



دائرة الصحة  
DEPARTMENT OF HEALTH


# DOH INTERNET OF MEDICAL THINGS (IoMT) SECURITY STANDARD

October 2020

PUBLIC

عام



|   |  |
|---|--|
| <br>دائرة الصحة<br>DEPARTMENT OF HEALTH  |  |
| <b>Document Title:</b>  | DOH Internet of Medical Things (IoMT) Security Standard  |
| <b>Document type</b>  | Standard   |
| <b>Document Ref. Number:</b>  | DOH/SD/IoMT/0.9  |
| <b>Effective Date:</b>  | The effective date of this Standard will be the date of its publication.   |
| <b>Previous versions</b>  | N/A  |
| <b>Document Owner:</b>  | Support Services Division  |
| <b>Applies to:</b>  | This standard covers all health care entities and services within the Emirate of Abu Dhabi, and shall be applicable to all healthcare/medical facility(s), healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s). |
| This document should be read in conjunction with Federal laws and DOH regulations including: <ul style="list-style-type: none"> <li>• Federal laws on Medical Liability and the Practice of Human Medicine,</li> <li>• Legal requirement for Patient consent and confidentiality of patient information,</li> <li>• DOH Manuals,</li> <li>• Abu Dhabi Healthcare Information and Cyber Security Standard,</li> <li>• DOH Data Management Policy and DOH Data Standards,</li> <li>• DOH Policy on Health Information Exchange,</li> <li>• DOH Policy on Digital Health</li> <li>• DOH Policy on Artificial Intelligence in the Healthcare Sector of the Emirate of Abu Dhabi,</li> </ul> |  |



## Table of Contents

|  |    |
|--|----|
| 1. Purpose .....   | 4  |
| 2. Scope .....   | 4  |
| 3. Definitions and Abbreviations .....                             | 4  |
| 4. Requirements.....   | 6  |
| 4.1 Onboarding a device .....                                      | 6  |
| 4.2 Security Requirements: .....                                   | 6  |
| 4.3 Additional Requirements: .....                                 | 8  |
| 4.4 Exceptions: .....  | 8  |
| 5. Enforcement and Compliance .....                                | 9  |
| 6. Appendix.....   | 10 |
| 6.1 Architecture of general IoT communication.....                 | 10 |
| 6.2 Security areas to be considered while procuring a device ..... | 10 |



## 1. Purpose

This Standard sets out mandatory requirements for the security of Internet of Medical Things (IoMT), the collection of medical devices and applications that connect to healthcare IT systems through information and communication technologies to collect, store, exchange and process information. As many devices are not able to satisfy every mandate due to their real-world limitations, entities may consider the trade-off between the limitations and the risks, and document the risks for where and how the device may be used.

## 2. Scope

- 2.1 All health care entities operating out of the Emirate of Abu Dhabi using IoMT devices and/or planning to use such devices .
- 2.2 All healthcare professional(s) and support staff who have access to patients' health/diagnostic/personal information, diagnostic lab(s), pharmacy(s) and insurance provider(s).

## 3. Definitions and Abbreviations

| Term                                | Definitions / Abbreviations  |
|-------------------------------------|--|
| Authentication                      | Process of verifying a claim of identity   |
| Authorization                       | Authorization is a mechanism of granting / validating access rights / privileges to resources,   |
| Access Control                      | Mechanism to enable authorized people to access physical or digital entity resources, while preventing unauthorized people from doing the same.  |
| Cryptography                        | Cryptography is the science of Information Security. Cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).   |
| Critical information infrastructure | Entity's Assets, including organizations, which provide essential services   |
| Data                                | All that can be stored, processed, generated and transferred such as numbers, letters, symbols, images and the like.<br>Health Information: Health data processed and made apparent and evident whether visible, audible or readable, and which are of a health nature whether related to health facilities, health or insurance facilities or beneficiaries of health services. |
| Entity                              | Entity in Abu Dhabi providing health services, health insurance services, facilitation, claims management, electronic health services,   |



