MDS – G38

Guidance to Pre-Market Cybersecurity of Medical Devices

Version Number: 1.0
Version Date: 18/6/2019

This document has been published after being distributed for public comments dated on 14/5/2019 for 30 days.

Table of Content

Introduction

With the continuous advancement in healthcare care, medical devices are more dependent on computers, network, and software. This reliance makes medical devices more susceptible to cybersecurity threats Therefore, cybersecurity controls have become a demand to assure that medical device is safe and reliable, and health information secured. This guidance developed by the SFDA to aid industry by identifying issues associated with cybersecurity that manufacturers should take into account through the design and development of their medical devices as well in preparing premarket submissions for those devices.

Purpose

The purpose of this guidance is to provide fundamental concepts and recommendations on pre-market submission and suggest best practices on how to secure medical devices connected to a network. These measures shall be taken into account by manufacturers to ensure that no risks are part of the finalized medical device.

Scope

This guidance applies to all medical devices categories that use software as a component of the medical product. Also, it defines terms that are relevant to these types of medical devices and terms used in cybersecurity controls. The focus of this document is the security risks of medical devices on a network, and aim guidance to medical device industry as well as healthcare personnel on how to optimize the performance and security of medical technologies by following best practices. This document provides a comprehensive overview of the cyber-security measures and best practice guidelines on how to mitigate and reduce cyber associated risks.

Cybersecurity Control

Manufacturers should develop and maintain cybersecurity controls to assure continuous functionality and safety of the medical device. These controls propose a procedure where manufacturers should continuously monitor, assess, and mitigate cybersecurity threats throughout the lifecycle of their product from design and developments to the finished medical device. The implementation of cybersecurity measures in the design and development of the medical product can ensure robust and efficient minimization of all associated risks. Manufacturers are advised to develop cybersecurity design inputs for their product, and establish a management system for cybersecurity vulnerability as component of their software validation process that could analyse risk and is mandatory by law.

Manufacturer should address cybersecurity control by:

- Identify threats, vulnerabilities in the system;
- Assess the effect of cyber threats and vulnerabilities on the device performance and safety, as well as, its impact on end users/patients;
- Determine the risk level and best mitigation strategies;
- Assess residual risk and risk acceptance criteria.

Manufacturers are responsible to administer comprehensive technical information that allow healthcare industry to maintain secure risk management system:

Device cybersecurity properties

- Details on the security properties of the device and the technical security controls implemented.
- The expected security environment into which a device may be installed and supplemental security measures that may be required.
- Security best practices and details on how security of the device should be maintained.
- Ongoing information about vulnerabilities discovered or security updates to be implemented.
- Description of any security-relevant third party components used, e.g., IT components or the operating system
- Details on security dependencies between device(s) and supplemental IT components, e.g., workstation, servers, or network components.

Security monitoring and response:

- Capabilities to detect, alert, and respond to security incidents.
- If implemented, fail-safe operational mode.
- If implemented, safe recovery.

Information privacy properties and requirements

- Description pertaining to information privacy of data stored on or transmitted by the device.
- If applicable, ability to pseudonymised or de-identify data.
- Description of technical measures to protect data privacy (e.g., encryption).
- Measures implemented to assure data authenticity and integrity.
- Tools that manage audit of access to healthcare data.
- Any features of the device supporting backup and restoration of patient and/or configuration data.

Authentication and authorization

- Role based, layered authentication.
- Emergency access management.
- Session and time-out management.
- Implemented password rules: strength, lifecycle, no hardcoded or default password, etc.
- Two factor authentication methods, esp. for privileged user access.
- Physical locks of ports and interfaces if needed.
- If implemented, device certificates and device authentication management.
- Secure software update, e.g., code signing.

Lifecycle management

- Special handling requirements during the lifecycle of the device (installation, maintenance, end of life, etc.)
- Specifically, lifecycle management activities required for keeping device security features up-to-date and effective.

Regulatory compliance and documentation

- Regulatory requirements and standards the device complies with (The Joint Commission, European Privacy Directive, IEC,ISO etc.)
- Hazard analysis, list of security risks considered, description of security controls.
- Process for regular and timely communication to device operator on newly discovered security risks.
- Specific security guidance for the operator of the device.

