Medical Device Cybersecurity Regulatory Pathway

Posted 26 July 2019 | By Carolyn Wright, MS

The snowballing innovation in the medical industry has resulted in a marketplace where it is common for medical devices to be connected to the internet. To keep pace, the US Food and Drug Administration (FDA) is leaning on the learnings from other industries to springboard the medical industry into a stronger cybersecurity position. This article discusses the changes in technology that has brought about the need for cybersecurity, regulatory history, recent developments in cybersecurity regulatory and postmarketing requirements, cybersecurity risk management programs and some best practices for medical device product development teams who are looking to design in cybersecurity.

Introduction

“In February 2016, the Hollywood Presbyterian Medical Center, CA, US, paid hackers $17,000 to regain access of the hospital’s computers after a “ransomware” virus locked doctors out of the system.”

The introduction of the internet in 1989 and the subsequent connection of critical medical systems in the late 1990s has improved the quality and efficiency of healthcare. However, this connectivity introduced additional risks to patient care and privacy. It is only a matter of time before situations previously considered fiction become reality.

FDA has been working diligently to keep up with the rapid rate of technology change and over the years has published guidance documents that require security measures be incorporated into medical software. One of the earliest guidance documents, *Off-the-Shelf Software use in Medical Devices* requires software designers build in the capability to update software after the product has been marketed and distributed to ensure that it remains safe and effective through its full life. Unlike pharmaceutical products that are consumed, a medical device may remain with the patient for 20-50 years, and if the software is later determined to need an upgrade due to security risks, there must be a method to provide these updates (patches) even for implanted devices.
New Capability Brings New Risks

Once the ability to access and update medical software became a reality the new risks of hackers and malicious software became a concern. To detour these risks cybersecurity requirements were developed and have become part of the current expectations for medical device software.

Cybersecurity is defined as the process of preventing unauthorized access, modification, misuse, denial of use or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.4

Failure to maintain current cybersecurity standards can result in compromised functionality, loss of data or exposure of other connected devices or networks to security threats. Once the software security has been breached the risk of patient illness, injury or death is dangerously high.5

Cybersecurity Threats

The mandate FDA placed on medical software, to be updatable after it has been marketed, requires remote access and association with a PC or other networked device. Unfortunately, this subsequent connection leaves the medical devices exposed to theft, scams and exploitation. Hackers are aware of device and network weaknesses and are able to use these flaws to exploit the device, steal medical records or patient case history databases.6 There are a constantly growing number of ways that software can be exploited using some of the more common malware listed below.

- Ransomware is a type of software used to capture, lock down or block the access to a computer system or its data.
- Spyware is software designed to collect information about a person or organization anonymously.
- Trojan Horse software is embedded inside a second apparently harmless software or data file. Once the software is downloaded by the user it can take control or cause whatever damage it is designed to do, including opening the system to ransomware or allowing another person to take remote control of the system.
- Virus – a virus is a self-replicating piece of software that clings itself to a program file or a drive. These viruses can corrupt or destroy valuable patient records or other stored medical data. Viruses also can stop or corrupt medical device commands or signals causing it to act incorrectly.
- Phishing is a process in which a person is contacted by email, telephone or text by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details and passwords. The data that is collected is later used to access important accounts which can result in identity theft and financial loss.7

Regulatory History

Congress passed the Medical Device Amendments (MDA) of 1976 which established for the first
time a comprehensive scheme for the pre and postmarket regulation of medical devices. FDA accordingly developed a three-part classification system defined by different rules.

Class I was assigned to those devices with the lowest risk. It was believed by lawmakers that general postmarketing controls would be enough to provide reasonable assurance of safety and effectiveness for these devices.

- Class II was assigned to devices of moderate risk, that did not fall into the Class I or Class III categories. General controls were not believed to be sufficient by themselves to provide reasonable assurance of safety and effectiveness, these devices were not considered to be life supporting or sustaining. Class II devices are required to follow Good Manufacturing Practices (GMPs) and, if applicable, FDA-established performance standards. For Class II devices to enter the market a 510(k) application is submitted to FDA, and after a successful review, it is cleared to enter the market. However, the 510(k) process does not require the manufacturer to prove device safety or effectiveness, only substantial equivalence to a predicate Class II device.

