet is maintaining patient trust, with both healthcare facilities and services. Information and cybersecurity strategy focuses on building confidence in the digital services provided.

There is great potential in improving the healthcare sector through a digital transformation but will require solving some unique challenges. Globally the healthcare sector is one of the most targeted industries for cybercrime and cyberattacks. Abu Dhabi, due to its geopolitical situation and the thriving economy, faces persistent cyber threats against critical infrastructure and services operations. All vulnerabilities must be identified and mitigated; else, threat actors could exploit and impact patient safety.

The release of the healthcare information and cybersecurity strategy marks both an essential initial milestone and a critical inflexion point in the ongoing cybersecurity journey for the Emirate of Abu Dhabi. Operationalising the plan and executing the various initiatives is an essential next step to achieving success for the overall strategy and national initiatives for cybersecurity.

Cybersecurity is dynamic and ever-changing. By adopting the principles highlighted in this document, we seek to establish a safe and secure healthcare sector aligned to the UAE leadership vision for a cyber-secure Abu Dhabi.

https://doh.gov.ae/