Integrating the Healthcare Enterprise

IHE PCD in Cooperation with MDISS White Paper

Medical Device Software Patching

Draft for Public Comment

Revision 1.0

Date: July 1, 2015
Author: IHE PCD Technical Committee
Email: pcd@ihe.net

Please verify you have the most recent version of this document. See here for Final versions and here for Public Comment versions.

Foreword

This white paper is published on July 1, 2015 for public comment. Comments are invited and can be submitted at http://www.ihe.net/PCD_Public_Comments/. In order to be considered in development of the final version of the white paper, comments must be received by July 31, 2015.

General information about IHE can be found at: www.ihe.net.

Information about the IHE Patient Care Device domain can be found at: ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE Patient Care Device Technical Framework can be found at: http://www.ihe.net/Technical_Frameworks.

CONTENTS

1 Executive Summary

The Medical Device Innovation, Safety and Security (MDISS) Consortium and Integrating the Healthcare Enterprise, Patient Care Device Domain (IHE PCD) have identified the need for a common understanding of existing regulations, industry standards, risks, and complexities as the essential first step in their effort to support the creation of a Medical Device Software Patching Best Practices to be applied by medical device manufacturers and healthcare delivery organizations (HDOs). This white paper focuses on the specific security risks to networked medical devices built on Commercial of-the-Shelf Software (COTS) and the importance of a timely and well-executed patch process to maintain the device's security posture to prevent compromise of device availability, integrity, and confidentiality; ultimately improving patient safety.

1.1 Ackowledgement

This whitepaper was developed in cooperation between MDISS (Medical Device Innovation, Safety and Security Consortium) and IHE PCD (Integrating the Healthcare Enterprise, Patient Care Device Domain). IHE PCS and MDISS would like to acknowledge the following contributors to this paper:

Britton Burton	Hospital Corporation of America
Dr. Dale Nordenberg	MDISS
Andrew Sargent	Philips Healthcare
Daniel E. Silverstein	Kaiser Permanente
Axel Wirth	Symantec

1.2 Problem Statement

Medical Devices utilizing COTS software in the operating system, for example, are at risk of hackers or malware targeting the respective COTS vulnerabilities. This can result in:

- Compromised device functionality
- Compromised data integrity
- Patient safety risks due to device or data compromise
- Operational impact due to downtime
- Penetration of the larger enterprise network due to exploitation of the device as the "weakest link"
- Financial impact due to loss of revenue and productivity, remediation costs, damage to reputation, and potentially law suites and fines

Typically, the medical device manufacturer's application software is less vulnerable to attacks as any vulnerability and its exploitation would have to be targeted and unique to that application software. COTS, on the other hand, are vulnerable to both a targeted attack as well as an indiscriminate or unintentional attack due to common vulnerabilities and broad distribution of malware.

Examples for COTS include:

- Operating Systems (Windows, standard Linux, etc.)
- Media Players, Readers, and other utilities
- Databases
- Runtime Environments (e.g., Oracle Java)

Timely deployment of manufacturer COTS patches one of the key measures HDOs can undertake in order to minimize vulnerabilities and exposure, resulting in a lower security risk. However, complex regulations, misinterpretation and misunderstandings, poor communication, and practical limitations often result in delayed patch deployment and poor patch hygiene.

Although the same concept of patching applies to open source, proprietary and COTS software, the urgency and required frequency is usually higher with COTS due to the larger number of well-known and exploitable vulnerabilities. What we see often is that medical device application software patches have been driven by bug fixes and feature enhancements, while COTS patching should be driven by security considerations, typically giving it a higher priority.

In addition to the complexity in patch management, there may be an even more insidious aspect hiding behind COTS products. It is becoming increasingly clear that the COTS software supply chain lacks sufficient transparency for any arbitrary member of the supply chain to determine what is actually in the COTS product and how this impacts the cybersecurity posture of the finished product. Accordingly, many necessary patches may not be applied simply because the "ingredients" of the COTS are not fully known and understood. This emerging additional risk can lead to a false sense of security. Tools are beginning to emerge which can detect this phenomenon and should be rapidly employed by participants in the software supply chain. Only with sufficient transparency into the COTS products can a strategy of regular patching succeed.

