The Internet of Medical Things—Anticipating the Risk

The Internet of Medical Things (IoMT) is and has been a driving force of the networked medical device landscape ecosystem. The number of medical devices in this space is growing at an astonishing rate and with this comes growing risk for the industry. Medical data breaches started well before the use of electronic devices and systems, but, naturally, with the increased use of electronic personal health information (ePHI), there is a growing trend of data breaches in the medical space. Between 2009 and 2018, there have been 2,546 healthcare data breaches in which more than 500 records were compromised.[1] Practitioners need to realize that the growing trend of connected devices creates many benefits, but also brings enhanced risk to the medical device ecosystem.

The value proposition of connected medical devices is clear—the benefits are for patients (consumers), healthcare institutions and providers. IoMT is clearly increasing the attack vectors and the risk of cyberbreaches for the industry. This will continue to increase over time as the demand for and abundance of connected medical devices increases. The connected health device market is expected to reach an estimated US$36.1 billion worldwide by 2023 and is forecasted to grow at a rate of 21.1 percent from 2018 to 2023.[2]

The connected medical device space can be segmented into two areas: wearable (e.g., home health management, patient monitoring by healthcare practitioners, activity trackers) and nonwearable, which are hospital- and clinic-based connected devices. These connected medical devices represent a large population of IoMT, and they are prone to vulnerabilities. Properly securing these medical devices helps strengthen the position large IoMT ecosystems play in the healthcare environment. The industry is increasingly focusing on securing devices, and regulatory bodies are expecting security by design in medical device products that are connected.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2MdVrDw

Mohammed Khan
Is global head of digital health, IT, cyber and privacy audit at Baxter, a global medical device and healthcare organization. He manages a global team responsible for enterprise risk management across the organization and conducting audits, assessments and advisory engagements. He has spearheaded multinational global audits and assessments in several areas, including enterprise resource planning systems, global data centers, cloud platforms (i.e., Amazon Web Services), third-party manufacturing and outsourcing reviews, process re-engineering and improvement, global privacy assessments (EU Data Protection Directive, the US Health Information Portability, and Accountability Act [HIPAA], the EU General Data Protection Regulation [GDPR]), and FDA guidance specific to medical device cybersecurity over the past several years. Khan previously worked as an advisory consultant for leading consulting firms and multinational organizations. He frequently speaks at national and international conferences on topics related to data privacy, cybersecurity and risk advisory. He volunteers as an *ISACA® Journal* article reviewer and contributes actively to the *ISACA Journal* and ISACA's blogs. In 2019, Khan received the ISACA® John W. Lainhart IV Common Body of Knowledge Award.

Enjoying this article?

- Read *Networked Biomedical Device Security. www.isaca.org/networked-biomedical-device-security*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Regulatory Guidance and Frameworks

Regulatory guidance and requirements are fundamentally uniform when it pertains to patient data security and privacy regulations. The following regulations are related to patient data security and privacy regulations and standards:

- **EU General Data Protection Regulation (GDPR)**—Products and systems that collect EU patient data must be considered from a privacy perspective. GDPR went into effect on 25 May 2018.
- **US Health Insurance Portability and Accountability Act (HIPAA)**—This US legislation provides data privacy and security provisions for safeguarding medical information.
- **US Health Information Technology for Economic and Clinical Health (HITECH) Act**—This US act was signed into law on 17 February 2009 to promote the adoption and meaningful use of health information technology.
- **US National Institute of Standards and Technology (NIST) Special Publication (SP) 800.53**—This is a catalog of security controls for all US federal information systems. It organizes basic cybersecurity activities at their highest level, known as functions.

