compliance & risks

Cybersecurity and Connected Medical Devices

Prepared by: Jerry Miller, Senior Regulatory Consultant, Compliance & Risks

August 2021

compliance & risks

1. Introduction

Medical devices are becoming more and more connected to the internet, hospital networks, and other medical devices. This connectivity provides additional and convenient features that help improve healthcare and increase the ability of doctors, nurses and therapists to treat patients. However, this same connectivity also adds to the risk of outside hacking and cybersecurity issues. One recent study found that connected devices outnumber people in healthcare settings by as many as 3 to 1, but many of those devices lack sufficient security to prevent attacks. Another poll found that 1 in 4 healthcare employees have never received cybersecurity training from their employer.

As medical devices become more advanced and the Software as a Medical Device (SaMD) industry increases, it is crucial to make sure medical devices are sufficiently protected from hacking attacks and personnel and policies are in place to provide education on the issue. The two main issues facing the healthcare industry are the security of their data systems and the security of the devices themselves.

Medical devices, such as pacemakers, light scopes, infusion pumps, and medical computer systems, can be vulnerable to security incursions, potentially impacting the safety and effectiveness of the device. Medical devices that either contain software, including firmware and programmable logic controllers can be at risk from either organized cyber criminals or everyday hackers.

This white paper provides an overview of how cybersecurity impacts on connected medical devices, and the regulatory developments surrounding this area. It will cover the difference between mobile apps and mobile medical devices, and will look at cyberattacks on medical institutions.

2. Medical Devices

This white paper will review cybersecurity in the context of medical devices that either contain software, including firmware and programmable logic controllers (e.g. pacemakers, insulin pumps), or exist solely as software (e.g. Software as a Medical device (SaMD)).

SaMD has been classified by the International Medical Device Regulators Forum (IMDRF) into 4 categories. It can range from software that allows a smartphone to view images obtained from a magnetic resonance imaging (MRI) medical device for diagnostic purposes to

Computer-Aided Detection (CAD) software that performs image post-processing to help detect breast cancer. Examples of software that is not classified as a medical device includes:

- Software that relies on data from a medical device, but does not have a medical purpose, e.g., software that encrypts data for transmission from a medical device
- Software required by a hardware medical device to perform the hardware's medical device intended use, even if sold separately from the hardware medical device

Differences do exist between EU and US regulations of SaMD. Some examples are:

- It is significantly harder in the EU to get SaMD approved and on the marketplace, whereas the US has removed some of its requirements
- Classification of SaMD in the EU is more complex than in the US, where it is very straightforward

The rise of the Internet of Things (IoT) and the push for greater connectivity, has made the connectivity of all devices, including medical devices, susceptible to both organized cyber criminals as well as malevolent hackers. In the US there are an estimated 10 to 15 connected devices per hospital bed, some or all of which are vulnerable to cyberattack.

The healthcare industry has long been a target of cyberattacks because of the copious amounts of patient health information and data and the number of devices that can present entry points of attack. Reducing cybersecurity risks is especially challenging and manufacturers, hospitals, and facilities must work together to manage the various cybersecurity risks.

Reasons why medical device cybersecurity is so important:

- Medical devices can be an easy entry point for attackers as new devices open up more potential entry points for security breaches. Medical devices and SaMD play a critical role in modern healthcare
- Healthcare facilities are a target because they act as storage for an immense amount of confidential patient data which can be sold for large sums of money or held for ransom
- Budget limitations and the hesitance of healthcare facilities to learn/teach new systems results in outdated technology, which means the healthcare industry is unprepared for attacks
- Time, budget and resource restraints result in medical professionals that are not trained to deal with online threats, and it is a difficult task for healthcare industry staff to be fluent in cybersecurity best practices
- The number of devices used in hospitals makes it difficult to stay on top of security

As early as 2012, the US government has been aware of the vulnerability of wireless medical devices and the possibility of the hacking of these devices. A government accounting office (GAO) report noted that researchers were able to demonstrate the potential for incidents resulting from intentional threats in two devices. First, an implantable cardioverter defibrillator and secondly an insulin pump. To date no such actual incidents are known to have occurred, according to the Food and Drug Administration (FDA). As medical devices may be susceptible to unintentional and intentional hacking, concerns include:

- Untested software and firmware
- Limited battery life

In one instance, right out of a mystery novel plot, Barnaby Jack, who worked as a professional hacker for McAfee, demonstrated ways to manipulate the wireless capabilities on devices made by Minneapolis-based Medtronic Inc. (MDT) to remotely take over the pumps and dispense fatal doses of insulin.