- Class III was assigned to devices with the most complexity, highest risk or those that were used for supporting or sustaining life. These devices would be subject to the most stringent controls and FDA approval, via a Premarket Application (PMA), was required prior to marketing and distribution of these devices.

In 1987, FDA revised the current Good Manufacturing Practice (CGMP) requirements for medical devices and incorporated them into a Quality System Regulation (QSR). This updated regulation included requirements and controls for designing, manufacturing, packaging, labeling, storing, installing and servicing of medical devices.

FDA conducted a subsequent review of the medical device industry and found one of the top four inspection deficiencies was in the area of design control. Therefore, additional requirements were added to the design process of medical devices, section 820.30 of Title 21, Code of Federal Regulations. This new expectation required manufacturers to establish and maintain procedures for design development, plans to control and verify device design as well as to ensure that the design requirements were met. The device manufacturer was now also expected to establish and maintain procedures that ensured the design requirements were appropriate for the intended use and needs of both the users and patients. The medical device design process according to §820.30 was expected to also include a comprehensive user risk assessment that was specifically based on the product design, and included human factors analysis.

In November 2018, to promote innovation and help patients access safe and effective treatments, FDA started actively encouraging device manufacturers to use recently approved (less than 10 years old) predicate devices with their 510(k) submission.

“As devices become increasingly complex, it’s important that they meet the latest standards for cybersecurity, interoperability, biocompatibility and usability engineering. FDA has recently advanced policies on these issues, and we know that older predicates often don't meet our more recent expectations.”

This medical device classification system, while upgraded over the years based on technology changes, has remained the foundation for the US medical device regulatory process. Cybersecurity is a more recent and additional requirement for medical devices, that contain software, and has been incorporated into the following areas:

- Guidance
- Standards
- Postmarketing Requirements
- Cybersecurity Risk Management Program

Cybersecurity Guidance

As part of the software validation and risk analysis, required by 21 CFR 820.30(g), manufacturers of medical software devices, standalone software applications and hardware-based devices that incorporate software, should establish a cybersecurity vulnerability and management analysis. FDA recommends that this approach include a set of cybersecurity design controls to ensure medical device cybersecurity and thereby safety and effectiveness.\(^{10}\)

The introduction of software into the medical area has brought with it the possibility of injury related to the compromise or lack of function of the software. In alignment with the risk management thought process described in ISO 14971 and to address this concern, a new risk classification, ‘level of concern,’ has been created by FDA to describe the software’s potential impact on injury severity. The level of software-related documentation to be included premarket submission generally depends on the device’s Level of Concern (Table 1).

<table>
<thead>
<tr>
<th>Software Documentation</th>
<th>Minor Concern</th>
<th>Moderate Concern</th>
<th>Major Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of Concern</td>
<td>A statement indicating the level of concern and a description of the rationale for that level.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>A summary overview of the features and software operating environment.</td>
<td>Tabular description of identified hardware and software hazards, including severity assessment and mitigations.</td>
<td>Summary of functional requirements from SRS.</td>
<td>No documentation is necessary in the submission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detailed depiction of functional units and software modules. May include state diagrams as well as flow charts.</td>
</tr>
<tr>
<td>Revision Level History</td>
<td>Revision history log, including release version number and date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unresolved Anomalies (Bugs or Defects)</td>
<td>No documentation is necessary in the submission.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>List of remaining software anomalies, annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The clearly identifying the cybersecurity design controls in the submission documentation package will allow FDA reviewers to quickly determine if the device meets the applicable cybersecurity statutory standard for premarket review.

**Cybersecurity Consensus Standards**

The emergence of consensus standards related to software has helped to improve the consistency and quality of software development and documentation, particularly with respect to critical activities such as risk assessment and management. These standards are generally created by industry groups and then after peer review can be submitted to FDA so that they will be recognized as a Consensus Standard.

**Postmarketing Requirements**

FDA laid out expectations for activities that should occur once the medical devices are cleared or approved to be marketed. However, the increased complexity of the security needs for data transmission and its associated impact on battery life have made compliance with these expectations difficult for manufactures.