There is no global regulation that requires medical device security as of this writing. What exists, however, are guiding principles and shifts in landscape in terms of where regulations are going. This can be seen by looking at the history of regulation of medical devices. Starting in 1976 in the United States, for example, medical device manufacturers were required to ensure the establishment of risk-based device classifications, controls around general and special processes, premarket notification, and approval. This resulted in the US Safe Medical Device Act (SMDA), federal legislation that was designed so that the US Food and Drug Administration (FDA) could quickly be informed of any medical product that had caused or was suspected to have caused a serious illness, injury or death.[3]

Subsequently, in 2014, the FDA—for the first time in its history and as the first regulatory body in the world—identified and addressed the cybersecurity risk of medical devices.[4] Its guidance specifically highlighted recommendations to consider medical device premarket submissions for effective management of cybersecurity. This was the first enhancement for safeguarding patients from a medical device cybersecurity perspective after the SMDA was issued. The most recent guidance was the premarket for cybersecurity guidance and post-market management of cybersecurity guidance from the FDA (**figure 1**). Additionally, the FDA prefers that medical device manufacturers share cyberintelligence through Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).

Classes of Medical Devices and Risk

It is important to understand the basic parameters of what makes a device a medical device. Due to the authority of the FDA, not only in regulating medical devices sold in the United States, but also as an organization at the forefront of medical device security as a forerunner of globally respected government institutions, the focus here is on an FDA-centric definition of medical device classes. The regulatory classes of medical devices are divided up by a classification mechanism called Class I, Class II and Class III. Since the classification of medical devices is based on risk, it is important to understand the risk level and, more important, what the device is medically going to be used for and its intended purpose. The classes, their risk range and example device classification are shown in **figure 2**.

IoMT

Many people wake up in the morning to an alarm set up on a watch that provides a report to a phone on how the user's sleep was the night before. Later, those users can assess how fast and long they ran on the treadmill, all while monitoring their heart rate and cadence, which then gets reported to a daily fitness monitoring chart.

A diabetic patient may have a wearable medical device that continuously checks the user's glucose level, all while maintaining proper levels in the body and alerting a healthcare practitioner not only of anomalies, but general vitals of the patient for active monitoring. An artificial pancreas device

Figure 1—US Regulatory Guidance for Medical Device Cybersecurity

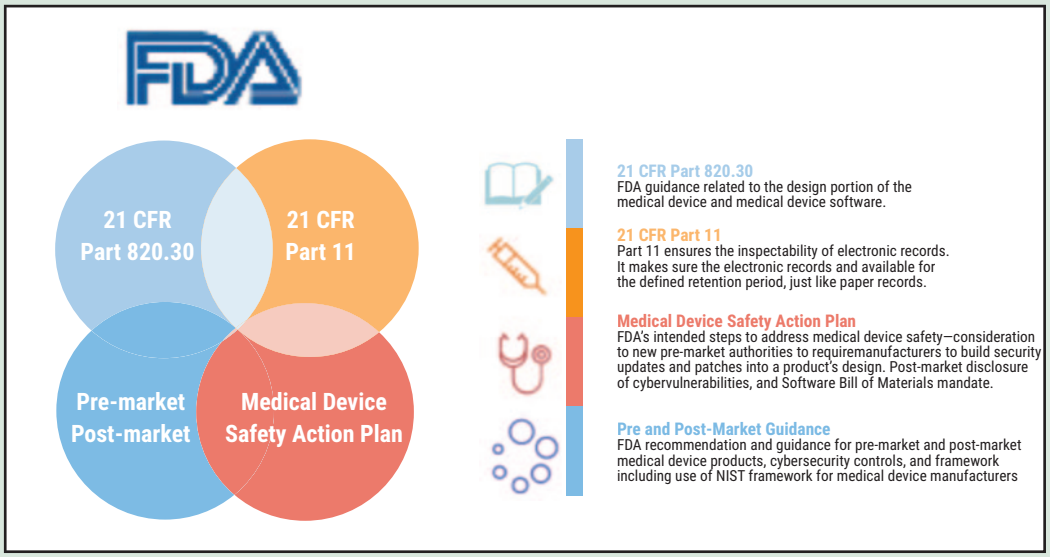
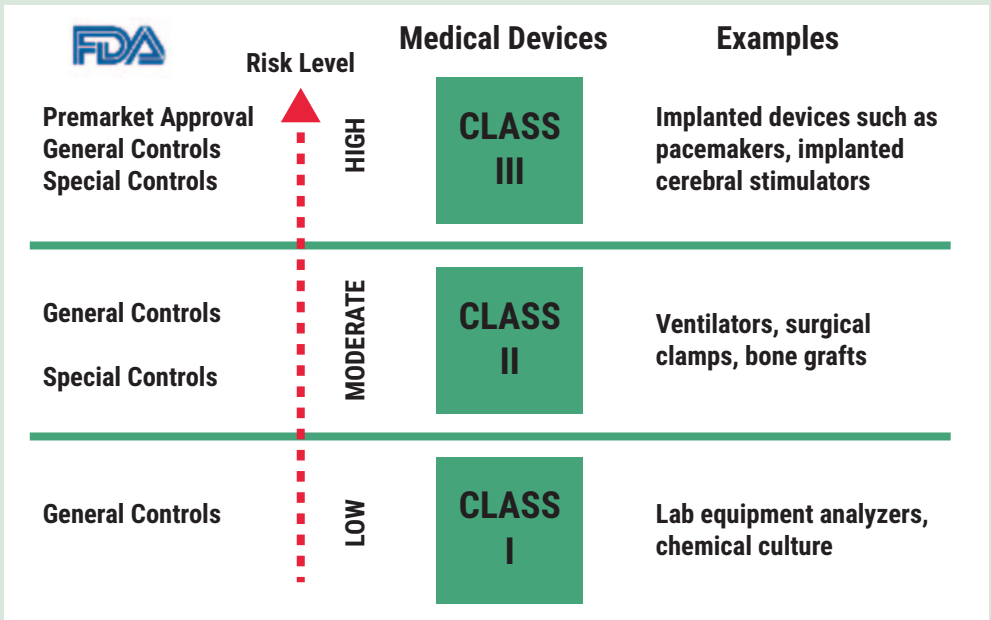