In another case, an independent security researcher discovered eight security vulnerabilities in the Medfusion 4000 Wireless Syringe Infusion Pump, which is manufactured by Smiths Medical. Alerts were published by the US Cyber and Infrastructure Security Agency (CISA).

Apps vs devices

From a regulatory viewpoint, apps are standalone software.The US FDA has defined apps and devices as follows:

- Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software
- Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device, and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device

Although the FDA has not issued an overarching software policy, the agency has formally classified certain types of software applications that meet the definition of a device and, through classification, identified specific regulatory requirements that apply to these devices and their manufacturers. These software devices include products that feature one or more software components, parts, or accessories, as well as devices that are composed solely of software.

The FDA has previously clarified that when a software application is used to analyze medical device data, it has traditionally been regulated as an accessory to a medical device or as medical device software. In 2014, the International Medical Device Regulators Forum established globally harmonized vocabulary for such software applications and defined the term "Software as a Medical Device (SaMD)."

European Union

In Europe, Article 1 of the Medical Device Directive (MDD) defines a medical device as "*software intended by the manufacturer to be used for human beings for the purpose of: diagnosis, prevention, monitoring, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap; investigation, replacement or modification of the anatomy or of a physiological process; control of conception.*" The EU does not use the SaMD acronym but instead uses the term Medical Device Software (MDSW).

This means that software such as a medical app that works in combination with a device (a smartphone) is a medical device. Before being put into free circulation and used in medical practice, mobile technology and medical apps must satisfy the legal requirements detailed in Directive 93/42/EC.

Many apps performing medical activities are not considered medical devices in a strict legal sense. Developers can get their way out of the requirements mandated by the MDF simply by not stating that the app has a medical purpose. The difference between considering an app to be a medical device or not is relevant for the safety of the patient, for doctors' liability, as well as for the relationship between patient and doctors.

3. Medical Devices / Healthcare Applications

Technology in healthcare devices includes both professional applications as well as everyday consumer products. Medical device applications are being used to treat a variety of conditions including:

- Heart disease
- Stroke
- Insomnia
- Digestion issues
- Immune system disorders
- Anxiety disorders

- Depression

Examples of new professional applications in wearable medical technology include:

- Cardiac monitoring
- Blood pressure monitors
- Glucose monitoring pumps and sensors
- Cancer detection sensors
- Portable dialysis devices
- Biosensors

Medical applications are also found in consumer products, like fitness trackers and smart watches, where devices are designed to collect the data of users' personal health and exercise. These devices can even send a user's health information to a doctor or other healthcare professional in real time.

For example, in 2020, Apple's Series 6 watch included a new blood oxygen saturation monitoring feature, new sleep-tracking capabilities, an improved FDA-approved electrocardiogram sensor, and upgraded heart monitoring features. Consumer demand to monitor their own health and track their own vital signs has more than tripled in the last four years. According to research from Insider Intelligence, more than 80% of consumers are willing to wear fitness technology.

4. The International Medical Device Regulators Forum

The International Medical Device Regulators Forum (IMDRF), is a voluntary group of medical device regulators from around the world. Recognizing the necessity to provide concrete recommendations to all responsible stakeholders on the general principles and best practices for medical device cybersecurity (including in vitro diagnostic (IVD) medical devices) they have created a guidance document for best practices and procedures involving cybersecurity.

It outlines recommendations for medical device security and describes important requirements on information security and cybersecurity such as the protection against unauthorized access. The document's intent is to minimize cybersecurity risks that could arise from use of the device for its intended purposes; and to ensure maintenance and continuity of device safety and performance.

This is intended to facilitate international regulatory convergence on medical device cybersecurity. Medical device manufacturers can improve their cybersecurity by implementing the following 7 steps:

1. Secure communications:
The manufacturer should consider how the device will interfere with other devices / networks, communication with devices supporting a less secure communication, and prevention of unauthorized access / modification when it comes to data transfer to and from the device.