It is mandatory for manufacturers, importers and device user facilities to report any medical devices that may have directly caused or contributed to a patient’s serious injury and/or death, 21 CFR 803, (voluntary for healthcare professionals, patients and consumers). Unfortunately, interoperability of medical devices is impacting the accuracy of these reports. Interoperability occurs when medical devices and digital health solutions interact with one another to provide the intended healthcare. When these devices fail to work together to give the proper treatment and as a system cause an adverse event, the devices causing the problem need to be reported. Unfortunately, it is no longer clear which of the component of the system caused the failure and should be reported.

Field software updates are another expectation of FDA for all types of connected devices because as technology evolves older software becomes less secure and therefore needs to be updated, patched. This security concern also extends to mobile (implanted or otherwise) medical device where the impact of failure to update could result in serious health risks to the patient. Field software updates are a critical capability that needs to be designed into the device during the product development stage and verified as effective prior to launch and after subsequent changes to the product design.
Cybersecurity risks to medical devices are continually evolving, and FDA understands it is not possible to completely mitigate all risks through premarket controls alone. Therefore, FDA has published a requirement that manufacturers of medical devices that are, or contain, software implement a comprehensive cybersecurity risk management program. It is expected that this program will address vulnerabilities which may permit the unauthorized access, modification, misuse denial of use or the unauthorized use of information that is stored, accessed or transferred from a medical device and may result in patient harm. FDA guidance entitled, *Postmarket Management of Cybersecurity in Medical Devices*, clarifies that manufacturers are expected to manage postmarket cybersecurity risks for medical devices and in a structured and systematic approach aligned with 21 CFR part 820. FDA further recommends the manufacturers incorporate elements consistent with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity into their cybersecurity program.

**Cybersecurity Risk Management Program**

In 2014, the *Cybersecurity Enhancement Act (CEA)* expanded the role of the National Institute of Standards and Technology (NIST) to include identifying and developing a cybersecurity risk framework, high level guidance that could be used by critical infrastructure owners and operators on a voluntary basis. The goal of this framework was to create a cost-effective approach that all companies could use to enhance their overall risk management program relative to cybersecurity. The Framework for Improving Critical Infrastructure Cybersecurity was initially released in February 2013 and later updated in April of 2018 after industry feedback and contributions through various workshops that were held by FDA.

The framework lays out five different voluntary behaviors that all companies should address to various degrees and then drills down to give categories and subcategories of activities. Finally, in Appendix A the framework provides a variety of standards that can be used to guide and encourage industry on how to establish these behaviors within their companies.

<table>
<thead>
<tr>
<th>Table 2. Cybersecurity Framework Behaviors and Supporting Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Behavior</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Identify</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
FDA is expecting that medical device manufacturers build cybersecurity risk assessment into their product development process and that they should independently have a company-based cybersecurity program. The level of complexity and detail the program recommends is based on the business need and product technology. The framework provides a seven step process that industry can use to create or update their current program. It also provides encouragement and techniques for self-assessment and external participation with industry on cybersecurity risk and defense techniques.18

New FDA Cybersecurity Tools
Ethical Hackers

FDA is now seeing value in the use of ethical hackers to identify and fix vulnerabilities in medical devices and software and security. Cyberattacks have been on the rise as technology has increased, potentially putting patient lives at risk. Medical device makers have historically resisted the use of ethical hackers; however, this concern has grown into a reality and FDA has started to engage in discussions on this topic. Recently, FDA has participated in a collaborative use of hackers encouraging them to investigate the possibility of taking control of a cardiac implant. This activity led to the issuance of a security warning and a corrective action to the device itself. The use of ethical hackers or penetration tests as a risk management tool have started to become more common for medical devices that contain software.

MedWatcher app

FDA developed the MedWatcher Mobile App to make it easier for the public and medical personal to conduct the voluntary reporting process and increase accessibility. The intent was to encourage patients and/or providers to report via the app on their mobile device, as compared to the traditional, more cumbersome, methods of mail, telephone or computer. This app was not to be used as a replacement for the manufacturers mandatory medical device reporting. Unfortunately, it is unclear how effective this app has been because it has been down, at the time of this writing, for an extended period of time.