Figure 2—Medical Device Classes and Risk



system will not only monitor glucose levels in the body, but also automatically adjust the delivery of insulin to reduce high blood glucose levels (hyperglycemia) and minimize the incidence of low blood glucose (hypoglycemia) with little or no input from the patient.[5]

If the patient goes to the hospital and checks into the emergency room (ER), data from the wearable device can be extracted and loaded into the electronic medical records (EMR) system, which is connected to the hospital network, which is further connected with physicians' tablet software so that, when the patient is seen, all data are available for the health practitioner.

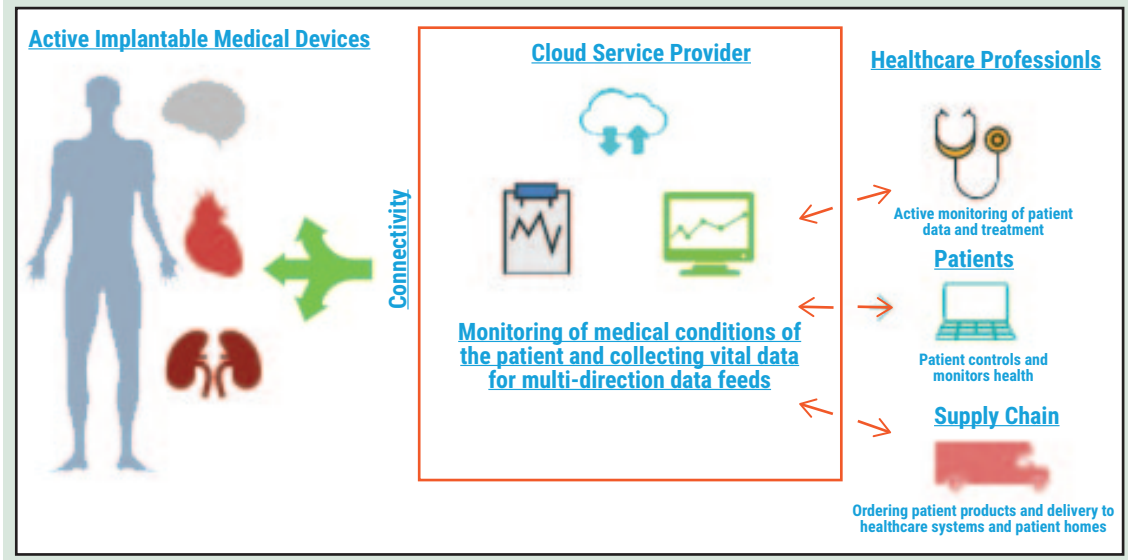
These are just some examples of how connected the world of medical devices has become. **Figure 3** shows an example. There are many device types that make up the IoMT space, and they can be divided into the following categories:

- **Implantable devices (wireless)**—There are several types of implantable medical devices that are considered Class III, and many of them can be wireless. These include deep brain neurotransmitters, cochlear implants, cardiac defibrillators/pacemakers and insulin pumps, just to name a few. These are normally multiyear implants, where the physician administers and manages the device through routine outpatient service checks.
- **Stationary medical devices**—These devices are generally used for outpatient and inpatient services, whether it is an ER visit or a routine operation. These devices are in the hospital-connected ecosystem and include infusion pumps, chemotherapy dispensaries and homecare cardiovascular systems. These are normally Wi-Fi-enabled and connect either to the patient's home network or the hospital networks.
- **Wearable medical devices**—The intent of these devices is for monitoring purposes and collecting data for further analysis by healthcare providers. These include wireless-enabled proprietary insulin pumps and electromechanical devices for pain medication.
- **Health monitoring devices**—These are normally not regulated; however, they pose a great deal of risk because the devices collect vitals (e.g., blood pressure, body temperature, heart rate, respiratory rate) and information about the consumer and/or patient. Bluetooth or Wi-Fi is enabled under the direction of the owner of the device, and these devices monitor physical activity and engage in significant communication with the paired mobile devices.

Device Manufacturers—A Snapshot of Guidance

Patient safety is the priority of all medical device manufacturers, or at least it should be, as they think about the medical device throughout its life cycle. Although the FDA has issued guidance and there are quite a few frameworks that help manufacturers navigate complying with regulator, hospital and patient needs and requirements, there is still room for interpretation by device manufacturers. There will always be risk and obligations to address when there is a medical device that is connected to the Internet of Things (IoT). Controls, including mitigation controls manufacturers need to have in place to avoid or eliminate patient risk, are critical. Risk factors can include improper access to the device or use of device data to exploit patient information or, worse, impact patient health or life due to device tampering or performance gaps caused by a cyberhack. Due to the connected

Figure 3—Implantable Medical Devices and Improving Patient Experience



device's ecosystem, especially in a hospital network, there is a likelihood the exploitability of the device or the hospital network is quite high due to the industry not being fully mature in the cybersecurity space.[6] Medical devices such as pacemakers, insulin pumps and magnetic resonance imaging (MRI) machines are increasingly vulnerable to hacking. At the moment, however, there is no US federal mandate for those devices to have cybersecurity protections.[7] Despite the lack of mandates, there are some key areas for medical device manufacturers to consider:

- **Weak access controls**—Limit access to the medical device that is connected, specifically focusing on ensuring devices have two-factor authentication built in for proper authentication techniques.
- **Periodic updates**—Apply security patches to the medical device on a frequent basis as best practice, per post-market guidance issued by the FDA. Although the FDA does not require approvals for patching medical device software for cyber-related fixes, it is important to ensure that the proper software development life cycle is put in place for the device well before the product is released in the market.
- **Coding standards**—Many successful cyberattacks have exploited vulnerabilities in code not rigorously tested prior to deployment in a live environment.[8] One of the important standards in the industry is issued by the International Electrotechnical Commission (IEC), IEC 62304. This standard provides a robust feature of how best to develop code from development to post-production release code life cycle management. In the European Union, it satisfies key requirements in the Medical Devices Directive (soon to be replaced by the EU Medical Device Regulation). And, in the United States, the FDA accepts IEC 62304 compliance as proof that regulatory processes, such as Section 510(k) of the FDA, which requires device manufacturers to notify the FDA of their intent to market a medical device at least 90 days in advance, have been fulfilled.[9]
- **Security by design**—Proper life cycle management of all aspects of the medical device, i.e., hardware and software bill of materials (BOM), to ensure proper inventory of all third-party and in-house hardware and software is crucial. This can also be enhanced further with the use of properly encrypted channels of communication from the device with the outside world.