Framework

SFDA suggests that medical device manufacturers consider cybersecurity framework as a guidance in their cybersecurity activities: identify, protect, detect, respond, and recover.

Identify and protect

Medical devices capable of connecting (wirelessly or hard-wired) to another device, to the internet or other network, or to portable media (e.g. USB) are more vulnerable to cybersecurity threats than devices that are not connected. The extent to which security controls are needed will depend on the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the likelihood the vulnerability will be exploited

(either intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity breach.

Manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g. home use vs. health care facility use) to ensure that the security controls are appropriate for the intended users. For example, security controls should not hinder access to a device intended to be used during an emergency.

The SFDA recommends that medical device manufacturers provide justification in the premarket submission for the security functions chosen for their medical devices.

Detect, respond and recover

- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use;
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;
- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised;
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

Cybersecurity documentation

SFDA advices manufactures to submit through MDMA system a premarket submission that covers the components in this section. These suggestions imply on the effective implementation risk management system that covers the cybersecurity threats and quality system in accordance to Regulation.

In the premarket submission, manufacturers should provide the following information related to the cybersecurity of their medical device that complement the ISO 14971 risk management processes. In addition, the manufacture needs to provide evidence of compliance to the following in regards to cybersecurity or provide an alternative method or approach, with appropriate justification.

Secure design

- Identifying cybersecurity risks during the design of the medical device.
- Implement control measures in the device to control identified risks and protect against threats.
    - Where a system can identifies and detect threats and respond to protect against these risks and eventually recover to function as normal medical device.

- List of controls that are in place to assure that the medical device software will remain free from malware from the point of origin to the point at which that device leaves the control of the manufacturer.

Risk management related to cybersecurity and in accordance to ISO 14971

- Conduct a hazard analysis on cybersecurity risks associated to the medical device.
- Maps all identified cybersecurity risks and control measures using traceability matrix.

Verification and validation testing

- List all of standards applied in respect to cybersecurity in the design and development of the device or other evidence of compliance.
- Cybersecurity testing evidence that includes reports of tests and summary of verification and validation of the security of the device
- Conduct Software Weakness Testing.

Planning for continued monitoring

- A plan for software updates necessary in the lifecycle of the medical device to remain safe and effective.
- Maintenance plan in the post-market process where manufacturer ensure continuous functionality and effectiveness of the device throughout its life-cycle.

Annexes

Annex (1): Definitions & Abbreviations

SFDA	Saudi Food and Drug Authority
MDS	Medical Devices Sector
Manufacturer	any natural or legal person with responsibility for design and manufacture of a medical device with the intention of making it available for use, under his name; whether or not such a medical device is designed and/or manufactured by that person himself or on his behalf by another person.
Medical Device	means any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article: A. Intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of: - Diagnosis, prevention, monitoring, treatment or alleviation of disease, - Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, - Investigation, replacement, modification, or support of the anatomy or of a physiological process, - Supporting or sustaining life, - Control of conception, - Disinfection of medical devices, - Providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and B. Which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.
In-Vitro Medical Device	a medical device, whether used alone or in combination, intended by the manufacturer for the in-vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes. This includes reagents, calibrators, control materials, specimen receptacles, software and related instruments or apparatus or other articles.

Accessory	a product intended specifically by its manufacturer to be used together with a medical device to enable that medical device to achieve its intended purpose.
MDMA	Medical Devices Marketing Authorization
Cybersecurity	A method to prevent the unauthorized access, use, modification of information that is stored, accessed, or transferred from a medical device to an external storage.
Data Integrity	Ownership of data, information and software to be correct and complete without improper modification.
Malware	software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected system
Risk	The combination of the probability of occurrence of harm and the severity of that harm.
Encryption	The cryptographic transformation of data into a form that conceals the data's 179 original meaning to prevent it from being known or used
Asset	A product that has value to an individual or an organization
Configuration	The possible conditions, parameters, and specifications with which a device or system component can be described or arranged.
Vulnerability	The state of being exposed to the possibility of being attacked or harmed.
Authorization	the right or a permission that is granted to access a device resource.
Hazard	All of the possible rick or danger from the use of medical device
Threat	The potential impact over the safety of medical device via unauthorized access, misuse, or modification of medical device data.
Software	a software system that has been developed for the purpose of being incorporated into the medical device being developed or that is intended for use as a medical device in its own right.