2. Data protection:
The manufacturer should consider whether a level of protection or encryption is required for data stored or transferred on the device and if the device needs confidentiality risk control measures.

3. Device integrity:
The manufacturer should consider risks that affect the integrity of the device, evaluate the system-level architecture to look for necessary design features, and consider anti-malware controls.

4. User authentication:
The manufacturer should consider user access controls that determine who can use the device or provide granting of privileges to user rolls.

5. Software maintenance:
The manufacturer should consider the communication process when implementing regular updates, how software will be updated or controlled, how the device will be updated to secure it against other vulnerabilities, the required connections to conduct updates, and the use of code signing for authenticity of the connection.

6. Physical access:
The manufacturer should consider implementing controls that prevent access of the device by an unauthorized person.

7. Reliability and availability:
The manufacturer should consider inputting design features that allow the device to detect, resist, respond, and recover from cybersecurity attacks.

compliance & risks

5. Standards Recommendations

The following international standards have been created and implemented in medical device cybersecurity protocols. These standards are voluntary.

1. AAMI TIR57:2016 Principles for medical device security—Risk management
2. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers
3. IEC 60601-1:2005+AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance
4. IEC 62304:2006/AMD 1:2015, Medical device software – Software life cycle processes
5. IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices
6. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
7. IEC TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
8. IEC TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
9. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes
10. ISO 14971:2019, Medical devices – Application of risk management to medical devices
11. ISO/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
12. ISO/IEC 27000 family - Information security management systems

13. ISO/IEC 27035-1:2016, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management

14. ISO/IEC 27035-2:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

15. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure

16. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling Processes

17. ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971

18. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements 21. UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

6. Cyber Attack Examples

While personal device hacking has been shown to be possible, to date there have been no reports of this having occurred. Attacks on medical organizations, however, have been documented.

1. On Friday 12 May 2017, a computer virus known as WannaCry, which encrypts data on infected computers and demands a ransom payment to allow users access, was released worldwide. WannaCry was the largest cyberattack to affect the NHS in England.

   NHS England initially identified 45 NHS organizations including 37 trusts that had been infected by the WannaCry ransomware. In total at least 81 out of 236 trusts across England were affected. A further 603 primary care and other NHS organizations were infected by WannaCry, including 595 GP practices. However, the department does not know how many NHS organizations could not access records or receive information, because they shared data or systems with an infected trust. NHS Digital told us that it believes no patient data were compromised or stolen.

The WannaCry ransomware attack affected hundreds of thousands of computers worldwide, costing companies and organizations millions of dollars in damages.

Yet the software vulnerability used by the attack, dubbed 'EternalBlue', was corrected and patched by Microsoft months before the attacks took place. If the affected computers had just had the security update downloaded and installed, they would never have been compromised.

2. In 2017, Erie County Medical Center, in Buffalo, NY, was hit with a ransomware attack that forced it to return to pen and paper records after shutting down its computer system. Rather than pay the $30,000 demand the hospital was forced to rebuild its entire IT structure at an estimated cost of 10 million dollars. Investigators believe the ransomware attack was caused by SamSam, an automatic program unrecognizable by anti-virus software. The hackers then tried millions of character combinations to identify a password allowing them to gain entrance into the hospital's system.

7. Methods of Cybersecurity Protection

In looking at ways to secure medical devices we can look at several different issues.

First, securing medical facilities, better training and policies for website, network and database security using digital certificates and online security policies, can ensure that medical organizations that use the internet for daily operations are secure from most hacking attempts. A 2018 report by Verizon found that, *"Healthcare is the only industry where the threat from inside is greater than that from outside. Human error is a major contributor to those stats."* Robust training programs are needed to help ensure data security from user error. Ensuring that every digital device or application has a digital identity that is authenticated (enabling encrypted communications), hospitals can greatly deter security break in attempts. Preventing hackers from access to the IT networks is the first step in stopping attacks on medical devices and other systems inside the network.