> "MEDICAL DEVICES SUCH AS PACEMAKERS, INSULIN PUMPS AND MAGNETIC RESONANCE IMAGING (MRI) MACHINES ARE INCREASINGLY VULNERABLE TO HACKING."

Coming Full Circle With IoMT

The world of connected medical devices is here to stay, and there is no turning back. Medical technology ecosystems around the world are increasing exponentially and will become the norm. The IoT healthcare market will reach US$136.8 billion worldwide by 2021.[10] Today, there are 3.7 million medical devices in use that are connected to and monitor various parts of the body to inform healthcare decisions.[11] Medical device manufacturers must ensure proper cybersecurity controls are considered as they become more vested in the safety of the patients and the ecosystems to which the medical devices connect. There continues to be a great deal of opportunity in the space of connected devices and, over time, as patients' health is improved with the advancement of technology, the industry and the vast number of regulators monitoring this arena need to keep up with the pace of advancement all while keeping cybersecurity in mind.

Author's Note

All views expressed in this article are those of the author and do not necessarily represent the views of his employer.

Endnotes

1 *HIPAA Journal*, "Healthcare Data Breach Statistics," *https://www.hipaajournal.com/healthcare-data-breach-statistics/*

2 24x7, "Global Connected Health Device Market to Reach $36 Billion by 2023," 16 July 2018, *www.24x7mag.com/2018/07/global-connected-health-device-market-reach-36-billion-2023/*

3 US Congress, "H.R.3095—Safe Medical Devices Act of 1990," USA, 1990, *http://thomas.loc.gov/cgi-bin/bdquery/z?d101:HR03095:@@@L&summ2=m&*

4 US Food and Drug Administration, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," 2 October 2014, *https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf*

5 US Food and Drug Administration, "What Is the Pancreas? What Is an Artificial Pancreas Device System?" *https://www.fda.gov/medicaldevices/productsandmedicalprocedures/homehealthandconsumer/consumerproducts/artificialpancreas/ucm259548.htm*

6 Zettter, K.; "Hospital Networks Are Leaking Data, Leaving Critial Devices Vulnerable," *Wired*, 25 June 2014, *https://www.wired.com/2014/06/hospital-networks-leaking-data/amp*

7 Marks, J.; "The Cybersecurity 202: Medical Devices Are Woefully Insecure. These Hospitals and Manufacturers Want to Fix That," *The Washington Post*, 29 January 2019, *https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/29/the-cybersecurity-202-medical-devices-are-woefully-insecure-these-hospitals-and-manufacturers-want-to-fix-that/5c4f4a661b326b29c3778cef/?noredirect=on&utm_term=.0a699b008196*

8 Williams, P.; A. Woodward; "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem," *Med Devices*, 2015, p. 305-316, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/*

9 Bellairs, R.; "What Is IEC 62304? Compliance Tips for Medical Device Software Developers," Perforce, 7 February 2019, *https://www.perforce.com/blog/qac/what-iec-62304-compliance-tips-medical-device-software-developers#ssc*

10 MarketWatch, "Internet of Things (IoT) Healthcare Market Is Expected to Reach $136.8 Billion Worldwide, by 2021," 12 April 2016, *https://www.marketwatch.com/press-release/internet-of-things-iot-healthcare-market-is-expected-to-reach-1368-billion-worldwide-by-2021-2016-04-12-8203318*

11 Marr, B.; "Why the Internet of Medical Things (IoMT) Will Start to Transform Healthcare in 2018," *Forbes*, 25 January 2018, *https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#4b9e610f4a3c*

50 ISACA

CSX CYBERSECURITY NEXUS
AN ISACA CYBER SOLUTION

INTRODUCING CYBERSECURITY CAREER PATHWAYS

In a recent survey, 58% of cybersecurity professionals indicated that they had unfilled cybersecurity positions in their organization. Nearly one-third of them said that it takes six months or more to fill those roles, often because applicants lack the qualifying skills.

With this in mind, ISACA has created three specific career-path training programs in their state-of-the-art Cybersecurity Nexus® (CSX) online cyber academy. Take the training you need today, to qualify for the job you want tomorrow.

Learn more at www.isaca.org/pathways-jv4