Regulators mandate that medical device manufacturers produce and sell safe and effective medical devices, requiring a formal product development, test, and release process. As a result, medical device product updates including patches are not deployed as frequently as they are in the normal IT environment.

At the same time, especially in consideration of todays sophisticated and numerous threats, the mitigation of COTS vulnerabilities is critical to availability, integrity, and confidentiality. A manufacturer's quality system has to be concerned about device safety as a result of cybersecurity vulnerabilities and therefore timely release of patches is critical. The growing tension between the need to patch frequently and the formal and time-consuming release process is an increasing challenge for all stakeholders: regulators, device manufacturers, and HDOs.

Recently, agencies like the US FDA, FBI, Homeland Security, and US CERT, have issued specific warnings and guidance on cybersecurity for medical devices.

It has to be noted that at the time of this writing, no case of a targeted attack on a medical device has been documented outside of security research. But a medical device does not have to be the target of malicious intent. Any device containing COTS is vulnerable to the growing number of malware targeting the respective COTS, and such vulnerabilities can result in infection and operational impact. Also, it has to be noted that even non-networked devices or stand-alone

device networks are at risk due to today's sophisticated malwares' ability to bridge air-gaps via; for example, USB thumb drives.

1.3 Regulatory Perspective

Regulators in all international markets have established requirements and prerequisites for the development, manufacture, release for sale, and use of medical devices in their respective countries. Although these regulations are harmonized to a certain extent, regional differences remain, and manufacturers need to be cognizant of the local requirements for validation, release, and sale of their products.

The US Food and Drug Administration (FDA) is currently leading the regulatory community in considering patient safety risks due to medical device security vulnerabilities. FDA's January 2005 "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software" explained some of FDA's rules for manufacturers of medical devices that use OTS software and connect to networks.[1]

FDA's Oct. 2014 "Guidance for the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" has focused on cybersecurity requirements for medical devices and its impact on device development, documentation, deployment, and lifecycle management.[2]

Even before cybersecurity became an issue, the FDA had established a medical device approval and classification regulatory framework based on the intended use of the device, the risks associated with the device, and the type and level of controls necessary to assure the safety and effectiveness of the device. These regulations have, in summary, the following impact on the device's cybersecurity posture:

- To assure continued safe and effective operation of their medical devices, manufacturers are required to properly validate and document cybersecurity updates prior to release for use in their specific device. As a result, the HDO must wait to install patches, security updates, or third party security software until after validation and approval by the medical device manufacturer. Although there may be exceptions, e.g., medical devices which are pure software products running on a standard computing platform that may not be considered part of the regulated device. Prior to installing any updates or additional software components the HDO should always confirm with the manufacturer whether any regulatory or other restrictions exist.
- The formal validation and release process is typically longer for medical devices compared to non-regulated IT systems. . As a result the time to release of medical device

[1] "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software", 14 January 2005, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

[2] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff", 01 Oct. 2014 URL: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

security updates and patches is typically longer for medical devices compared to non-regulated IT systems.

- Typically, it is the device manufacturer's responsibility to articulate the urgency of a patch and make recommendations on its timing and deployment. However, depending on the support relationship between manufacturer and HDO and depending on the device's architecture and use case, impact analysis the deployment and installation of the update can be controlled by the HDO. In most cases, this relationship is established with a formal contractual agreement.
- COTS patches only require resubmission to the FDA in the exceptional case where they would change the device's features or use. Validation is required, but in most cases, no resubmission or re-approval is required.
- In addition, it remains to be seen when and to what extent the FDA's recent "Guidance for Industry" will lead to new requirements for premarket submissions or new regulations with the goal to reduce the risk to patients due to a cybersecurity incident.
- It has been documented that European regulators are watching the current development in the US and specifically the FDA's approach and decision process very closely as they are also recognizing the risk of cyber threats to medical devices.[3]

1.4 Healthcare Delivery Organization Perspective

As a result of the regulatory status discussed above, healthcare organizations will rarely be in a position to decide on their own whether to patch a medical device. It has to be assumed that in most cases they do not have the detailed knowledge to assess a patch's impact on the medical device's safety and effectiveness.