Second, is building security into a device. This requires security features that will protect the device from attack, protect the integrity of the device, and enable device identity. Manufacturers, suppliers, and designers in the sector have adopted best-practice technologies for connected device security, including:

- Embedded software APIs that ensure software integrity known as "secure booting"

- Embedded firewalls that prevent communication with unauthorized devices and block malicious messages
- Secure remote updates - a methodology by which updates are authenticated and validated before permitting their installation
- Secure element integration - the addition of a chip that is by design protected from unauthorized access and used to run a limited set of applications, as well as store confidential and cryptographic data

Another issue to consider regarding medical devices is coordinated vulnerability disclosure (CVD). CVD is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public. CVD should be part of manufacturers' proactive approach to medical device cybersecurity because it aids in improving patient health and safety.

Security vulnerabilities remain a problem for vendors and deployers of software-based systems alike. No software-enabled medical device is free of vulnerabilities so participating in CVD should be a part of routine practice. It is not the number of vulnerabilities that serves as an indicator of a manufacturer's cybersecurity policy, but rather the way in which it responds. CVD should be part of a manufacturers' medical device cybersecurity protocol because it aids in protecting patient health and safety.

Vendors play a key role by providing fixes for vulnerabilities, but they are not the only entities with the ability to discover vulnerabilities in their products and services.

Healthcare providers and patients should be made aware that CVDs from manufacturers and through computer emergency response teams (CERT) and Computer Security Incident Response Teams (CSIRT) or government regulators are authoritative sources of information regarding potential vulnerabilities.

For example, the US Cybersecurity & Infrastructure Security Agency (CISA) CVD program, coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in industrial control systems (ICS), Internet of Things (IoT), and medical devices, as well as traditional information technology (IT) vulnerabilities. The goal of CISA's CVD program is to ensure that CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously, to ensure that users and administrators receive clear and actionable information in a timely manner.

The Health Information Trust Alliance (HITRUST) Risk Management Framework (RMF) is a model implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Consistent with the NIST framework, the HITRUST CSF provides a comprehensive, prescriptive, yet flexible, information security control framework that leverages the risk analyses used to develop its supporting authoritative sources.

HITRUST reviewed several cybersecurity related best practice frameworks, including the SANS 20 Critical Controls for Cybersecurity 12 and, in June 2013, identified 59 CSF controls determined to be most relevant to cybersecurity, which helps provide assurances as to how well one is addressing cyber-specific threats.

CVE® is a list of publicly disclosed cybersecurity vulnerabilities and exposures that is free to search, use, and incorporate into products and services. It is currently maintained by MITRE and is available at https://cve.mitre.org/cve/.

MITRE manages federally funded research and development centers (FFRDCs) supporting various US government agencies in the aviation, defense, healthcare, homeland security, and cybersecurity fields, among others.

NIST manages and maintains the National Vulnerability Database (NVD). The NVD is the US government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

The NVD is the CVE list augmented with additional analysis, a database, and a fine-grained search engine. The NVD is synchronized with CVE such that any updates to CVE appear immediately on the NVD.

8. Alerts

In the US, when notified of a software medical device vulnerability, the FDA will publish a Safety Communication. For example:

Security researchers have identified 12 vulnerabilities, named “SweynTooth,” associated with a wireless communication technology known as Bluetooth Low Energy (BLE). BLE allows two

devices to “pair” and exchange information to perform their intended functions while preserving battery life.

The potential impacts of the SweynTooth vulnerabilities fall into three categories. An unauthorized user can wirelessly exploit these vulnerabilities to:

- Crash the device - the device may stop communicating or stop working
- Deadlock the device - the device may freeze and stop working correctly
- Bypass security to access device functions normally available only to an authorized user

The FDA is currently aware of several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities.

- Cypress
- Dialog Semiconductors
- Microchip
- STMicroelectronics
- Telink Semiconductor

9. Recall Examples

The below examples highlight some medical device cybersecurity issues that have arisen in recent times:

1. Smiths Medical has become aware of a software issue in the most recently updated Medfusion® 4000 Syringe Pump Firmware, Version 1.7.0, that could potentially cause the low battery alarms to stop working. If the battery alarms do not work, the healthcare provider using the pump will not receive audible or visual notification that the battery is shutting down. This may lead to an interruption of therapy which may lead to serious injury, adverse events, or death.

