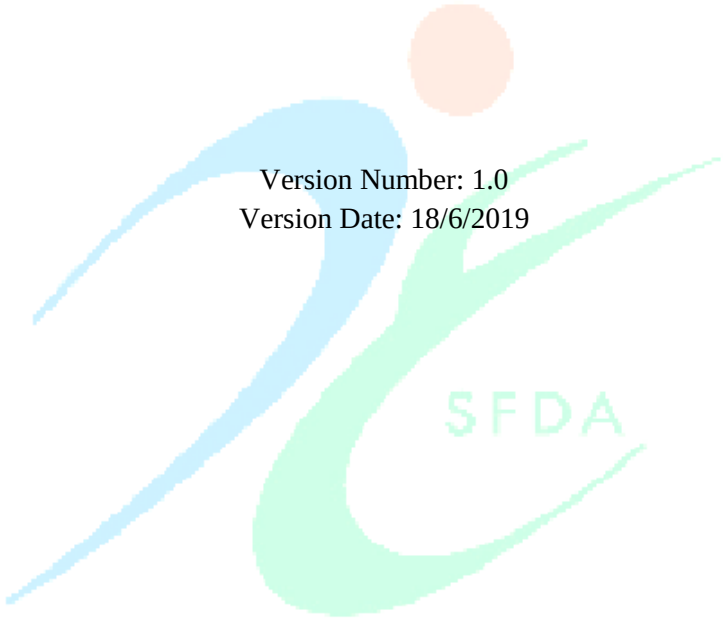
MDS – G36

Guidance to Medical Devices Cybersecurity for Healthcare Providers



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.

Purpose

The purpose of this guidance is to give recommendations to healthcare providers on cybersecurity of medical devices .The SFDA is recommending that health care facilities shall take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Scope

This guidance document applies on healthcare providers that have any medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

Background

The SFDA has issued this guidance in accordance to Article Thirty Seven of The Medical Devices Interim Regulation Issued by the Saudi Food and Drug Authority Board of Directors decree number (1-8-1429) and dated 27 December 2008 which states “The SFDA shall monitor the use of medical devices in the KSA and take the appropriate measures to ensure their proper installation and maintenance in respect of the safety of patients, users and other persons”.

Incidents or malware at hospitals

Incidents or malware at hospitals may come in different ways. Hospitals shall have the ability to recognize and consider the following:

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals.

SFDA recommendations to healthcare providers

- Restricting unauthorized access to the network and networked medical devices.
- Making certain appropriate antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
- Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device.
- Developing and evaluating strategies to maintain critical functionality during adverse conditions.
- Reporting any incident or event to SFDA via the following reporting channels:

- **National Center for Medical Devices Reporting**
  https://ncmdr.sfda.gov.sa/Default.aspx
  Saudi Vigilance System
  https://ade.sfda.gov.sa/
- **Call SFDA unified number: 19999**

References

1. Food and Drug Administration, www.fda.gov
2. Daniel B. Kramer, "*Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance*".(2012)
3. ICS-CERT Web Site, http://ics-cert.us-cert.gov/

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: 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.

Healthcare provider	any party, governmental or private, provides healthcare services with KSA including health clinics.
Incidents	Events involving* medical devices that have resulted in, or could have resulted in (i.e. near misses), harm to a patient, health professional or other person. Other issues involving* medical devices that have not led to harm, but affect quality, timeliness and cost-effectiveness of health care delivery and may, if it happens often enough, lead to harm. * "Involving" in this means associated with the use, or misuse, of a medical device – either caused or partially attributable to a device
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.
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.