There may be a few regulatory exceptions (e.g., a medical device may be a specific software product, and may not include the workstation or operating system it runs on), but healthcare organizations also need to bear in mind the impact on support, as a change not approved by the manufacturer may violate contract or warranty agreements and the healthcare organization may incur significant liabilities with regards to risks to patient safety.

Patch updates for COTS are recognized as a safety issue and may be provided at no cost to the HDO. Additionally the manufacturer must evaluate and certify patches for all COTS provided with the original equipment at time of purchase or provided during the product's lifecycle support.

In light of the above, the most practical approach for healthcare organizations would be to cooperate with the vendor by:

- Communicating security concerns to the manufacturer;
- Receiving timely communication on patches and security updates and being informed about their criticality;

[3] "Cyber security and health technologies", European Public Health Alliance (EPHA) Briefing Paper, updated May 2013

- Deploying manufacturer-approved patches in a timely and efficient manner;
- Educating staff on cybersecurity issues and risks; and
- Creating a cooperative environment between IT Personnel, Privacy and Security Officers, and Biomedical Engineers.

1.5 Solution Approach

With increasing urgency to address patch management and the anticipated tighter regulatory scrutiny and market pressure, this document will discuss patch management and complementary solutions. In summary:

- Improve manufacturer patch release process based on criticality and resulting risk and in line with the manufacturer's quality system processes.
- Introduce a formal change management process:
  - End-user impact analysis;
  - Rigorous and timely patch deployment by the HDO.
- Discuss communication between all stakeholders:
  - Manufacturer and HDO on patch availability, criticality, and implementation;
  - HDO Biomedical Engineering and IT departments on security strategy, responsibilities, and implementation;
  - Information of cybersecurity incidents to local regulating agencies (e.g., the US FDA)
  - Information about breach of Protected Health Information (PHI) to local authorities (e.g., US Health and Human Services (HHS) Office of Civil Rights (OCR)).
- Use of supplementary technologies to address the gap between vulnerability discovery and patch deployment:
  - Host Intrusion Prevention System (HIPS) software on the medical device itself (as appropriate for the device's architecture and platform);
  - COTS hardening based on software suppliers guidelines or public resources;
  - For more complex COTS components, like the operating system, remove all unused components to eliminate the associated vulnerabilities, e.g., media players, email, or native web browsers;
  - Network segmentation to reduce exposure resulting from vulnerabilities and to contain malware outbreaks (although network segmentation comes with a certain overhead and increased complexity);
  - Where practical, use of external security technologies, e.g., firewalls;
  - Security-conscious device handling and lifecycle management policies and procedures;
  - Staff cybersecurity education.

Patching is a critical part of a good security program, although it always has to go hand in hand with other security measures. However, medical devices are unique because:

- Compromises of medical devices have potential for patient harm.
- Many devices have 24x7 operational requirements and interruption can have both operational and safety implications.
- Medical device development, test, manufacture, and maintenance are heavily regulated.
- Medical device COTS tend to lag in patch level and cybersecurity protection.
- Implementing and maintaining security measures, including patching, is complex and requires coordination across stakeholders.
- COTS lifecycle and end of support (EOS) may be shorter than that of the actual medical device and need to be supported/replaced for a reasonable lifecycle based support model of the medical device.
- To minimize system vulnerability, manufacturers should remove all COTS components and functions not necessary to provide clinical function or support of the medical device and should follow general industry best practices as applicable to the respective COTS component.

This document will discuss the regulatory background, implications on manufacturers and HDOs, and elements of a solutions path forward.

2 Introduction

Medical devices have a unique function of providing patient care, and their reliability has direct impact on patient safety. Increasingly, these devices are being connected to the enterprise network to enhance functionality through integration and improve efficiency through automation. Regulatory agencies require products to be verified and validated to assure safety and effectiveness prior to market release. This formal release process must be balanced with the requirement to provide timely updates and patches, including updates to address cybersecurity vulnerabilities. The medical device may use COTS for the operating system, database, runtime environment, or the like. Figure 1 summarizes some of the most common medical device risk and impact scenarios.

Although patching should not be the only security measure in the hardening process, it is essential. Regularly applied in the traditional IT environment, workstations or servers typically get patched to minimize exposure to cyber risks. But with medical devices, regulations mandate a formal and structured release process, often resulting in a weakened security posture through delayed availability and implementation of security patches. There is always a balance to be maintained between properly maintaining device availability and safety versus timely update of a weakened security posture.

