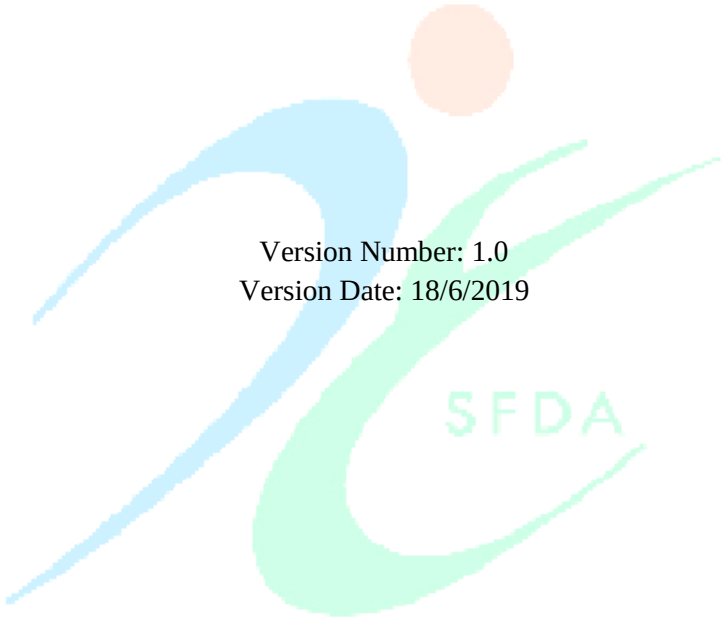
MDS – G37

# Guidance to Post-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 contents

## Introduction

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.

All medical devices carry a certain amount of risk. While the increased use of wireless technology and software in medical devices also increases the risks of potential cybersecurity threats, these same features also improve health care and increase the ability of health care providers to treat patients.

Addressing cybersecurity threats, and thus reducing information security risks, is especially challenging. Because cybersecurity threats can not be eliminated, manufacturers, hospitals and facilities shall work to manage them. There is a need to balance protecting patient safety and promoting the development of innovative technologies and improved device performance.

## Purpose

The purpose of this guidance is to provide fundamental concepts and recommendations on medical devices post-market requirements for cybersecurity protections against malwares and other threads. These measures shall be taken into account by manufacturers.

## Scope

This guidance applies to any marketed, distributed medical devices within the KSA including the following categories: medical devices that contain software (including firmware), software that is a medical device, including mobile medical applications.

## Medical devices post-market requirements to eliminate the potential risk of cyber-attacks.

Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. Manufacturers should respond in a timely fashion to address identified vulnerabilities. Critical components of such a program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Maintaining robust software lifecycle processes that include mechanisms for: monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle;
- Design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice;
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

Post-market cybersecurity information may originate from an array of sources including independent security researchers, in-house testing, suppliers of software or hardware technology, health care facilities, and information sharing and analysis organizations.

## Cybersecurity framework

| Function | Category | Subcategory | Informative Reference |
|---|---|---|---|
| **Identify** | | | |
| **Protect** | | | |
| **Detect** | | | |
| **Response** | | | |
| **Recover** | | | |

## Risk management of medical devices cybersecurity

To manage post-market cybersecurity risks for medical devices, a company should have a structured and systematic approach to risk management and quality management. A manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. This process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information. Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk. It is not possible to describe all hazards, associated risks, and/or controls associated with medical device cybersecurity vulnerabilities in this guidance. It is also not possible to describe all scenarios where risk is controlled or uncontrolled.

## References


1. National Institute for Standards and Technology, https://www.nist.gov
2. Food and Drug Administration, www.fda.gov
3. Daniel B. Kramer, "*Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance*".(2012)
4. Fu, Kevin. "Controlling for cybersecurity risks of medical device software." (2013).

# Annexes

# Annex (1): Definitions & Abbreviations

| | |
|---|---|
| KSA | Kingdom of Saudi Arabia |
| Medical devices | means any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article:<br>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:<br>- Diagnosis, prevention, monitoring, treatment or alleviation of disease,<br>- Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,<br>- Investigation, replacement, modification, or support of the anatomy or of a physiological process,<br>- Supporting or sustaining life,<br>- Control of conception,<br>- Disinfection of medical devices,<br>- Providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body;<br>and<br>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. |
| Compensating control | A safeguard or countermeasure deployed in the absence of controls designed in by device manufacturer. These controls are external to the device design, configurable in the field, employed by a user and provide a supplementary or comparable cyber protection for a medical device. |
| Controlled risk | It is presenting when there is acceptable residual risk of patient harm due to a device's particular cybersecurity vulnerability. |
| Uncontrolled risk | Unacceptable residual risk of patient harm due to inadequate risk mitigations. |

| | |
|---|---|
| Threat | Threat is any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or essential performance of the device. |
| Threat modeling | Threat modeling is a methodology for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent mitigate the effects of, threats to the system. |
| Vulnerability | A vulnerability is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat. |
| Cybersecurity routine updates and patches | Are changed to a device to increase the device security and remediate only these vulnerabilities associated with controlled risk of patient harm. These changes are not intending to reduce the uncontrolled risk of patient harm, and therefore not to reduce a risk to health. They include any software upgrade, firmware, hardware, programmable logic or security of the device.<br>Cybersecurity routine updates and patches are generally considered to be a type of device enhancement that may applied to vulnerabilities associated with controlled risk. |
| Cybersecurity signal | Any information which indicates the potential of hacking or confirmation of a cybersecurity vulnerability that affects, or could affect directly or indirectly the medical device. |
| Exploit | An instance where a vulnerability can be exercised.<br>Patient Harm<br>Remediation<br>Threat<br>Threat Modelling<br>Uncontrolled risk<br>Vulnerability |