|                                   |  |
|-----------------------------------|--|
| Exchange of Health information    | Access, exchange, copying, photocopying, transfer, storage, publication, disclosure or transmission of health data and information.  |
| Health Authority                  | Any federal or local governmental body concerned with health affairs in the country. (DOH – Department of Health)  |
| Incident                          | An incident is an event that could lead to loss of, or disruption to, an Entity's operations, services or functions  |
| IoT Device                        | Any device that connects to a network and has the ability to receive and / or transmit data.   |
| IoT Platform                      | Complete set of components of IoT devices, gateways, and infrastructure that supports the operation of the IoT devices.  |
| Internet of Medical Things (IoMT) | The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Medical devices equipped with network connectivity (Wi-Fi, GPRS, cable based connectivity) allow the machine-to-machine communication that is the basis of IoMT. |
| Logging                           | Automated / manual record keeping of system, network or user activity  |
| Multifactor Authentication        | Mechanism of using two or more factors to achieve authentication. I.e factors such as 'What you know', 'What you are' and 'What you have'.   |
| Network                           | Comprises of a number of different computer systems connected by physical and/or wireless connections.   |
| Processing                        | Creating, entering, modifying, updating or deleting information electronically.  |
| PII                               | Personally identifiable information  |
| PHI                               | Protected health information   |
| Physical Access controls          | Controls that monitor and control the physical environment of the entity such as workplace that includes computing facilities.   |
| Patch Management                  | Process of managing systems that involves acquiring, testing, and installing appropriate patches.  |
| Risk Assessment                   | The overall process of Identifying, analyzing, assessing and mitigating entity's risks   |
| Vulnerability / Threat Management | Systematic examination of identifying, classifying, prioritizing, remediating, and remediating security deficiencies.  |



## 4. Requirements

### 4.1 Onboarding a device

- 4.1.1 Entity shall evaluate and ensure that the manufacturer's recommendations and/or the requirements of this standard, whichever is more restrictive, shall be established to create security for the device being deployed.
- 4.1.2 Entity shall conduct a risk assessment with the following criteria prior to onboarding a device:
  - 4.1.2.1 Identification of assets, threats, and vulnerabilities i.e the devices that are going to be on boarded and their impact on existing assets.
  - 4.1.2.2 Assessment of the impact of threats and vulnerabilities on device functionality and patients
  - 4.1.2.3 Assessment of the likelihood of a threat exploiting a vulnerability
  - 4.1.2.4 Determination of risk levels and suitable mitigation strategies
  - 4.1.2.5 Compensating controls & corresponding Risk mitigation strategies
  - 4.1.2.6 Assessment of residual risk and risk acceptance criteria
  - 4.1.2.7 Outcomes of vulnerability assessment and software validation

### 4.2 Security Requirements:

There are a number of security requirements that an entity shall implement when procuring and/or using IoMT devices. The controls listed below forms the essential set of requirements that each entity using IoMT platforms/devices shall comply with:

| Control Reference | Requirements  |
|-------------------|---|
| IOMT-C01          | Establish applicable policies / procedures for access controls, data classification, patch management, vulnerability management etc. to handle IoMT devices securely.   |
| IOMT-C02          | Establish a Risk Management Policy / Procedures and ensure the IoMT risks are periodically evaluated, documented and mitigated.   |
| IOMT-C03          | Identify various responsibilities involved in the lifecycle of IoMT and assign it to appropriate roles ensuring segregation of duties including roles for Information / Cyber Security.   |
| IOMT-C04          | Establish a process to include the devices such as devices not having unique identifier / devices that are not able to enroll in the Entities centralized asset management system, including devices that are not connected to entities' network, and devices that provide little or no information on its hardware, software and firmware. |
| IOMT-C05          | Maintain an up to date inventory of devices with End of Life support. Including the details of End of Vendor / Manufacturer Support.<br>Ensure relevant compensating controls are in place if any device stays in operation past the date on which the manufacturer stops providing security updates / fixes.                               |
| IOMT-C06          | Ensure adherence to the health specific security and privacy standards.   |
| IOMT-C07          | Establish and enforce rules on the acceptable use of IoMT devices and communicated to all employees and contractors in support of care delivery, which  |