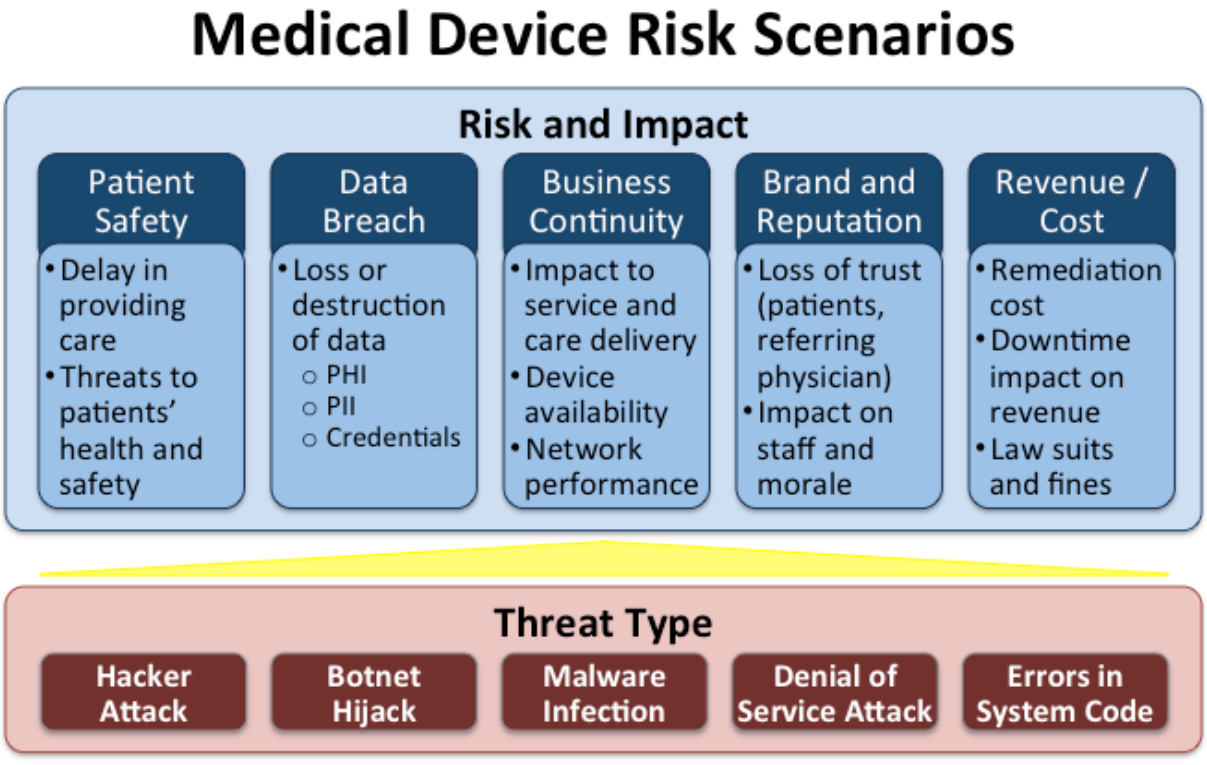


Figure 1: Example Threats and Risks for Networked Medical Devices

Risk management, which encompasses change management and cybersecurity, must be balanced with the intended use and the patient care provided by the device. Security measures, like patching, need to be included in the regulated, formal release process of the product and need to integrate with the customer and patient environment. Medical devices have specific requirements for safe and effective use, which may conflict with IT and Cybersecurity Best Practices. It is this balance between medical device reliability and IT Security that is challenging for all constituencies: HDOs, Medical Device Manufacturers, and Regulators.

Medical devices that store, process and transmit patients' medical information are increasingly controlled by software and are capable of connecting to hospital networks using both wired and wireless communications technology. With this increase in connectivity comes the benefit of greater access, functionality, and management of these devices, which allows for more efficient provision of care and better patient outcomes.

