GLOBAL DIGITAL HEALTH
PARTNERSHIP

Medical Device Manufacturer Internet of Things (IoT) Code of Conduct

DRAFT

Draft Date: January 2020
Version: 1.x
Authored By: GDHP Cybersecurity Workstream

Contents

INTRODUCTION

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT can provide computing functionality and network connectivity for equipment that previously lacked this utility. The full scope of IoT is vast and many organizations are not necessarily aware they are using a large number of IoT devices. These interconnected and internet connected devices can affect their cybersecurity and privacy risks in different ways than traditional information technology (IT) devices.

Securing IoT devices is a major challenge, as manufactures tend to focus on functionality, compatibility requirements, customer convenience, and time-to-market rather than security. Meanwhile, security threats are increasing. For example, Symantec reported a 600% increase (YoY: 2016 to 2017) in attacks against IoT devices[1].

Internet of Things (IoT) Concepts

The Internet of Things consists of the following elements:

- The components (i.e. devices, applications, phones, appliances etc.)
- Components connected / interconnected by a digital network and
- Components communicate with sensors that allow the components to observe, send and receive information about themselves or their environment.

IoT In Healthcare

The Internet of Medical Things (also called the internet of health things) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. In the healthcare sector, health IoT gathers, transmits and analyzes data derived from electronic health records (EHR) containing personally identifiable information (PII), protected health information (PHI), patient generated health data, and other machine-generated healthcare data. Health IoT supports services like such as real-time monitoring, medication compliance, and imaging.

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf

tools within a healthcare delivery organization (HDO) – ultimately contributing to the Internet of Medical Things (IoMT).

Health IoT Security Objectives

The security objectives of health information technology (HIT) includes implementation of security controls that provide for the confidentiality, integrity, and availability of patient information and for the systems supporting the use and exchange of that information.

The security objectives of ***medical devices*** are concentrated around ***patient safety*** and focus more on Integrity and Availability. Cybersecurity Risks are different from patient safety risks but they can affect patient safety. The threats and vulnerabilities for cybersecurity risks can be much broader in scope than typical safety hazard, harm, or device failure.

> *"The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network- connected devices, portable media (e.g. USB or CD), and the frequent electronic exchange of medical device-related health information"….*
>
> *"Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the US and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm."* (United States Food and Drug Administration, 2018)

The Role of Medical Device Manufacturers in the Security Management Process

Manufacturers can affect and improve the protection of systems, data and patient safety by incorporating technical safeguards (i.e., security features) in their devices during design phase of their product. This approach can provide a pre-distribution device designed with the goal of (1) reducing cybersecurity intrusion and misuse; (2) improving availability, reliability, and accuracy; and (3) adhering to generally accepted security procedures.

CODE OF CONDUCT

Purpose

The purpose of this code of conduct is to establish a central guide and reference for device manufacturers that enumerates various cybersecurity best practices and recommendations that will provide a baseline for achieving the desired state of cybersecurity posture for medical devices. This code provides guidance that is holistic in nature, with cybersecurity practices that device manufacturers can implement both pre- and post-deployment of their medical devices.

The Code of Conduct can also be used to identify opportunities for improving cybersecurity posture by comparing the best practices provided with the currently implemented security controls.

Objectives

The objective of this document is to provide baseline guidance that can assist manufacturers in considering cybersecurity controls during development of medical devices.

Confidentiality	Health IoT requires the protection of patient information from unauthorized disclosure and access.
Integrity	Health IoT requires the protection of patient safety from unauthorized modification of the intended use of the medical device.
Availability	Health IoT requires that patient information is available to authorized entities when it is needed and that the medical device's functionality continues to be available when needed.

GENERAL CYBERSECURITY CONSIDERATIONS

Device manufacturers should consider security objectives as a basis for building and enhancing their corporate cybersecurity program, including the following:

- Protecting patient data from malicious code.
- Protecting patient sensor data from tampering.
- Protecting medical device processing capability.
- Protecting patient data from unauthorized disclosure or modification.
- Ensuring availability of patient information to authorized users and entities.
- Establishing a rapid and secure patch distribution methodology for deployed medical devices.

- Applying continuous security risk management throughout the device lifecycle.
- Exploring and promoting, where appropriate, existing and emerging technologies to enhance security and confidentiality of health information.
- Educating consumers on security and privacy issues related to the use of devices.
- Identifying, appointing and publishing individuals who are responsible and accountable for administering device system components.
- Establishing and maintaining procedures for validating the devices design that includes software validation and risk analysis.

BEST PRACTICES AND RECOMMENDATIONS

The best practices and recommendations listed below address additional security concerns that are worthy of consideration. These additional recommendations can help to reduce risk factors or prevent them from becoming greater risks.