2. In 2017, the FDA recalled 465,000 radio-controlled implantable cardiac pacemakers made by St. Jude Medical due to the potential for cybercriminals to hack the devices. For instance, hackers could run down the batteries or alter the patient’s heartbeat, both worst-case scenarios that could result in the death of the patient. Affected patients did not have to have the devices removed. Instead, Abbott, which owns St. Jude, issued a firmware update in 2018, incorporating more stringent security.

10. Conclusion

Medical device cybersecurity is a shared responsibility between users, manufacturers, and healthcare providers. All parties must understand their responsibilities and work closely with other parties to continuously monitor, assess, mitigate, communicate, and respond to potential cybersecurity risks and threats.

In order to prevent the types of attacks we have seen on organizations and mainframe devices, manufacturers and developers must work closely to prevent vulnerabilities from reaching the marketplace and the individual devices. Potential hacking of individual devices has been shown to be possible and is likely an issue of when, not if, hacking of this type will happen. Cybersecurity has to continue throughout the life cycle, from cradle to grave, of the medical device.

Achieve Uninterrupted Market Access for Your Medical Devices!

Compliance & Risks provides companies with the confidence that their medical devices are compliant with global regulations.

With C2P, the market access and compliance knowledge management platform, manufacturers are able to simplify the complex world of compliance and stay on top of new and changing legislation.

Our clients can easily monitor the changing regulatory environment, manage their product requirements, and control the evidence to prove their compliance. All from a single, purpose-built tool.

Book a Demo

compliance & risks

11. Sources

1. https://www.fda.gov/news-events/fda-brief/fda-brief-fda-warns-patients-providers-about-cybersecurity-concerns-certain-medtronic-implantable
2. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
3. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
4. https://www.promenadesoftware.com/blog/why-cybersecurity-is-becoming-more-important-in-medical-device-1
5. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
6. https://www.accesspartnership.com/access-partnerships-guide-to-computer-emergency-response-teams-certs/
7. https://us-cert.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf
8. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches
9. https://www.gao.gov/products/gao-12-816
10. https://thehackernews.com/2012/10/medical-devices-vulnerable-to-hacking.html
11. https://vuls.cert.org/confluence/display/CVD
12. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
13. https://www.fda.gov/medical-devices/medical-device-safety/safety-communications
14. https://us-cert.cisa.gov/ics/alerts
15. https://nvd.nist.gov/
16. https://cve.mitre.org/cve/
17. https://healthmanagement.org/c/healthmanagement/issuearticle/medical-apps-a-view-from-medical-device-and-data-protection-law
18. https://www.fda.gov/media/80958/download
19. https://www.fiercehealthcare.com/privacy-security/buffalo-hospital-sinks-10m-into-rebuilding-its-network-after-a-ransomware-attack
20. https://www.ept.ca/features/keeping-medical-devices-safe-from-cyber-attacks/
21. https://www.medpro.com/cybersecurity-training-for-healthcare-workers
22. https://healthtechmagazine.net/article/2019/10/why-all-healthcare-workers-need-cybersecurity-training
23. https://www.fda.gov/medical-devices/software-medical-device-samd/what-are-examples-software-medical-device
24. https://www.bsigroup.com/globalassets/localfiles/en-th/Medical%20devices/brochure/software-as-a-medical-device--th.pdf
25. https://www.mpo-mag.com/issues/2018-06-01/view_columns/mobile-medical-applications-the-regulatory-framework-in-the-us-and-the-eu/
26. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7381013/

About the Author

Jerry Miller

Senior Regulatory Consultant, Compliance & Risks

Jerry is a Senior Regulatory Consultant with 20 years experience in regulatory and standards interpretation, spanning the fields of consumer products and environmental investigation.

At Compliance & Risks, Jerry performs international research and database creation for clients and acts as a subject matter expert on various laws and standards.

About Compliance & Risks

Compliance & Risks helps manufacturers, retailers and their supply chain partners monitor and manage requirements, regulations and standards for a cleaner, safer and better world. It creates business advantage for clients by providing reliable legislative information, insights and actions through C2P, its compliance knowledge management platform, consulting, market access, managed services and other solutions.

The company is recognized as the end to end global regulatory solutions provider across the technology, consumer goods and retail, industrial goods and life sciences sectors. Headquartered in Cork, they also have offices in Brussels, California, London and New York. For more information, please visit www.complianceandrisks.com