By allowing medical devices to connect to hospital networks and by allowing device manufacturers maintenance access via the Internet, HDOs expose those devices to the same cybersecurity risks that exist for standard IT assets, yet these devices are typically more vulnerable due to their lack of patching or added cybersecurity measures. This results in both, patient safety concerns as well as HIPAA risks to information confidentiality, integrity and availability as it can cause devices to malfunction, lead to operational downtime, impact patient care, or expose Protected Health Information (PHI). The increase in connected medical devices has brought significant complexity to securing and defending devices against cyber attacks without compromising patient care and staying compliant with federal regulations.

3 Challenges & Risks

In order to understand why patch management is important, we must first understand the threat vectors and how they can impact devices. Patching, especially of commercial off-the-shelf COTS software components, such as the operating system, is one of the key components of a mature cybersecurity program and helps to protect a device from cyber threats and software-related vulnerabilities.

3.1 Introductory Example: Malware

Malware is malicious software that can infect computer-based devices, including medical devices. Today's sophisticated malware has the ability to proliferate and spread rapidly through networks, shared folders, portable media, etc. Malware can broadly be categorized in the following main types: Virus, Trojan, Worm, Backdoor, Rootkit, Spyware, and Botnet. In fact, today's malware may combine the characteristics of several of the traditional types and often has the capability to upgrade itself or download additional malware based on instructions received from a remote Command and Control server.

Typically, malware exploits known vulnerabilities in COTS (OS, middleware) so patching helps to close those vulnerabilities. Additional and complementary best practice defenses include system hardening (e.g., close unused ports), intrusion prevention software (e.g., control processes and configuration); and anti-malware tools (e.g., signature- or behavior-based technologies).

3.2 Example Malware Scenario: Conficker

Conficker (also named Downup, Downadup, or Kido) is a computer worm, i.e., malware that can self-replicate. It targets the Microsoft Windows operating system (Windows XP and earlier). On infected systems, Conficker may compromise administrator passwords, may install further malware, or form a botnet based on instructions received from a command-and-control server. It initially appeared in November 2008 and rapidly spread to over 200 countries, infecting millions of computers and making it one of the largest outbreaks of its time.

Conficker's unique characteristic makes it a specific problem for medical devices and makes it challenging to remediate. It is difficult to counter as it uses several advanced malware techniques. Over time, at least five main variants (Conficker A-E) evolved, each being more sophisticated in its propagation method and ability to defend itself against detection and removal. As a worm, once an initial system is infected, it has the ability to self-replicate and propagate.

The initial version of Conficker spread via the Internet, but a second variant (Dec. 2008) could propagate via LAN, shared folders, mapped drives, peer-to-peer networking, and portable media. Some versions exploit the AutoRun feature to infect a device via removable media, e.g., a USB flash drive. Once a system is infected, Conficker upgrades itself to a newer version or may install other malware. Further, it has the ability to hide in a system and defend itself from removal by encrypting its payload or by disabling system services, like automatic update, see Figure 2.