Participation in an Information Sharing Analysis Organization (ISAO)

While it is still voluntary the agency considers active participation in an ISAO to be a critical proactive approach to management of postmarket cybersecurity threats and vulnerabilities. For companies that actively participate in such a program and follow other recommendations in this guidance, the agency does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (Section VII).

Example of a Filing Requirements for a Medical Device Containing Software

The regulatory pathway for a medical device may on the surface seem straight forward especially if there is a predicate device on the market with the same intended use and mechanism of action. However, the connectivity of medical devices brings with it increased requirements and responsibility for the manufacturer.

If a medical device is designed to be networked to facilitate patient care, the additional programs and documentation are required by FDA to market and distribute the medical device. To give a tactical example of the increased requirements for medical devices that contain software a list of medical device filing requirements is provided below.

Standard Activities for Medical Device Application

identification of the device’s intended use
identification of device’s mechanism of action
expected classification of medical device
identification of the class II predicate device(s) for the application

**Design Control Requirements**

documented product development process
user requirements (user needs)
system requirements
risk assessment – ISO 14971, FMEA or other

If the intended use of the device is to monitor, communicate or control, the software will be incorporated into the device which will invoke the need to apply software requirements to ensure the safety and effectiveness of the device over as long as it is in use.

**Additional Cybersecurity Requirements**

inclusion of cybersecurity design requirements in the system requirements
development of a cybersecurity risk management program
assessment of the software level of concern
software validation
method for updating all marketed devices when a cybersecurity patch is required
device performance monitoring including:

cybersecurity detection monitoring
values identified as a detection method for device risks identified in the device risk assessment
parameters identified during quality audits, complaint management or as part of a Corrective or Preventative Action (CAPA) by the quality management system

**Conclusion**

The snowballing innovation in the medical industry has caused it to be commonplace for medical device to be connected to the internet and to each other. However, the healthcare sector has not advanced in the area of cybersecurity to the same degree as other industries. “As an entire critical infrastructure sector, we are behind finance and some of the other sectors,” says Suzanne Schwartz, acting director of emergency preparedness and medical countermeasures.

Historically, the major focus of hackers has been on other industries, so until recently there has not been an aggressive threat to patient health. Healthcare cybersecurity is now being taken more seriously and FDA is leaning on knowledge acquired by other industries to springboard the medical industry into a more secure position. Manufacturers of software bearing medical devices need to take very seriously the recommendation to implement, the *Framework for Improving Critical Infrastructure Cybersecurity*, as well as the recommendation to actively join Information Sharing Analysis Organization (ISAO). FDA needs to develop methods to monitor the incorporation of these recommendations quickly so that they can be included in medical device audits. There is no way to know for certain if the incorporation of cybersecurity techniques by manufacturers can be done quickly and effectively enough to prevent data breach events. However, now that FDA
recommendations are public, medical facilities and manufacturers need to work together to quickly educate each other and drive swift cybersecurity implementation to protect patient health and privacy.

References

2. Ibid.
5. Ibid.
7. Ibid.
12. Ibid.
13. Op cit 11
16. Ibid.
18. Ibid.

About the Author

Carolyn Wright, MS, is director of clinical operations at QST Consultations with more than 15 years of drug and medical device experience in areas of clinical efficacy and safety, quality assurance, regulatory affairs, trial stage and commercial product manufacturing. She received her master’s degree in regulatory for drugs, biologics and medical devices from Northeastern University. She has a
Six Sigma Black Belt and has managed multiple ANDA transdermal product development programs as well as global regulatory and safety assessments for new topical, nutritional and medical device products. She has authored papers related to risk management, IOT connected device validation and cybersecurity. Wright’s combined quality, operational and global regulatory experience has enabled her to lead teams to successful execution while ensuring exceptional quality. She can be contacted at cwright@qstconsultations.com.

Cite as: Wright C. “Medical Device Cybersecurity Regulatory Pathway.” *Regulatory Focus*. July 2019. Regulatory Affairs Professionals Society.