1. **Develop or Mature Cybersecurity Policies and Documentation**

   1.a Establish a cybersecurity function within the development team that is responsible for ensuring the incorporation of appropriate security controls during the design and development process.

   1.b Develop or update policies and procedures to ensure a holistic risk management approach that includes:
   - Security testing during the development and design phases; and
   - Continuous security monitoring during deployment, sanitization, and reuse of medical devices.

   1.c Enroll in and receive cybersecurity vulnerability advisories for medical devices from governing bodied or information sharing organizations.

   1.d Manufactures have a responsibility to ensure security safeguards are included as a part of medical device implementation plans. Establish a process to communicate and share documentation with health care providers that will help them understand the privacy and security features of the medical devices they purchase. Topics may cover:
   - ePHI encryption
   - Auditing functions
   - Backup and recovery routines
     - How backup and recovery system works
     - Where backups are stored
     - Recommended frequency of testing recovery system
   - Unique user IDs and strong passwords

- Role- or user-based access controls
- Auto time-out
- Emergency access
- Amendments and accounting of disclosures
- Available training on security features configuration
- Trusted communication protocols
- Remote access to provide support and other services. Security of remote access.

1.e Document an inventory of device components that reflects the current system.

- System components may include programmable logic controllers, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.
- Documentation may include information deemed necessary for effective accountability of device components, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses.
- Inventory specifications may include manufacturer name, device type, model, serial number, and physical location.
- Device software inventory should be reviewed and updated on a regular reoccurring schedule. Device software components may include software license information, software version numbers, user interface software and operating systems.

1.f Provide health care providers with a vulnerability disclosure policy/procedure and vulnerability reporting updates.

1.g Document device security posture, new vulnerabilities, security recommendations and compensating controls.

2. Implement Cybersecurity and Risk Management Practices and Procedures

2.a Incorporate a formal security risk management process during all medical device lifecycle phases, addressing cybersecurity from medical device conception to disposal.

2.b Address medical device security risks during the design and development phase through a risk management process that includes privacy objectives as well as the objectives of secure design: Confidentiality, integrity (including authenticity and non-repudiation), and availability.

2.c Collaborate with healthcare providers to ensure that risk control measures intended to increase security do not degrade the intended use of the device, including requirements related to emergency access.

2.d Implement procedures to test (i.e. vulnerability scanning, penetration testing, ethical hacking methods), identify and continuously monitor the security controls of devices. If new vulnerabilities are identified, assess if additional security controls can be implemented without compromising the safety and effectiveness of the device.

2.e Establish mechanisms to receive relevant cybersecurity-related information from applicable suppliers.

2.f Collaborate with health care providers during security incidents in order to, as appropriate, uncover facts, appropriately inform health care delivery organizations or other stakeholders, and to employ additional security control measures when appropriate.

2.g Establish and support a coordinated disclosure process that provides a pathway for researchers and others to submit potential vulnerabilities, to the organization.

2.h Continuously manage device cybersecurity throughout its lifecycle. Including timely sharing of known threat and vulnerability information, which enables organizations to efficiently respond to new threats.

2.i Implement a cybersecurity vulnerability and patch management approach as part of the software validation and risk analysis.

2.j Establish and implement a patch deployment approval process.

REFERENCES

- ***FDA DRAFT*** Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, September 6, 2018, *When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014*
- FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, October 2, 2014 (https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf)
- FDA Guidance for Industry, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, January 14, 2005. (https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf)
- ONC Guide to Privacy and Security of Electronic Health Information, April 2015 (https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf)
- OCR November 2016 Cybersecurity Newsletter "Understanding DoS and DDoS Attacks and Best Practices for Prevention" (https://www.hhs.gov/sites/default/files/december-2016-cyber-newsletter.pdf)
- ***NIST Draft*** NISTIR 820 – Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) (https://csrc.nist.gov/publications/detail/nistir/8200/draft)
- ***NIST Draft*** SP 1800-8 – Securing Wireless Infusion Pumps in Healthcare Delivery Organizations (https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf)
- NISTIR 8183 – Cybersecurity Framework Manufacturing Profile, September 2017 (https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf)
- NIST Special Publication 800-160, Vol 1, Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016 (https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=922194)
- National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, version 1.0, February 12, 2014, (https://www.nist.gov/document-3766.)
- NIST Special Publication 800-64 Revision 2, Security Considerations in the System Development Life Cycle, October 2008 (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-64r2.pdf)

- 2018 Internet Security Threat Report, Symantec Corporation, March 2018. (https://www.symantec.com/security-center/threat-report)
- D. Fred, *A Brief History of the Internet of Things*, FireceMobileIT, July 2014. (http://www.fiercemobileit.com/story/brief-history-internet-things/2014-07-2)
- HIMSS/NEMA Standard HN 1-2013 – Manufacturer Disclosure Statement for Medical Device Security