|          |   |
|----------|---|
|          | shall be read and acknowledged.   |
| IOMT-C08 | Ensure that any interface used for administration or test purposes, during development, are removed / disabled or made physically inaccessible. Ensure to implement relevant access controls and exception process if there is a need to have an administration port for administration activities.   |
| IOMT-C09 | Select and use devices that incorporates security features to strengthen the protection and integrity of the device. i.e specialized security chips / coprocessors that integrate security into the device, embedded in the processor, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing non-privileged from accessing sensitive codes and security information. |
| IOMT-C10 | Implement a formal user registration and de-registration process for handling IoT devices such as established criteria, unique user accounts for each individual requiring access, revoke user accounts during employee exit and when there are no need.  |
| IOMT-C11 | Restrict and control allocation of privileges with strong password authentication, based on principles of need to know & least privilege. Ensure that normal user accounts are not used as service accounts, privileges are restrictive in nature, privilege or administrative accounts are not used for conducting day to day operational activity etc.  |
| IOMT-C12 | Ensure that the secure boot of the device cannot be bypassed and the device is hardened in accordance with any industry standards / manufacturers' recommendations.   |
| IOMT-C13 | Ensure that the devices with web interface are tested for critical vulnerabilities like XSS, SQLi, CSRF and are compliant with OWASP top 10 Security Vulnerabilities and recommendations, as a baseline, at all time.<br>Ensure that the device interface uses Secure Coding (for example prevention on the use of old Java code, Vulnerable J-Query plugins etc.)  |
| IOMT-C14 | Ensure that security events and incidents can be detected, recorded, retained and handled as needed; such as correction, corrective action, preventive action and lessons learnt etc.   |
| IOMT-C15 | Ensure the off the shelf applications supplied by third party vendors have gone through the security assessment, testing and validation.<br>Ensure to validate and document prior to production implementation.   |
| IOMT-C16 | Implement necessary network controls and ensure devices operate with only minimum needed TCP/UDP ports VLAN controls and prohibit the use of insecure protocols like FTP, Telnet and use only secure protocols such as HTTPS, SFTP.   |
| IOMT-C17 | Ensure to have a defined Vulnerability Management Policy / Procedure to ensure vulnerability assessments & Penetration tests are performed, and identified vulnerabilities are remediated timely (including during major changes in the existing environment / configuration of devices).   |
| IOMT-C18 | Define the policies / procedures to appropriately control if the device supports / permits remote service connections for device analysis / repairs. (including software updates)   |
| IOMT-C19 | Ensure that communication and storage of data related to IoT devices are encrypted, where necessary, and that the encryption algorithm used is industry standard, accepted and adequately strong.   |
| IOMT-C20 | Ensure to perform relevant tests in test environment prior to applying the Patches / Upgrades / Configuration / Firmware in production. Ensure to have a defined Patch Management Policy / Procedure to apply patches / upgrades in a timely  |



|                 |  |
|-----------------|--|
|                 | manner.<br>Ensure that the device is configured in such a way that 'fail safe' mechanism is enabled so that the device will be in a known safe state in the event an update fails.<br>Obtain updates only from the authorized sources. |
| <b>IOMT-C21</b> | Ensure that entities' Asset Disposal Policy / Procedure includes secure disposal of IoMT devices as well, and the relevant records are retained as appropriate, and also includes an end-of-life strategy for the devices.             |

#### 4.3 Additional Requirements:

- 4.3.1 The entity shall include the ways to manage risk of evolving IoMT devices / device types, as the capabilities of these devices vary widely from one device type to another, includes lack of data storage and centralized management capabilities, numerous sensors and actuators, using local and remote data storage and processing capabilities, and being connected to several internal and external networks.
- 4.3.2 The entity shall evaluate and implement additional security requirements based on the results of the risk assessment in the following areas.
  - 4.3.2.1 Security by Design
  - 4.3.2.2 Privacy by Design
  - 4.3.2.3 Suitable technical controls
  - 4.3.2.4 Network controls
  - 4.3.2.5 Authentication / authorization mechanisms
  - 4.3.2.6 Encryption, logging, Web & API security
  - 4.3.2.7 Centralized management control
  - 4.3.2.8 Asset Management / Patch Management / Incident Management / Vulnerability Management / Secure coding principles

#### 4.4 Exceptions:

- 4.4.1 In some cases, the entity may find difficulties in adhering to the requirements of this standard, such cases could be:
  - 4.4.1.1 Devices that cannot fulfil the requirements given in this standard, yet it is important for medical reasons for the entity to use such devices
  - 4.4.1.2 Limitations in demonstrating compliance with the requirements when manufacturer provide devices / services free.
- 4.4.2 In such cases, the exception to compliance with this standard can be established based on the following conditions:
  - 4.4.2.1 Identifying the alternate devices that fulfil the requirements
  - 4.4.2.2 Risk assessment to understand the risks of not adhering to the requirements
  - 4.4.2.3 Risk mitigation plan along with compensating controls and record of controls applied
  - 4.4.2.4 Reporting to relevant authority whenever needed
- 4.4.3 In all cases, appropriate documents shall be maintained and produced to DoH or its associates when requested.





## 5. Enforcement and Compliance

- 5.1 Compliance with this standard is mandatory.
- 5.2 Both internal and external audits/assessments of the entity, on a periodic basis, shall monitor compliance with the requirements of the DOH IoMT Security Standard, together with independent reviews and assessments.
- 5.3 The entity shall retain and furnish outcomes of such audits/assessments to DOH on a need basis.

## 6. Appendix Guidance to IoT

Health care is undergoing a renaissance of technological advancements. Electronic Health Records (EHRs), Electronic Medical Records (EMRs), and connected medical devices are improving doctor / patient communication and outcomes by enabling real-time updates and greater interaction, which in-turn increases the use of Internet and network connected devices, and the frequent electronic exchange of health information.