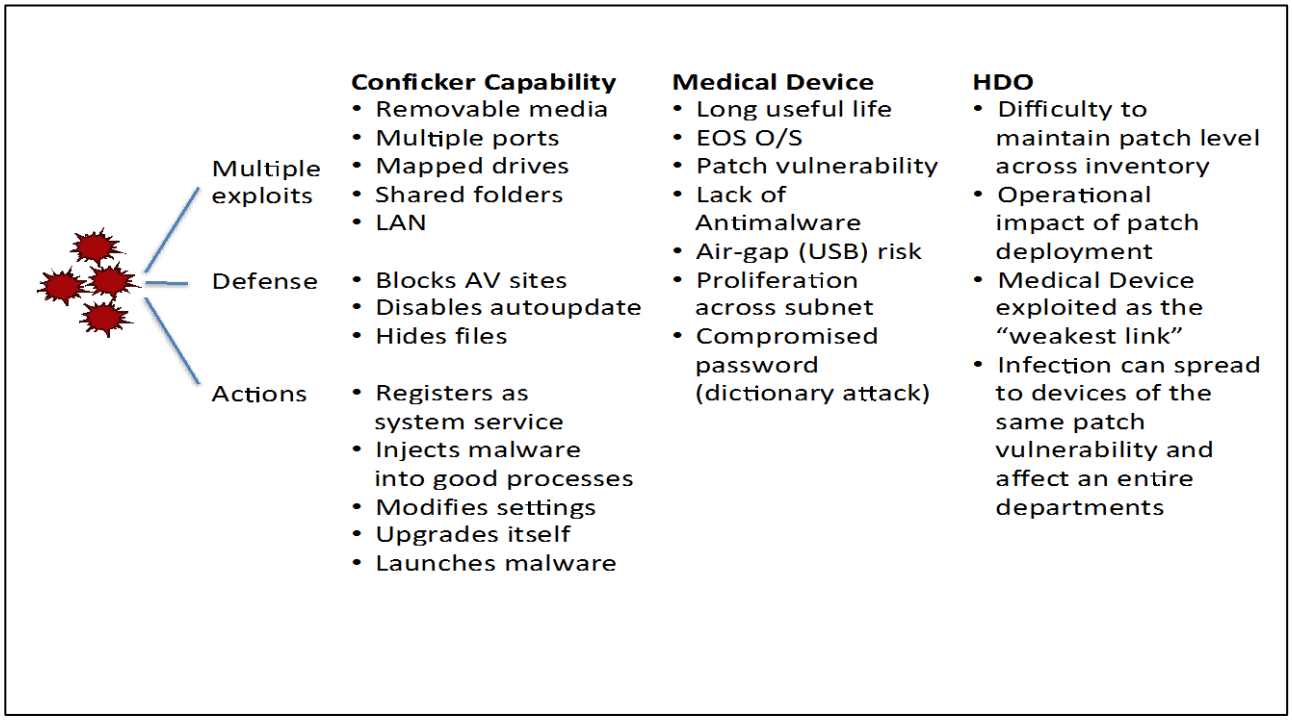


Figure 2: Conficker Capability / Device Vulnerability / HDO Impact

Microsoft has issued patches for Conficker variants since late 2008 and corporate networks have generally been upgraded and protected. However, due to the sophistication of some of the newer variants, Conficker infections continue to reoccur. Commercial anti-malware products with up-to-date signature files typically provide protection against infection. Other supplementary security measures like firewalls, network IPS protection, and device control measures (e.g., disable AutoRun) are also recommended.

Conficker has been reported to be a prevalent and ongoing problem for medical device networks. Medical devices have a long useful life and many of the targeted operating systems are no longer in production but still in use and/or behind in patch level, leaving the underlying Windows vulnerability exposed. In addition, many devices on a medical device network are of the same patch level, allowing the worm to spread to devices with the same vulnerability, especially since most do not have supplementary security products installed, such as commercial anti-malware or HIPS (host intrusion prevention system) software.

Medical device networks may have reasonable perimeter protection, but inside the organization the individual devices remain vulnerable and are susceptible to infection via USB drive across the, so-called, air-gap attack. Once a device is infected, the malware can quickly spread within the medical device subnet. Further, for easy maintenance and access, many medical devices use simple default administrator passwords, which can be compromised by the Conficker malware through a dictionary attack.

This analysis using Conficker demonstrates the importance of patching medical device networks. A mature patch process should include a patch release from the device manufacturer,

communication of patch availability and criticality to the healthcare organization, and timely installation of the patch to all affected devices on site.

4 Understanding the Regulatory Baseline

Regulators in all international markets have established requirements and prerequisites for the sale and operation of medical devices in their respective countries. Although these regulations are harmonized to a certain extent, regional differences remain and manufacturers need to be cognizant of the local requirements for verification, validation, release, and sale of their products. For most manufacturers, the U.S. Food and Drug Administration (FDA) and its Quality System Regulation are the most relevant. Therefore the following sections will use the FDA regulation as the leading example.

In the U.S., the FDA has established a medical device approval and classification system based on the intended use of the device, the risks associated with the device, and "the level of control necessary to assure the safety and effectiveness of the device."[4] Devices are classified into one of three categories:

- Class I (low to moderate risk): General Controls
- Class II (moderate to high risk): General Controls and Special Controls
- Class III (high risk): General Controls and Premarket Approval (PMA)

4.1 FDA General Regulatory Controls

General Controls are the basic provisions of the May 28, 1976 Medical Device Amendments to the Food, Drug and Cosmetic Act that provide the FDA with the means of regulating devices to ensure their safety and effectiveness. They include provisions that relate to adulteration; misbranding; device registration and listing; premarket notification; banned devices; notification, including repair, replacement, or refund; records and reports; restricted devices; and Good Manufacturing Practices. As device class increases from Class I to Class II to Class III, the regulatory controls also increase. General controls are the most basic level of control and apply to all medical devices regardless of their classification status, unless exempted by regulations.