By considering the increased usage of IoMT devices, which collects, stores, exchanges and process information and the risks / challenges that poses, it has become more vital to guide entities for better understanding and managing the security risks associated throughout the devices' lifecycles.

### 6.1 Architecture of General IoT Communication

The following diagram illustrates the general IoT communication architecture. It is essential that the entity understands their IoT ecosystem that includes, but not limited to, 'understanding of the architecture', 'technology involved', 'method of communication', and 'impact in case of any compromise'.

The understanding of the ecosystem helps to implement the relevant technology / controls wherever necessary to identify threats / vulnerabilities, and to mitigate the risks affecting IoT, proactively.

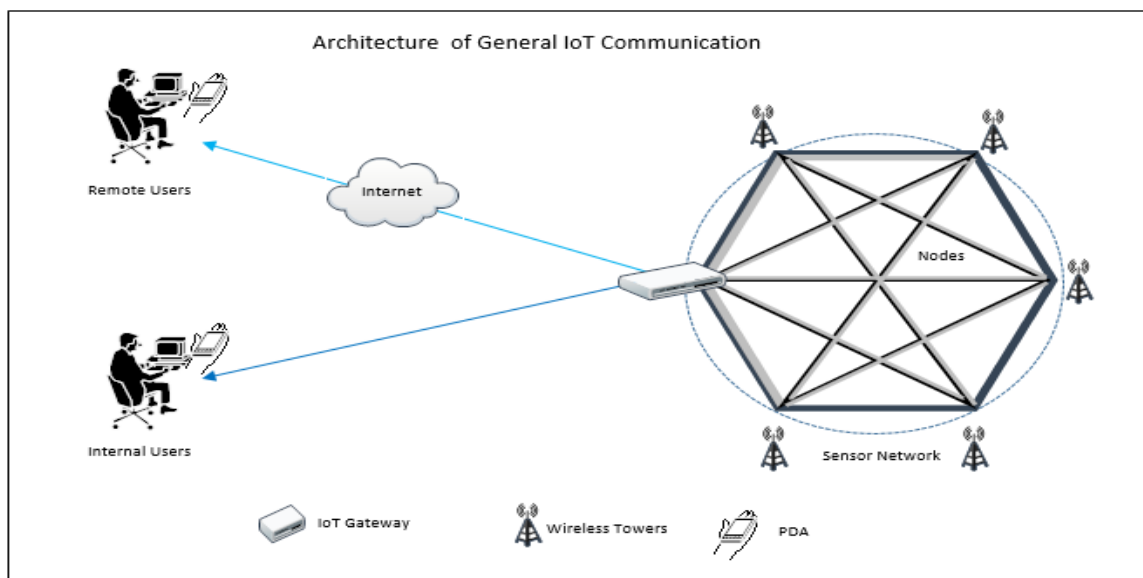


Figure 1 Architecture of General IoT Communication

Reference - [www.sans.org](http://www.sans.org)

### 6.2 Security areas to be considered while procuring a device

The entities should ensure the following basic security requirements at bare minimum while procuring the devices. These basic security requirements will significantly help the entities in procuring a secure IoMT device.

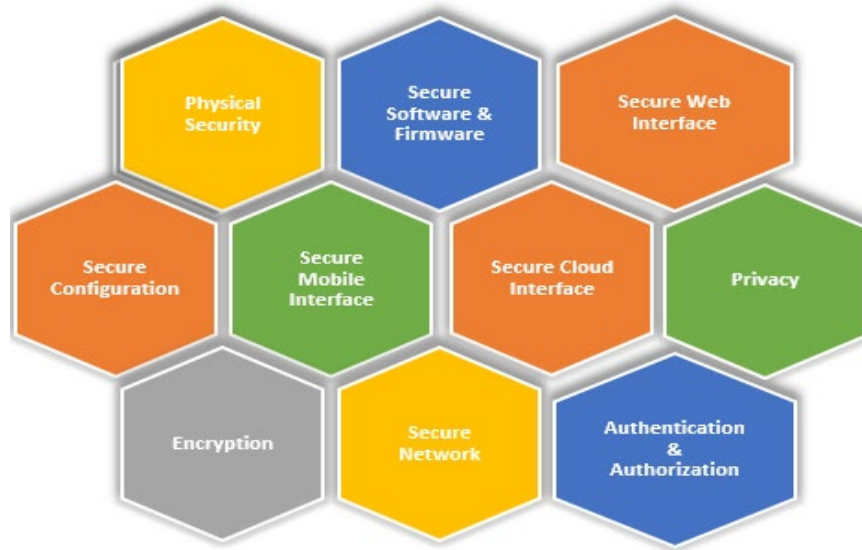


Figure 2 Domains of IoMT security