The Good Manufacturing Practices requirement specifically refers to the Quality System Regulation, defining the methods used in, and the facilities and controls used for, the manufacturing, packing, storage, and installation of a device. This is to ensure that manufacturers' products consistently meet applicable requirements and specifications. Because the regulation must apply to so many different types of devices, the regulation does not prescribe in detail how a manufacturer must produce a specific device. Rather, the regulation provides the framework that all manufacturers must follow by requiring that manufacturers develop and follow procedures and fill in the details that are appropriate to a given device according to the current state-of-the-art manufacturing for that specific device.[5]

---

[4] "Classify Your Medical Device", U.S. Food and Drug Administration, 2012, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/

[5] "General Controls for Medical Devices ", U.S. Food and Drug Administration, 2014, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/ucm055910.htm

4.1.1 General Controls: Premarket Notification (AKA 510(k))

The 510(k) submission identifies characteristics of the new or modified medical device as compared to an existing medical device with similar intended use, legally distributed within the United States. A manufacturer cannot commercially distribute a device that requires the submission of Premarket Notification 510(k) until it receives a letter of substantial equivalence from FDA authorizing it to do so. The current legally marketed device is referred to as the "predicate" device[6].

Many Class I and some Class II devices are exempt from Premarket Notification, and a list of exempt device types is provided by the FDA.[7]

4.2 FDA Special Regulatory Controls

Special controls are regulatory requirements for Class II devices. FDA defines Class II devices as those devices for which general controls alone are insufficient to provide reasonable assurance of the safety and effectiveness of the device, and for which there is sufficient information to establish special controls to provide such assurance.

Special controls are usually device-specific and include: Performance standards, post-market surveillance, patient registries, special labeling requirements, premarket data requirements, and other guidelines.[8]

4.3 FDA Premarket Approval (PMA)

A PMA is required for FDA Approval of Class III devices that pose a significant risk of illness or injury, or devices that are not found to be substantially equivalent to any Class I or II predicates through the 510(k) process. An approved PMA is, in effect, a private license granting the applicant (or owner) permission to market the device. Section 515(c)(1) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) specifies the required contents of a PMA.

4.4 FDA Position on Cybersecurity Patching

The FDA has been consistent in its position on patching for the past decade. Since 2005, FDA has released four documents that address cybersecurity in medical devices:

- "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" released on May 11, 2005.
- A Safety Communication titled "Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility" which was released on November 4, 2009.

---

[6] "Premarket Notification 510(k)", U.S. Food and Drug Administration, 2014, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm

[7] "Medical Device Exemptions 510(k) and GMP Requirements", U.S. Food and Drug Administration, 2014, URL: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/315.cfm

[8] "Regulatory Controls ", U.S. Food and Drug Administration, 2014, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/ucm2005378.htm#top

- More recently, FDA released another Safety Communication "Cybersecurity for Medical Devices and Hospital Networks" on June 13, 2013.
- Lastly we received the FDA's Oct. 2014 "Guidance for the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" with focus on cybersecurity requirements for medical devices and its impact on device development, documentation, deployment, and lifecycle management.

In all of these documents, FDA has consistently taken the position that:

1. FDA's Quality System Regulation requires medical device manufacturers to correct or prevent quality problems. This is generally interpreted to include cybersecurity related patches.
2. Medical device manufacturers and healthcare providers should work collaboratively to address cybersecurity issues in a timely manner.
3. FDA does not typically need to review or approve medical device software changes made for cybersecurity reasons if the software change does not impact performance features or functionality of the device.
4. Medical device manufacturers should validate all software changes that address cybersecurity before installation to ensure that they do not affect the safety and effectiveness of the medical device.

An FDA software compliance expert, John F. Murray, summed it up this way:

> *"The rules are basically still the same for cybersecurity patches as they are for other changes. One is if it does not change the intended use of a device, there's no requirement for pre-market submission. Two is that it doesn't introduce any new elements of risk. Our opinion is that we can't think of a case where a cybersecurity patch would represent a change of intended use or the introduction of new risk. In fact we believe that this is a decrease of risk. Although we don't absolutely say 100% of the time that this could be true. We really believe that it's unlikely that a software patch for cybersecurity would require pre-market approval."* [9]

4.5 Risk and Hazard Analysis

The individual devices as well as the integrated network of devise are complex and tightly regulated, requiring a risk or hazard analysis based approach. For the manufacturer this falls under ISO 14971 "Medical devices -- Application of risk management to medical devices" and for the HDO this falls under Joint Commission EC.02.04.01, requiring that "the hospital manages medical equipment risks." However, these analyses do not address the risks associated with a network of medical devices and supporting components. In such a network, the vulnerabilities of one device or component form a risk to the entire system. Conversely, the larger system's vulnerabilities can be a risk to the individual device.

[9] "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software", Murray, 2005, URL: http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ucm127816.htm

These network problems are commonly referred to as the "system of systems" problem and span all aspects of system integration, from communication protocols, reliability, performance, to cybersecurity. To specifically address these risks, a relatively new series of standards – ISO/IEC 80001 "Application of risk management for IT-networks incorporating medical devices" -- has been developed and is recommended as a best practices framework. Although not mandated or binding, IEC 80001 does provide a comprehensive approach to manage the unique risks of medical device networks, including non-medical components like routers, firewalls, workstations, and servers.

4.6 International regulations

It appears that, at the time of this writing, the main regulatory driver for medical device cybersecurity is the U.S. Food and Drug Administration. Other regional regulatory bodies are not providing specific guidance with regards to medical device cybersecurity, and specifically patching. In fact, several international regulators are currently looking at the evolving guidance by the FDA as input to their decision making process.

The general requirement to assure safe operation of medical device, which would include protection from cyber threats and maintaining privacy of any data stored on or transmitted by the device, is a requirement found in existing healthcare and data privacy regulatory frameworks, with several of the respective regulations currently under discussion for future revision.

Regulations that may not be specific to medical device cybersecurity, but are to be considered as general, overarching requirements in the design, testing, approval, and sale of medical devices in the respective regions are for example:

- The general safety and security rules applicable to medical devices as well as the supporting regulatory processes equally apply to any software used as an integral part of, in combination with, or as an extension of a medical device. Any medical device needs to undergo verification and certification to obtain regional approval, for example the "CE" marking for the European market.[10] Any software that comes with a medical device is verified and certified together with the device itself, and any standalone software meant to be used for medical purposes is considered as a medical device in its own right, i.e., it is in itself subject to the same regulations and processes.[11]
- Under these regulations, the verification and certification process is supposed to assure that the device/software is state of the art, meets the essential requirements of performance, safety and security applicable to its product class and risk category, and complies with any applicable industry standards, for example the US/EU harmonized standard IEC 62304, Medical device software—Software life cycle processes. Once a product is on the market, it is subject to continuous monitoring. The manufacturer should address any new elements, circumstances, or risks affecting performance, safety or

[10] "Council Directive 93/42/EEC of 14 June 1993 concerning medical devices", URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:EN:PDF

[11] "Guidance MEDDEVs", URL: http://ec.europa.eu/growth/sectors/medical-devices/guidance/index_en.htm

security and should be addressing these in a timely manner. For software, this typically means vulnerability patches, compatibility upgrades, and bug fixes.

- Since the data generated, processed, transmitted and stored by medical devices typically classifies as sensitive personal data, it is therefore subject to the same stringent data security requirements applicable to such data under EU law. The current rules require "appropriate technical and organizational measures" to secure all personal data, at rest or in transit, from loss, destruction or any other form of compromise.[12]

Further, specific ongoing discussions and regulatory projects may result in future changes, for example:

- New legislation under way in Europe is building on the existing regulations, which have been in place since the 1990's, but aim to overcome some of the current regulations' limitations and accounting for technological and scientific progress, and reducing divergences in the interpretation and application of those rules. This is to assure the safety of medical devices and enable their free movement within the internal EU market. Although this new proposed regulation addresses regulatory gaps or uncertainties with regard to certain product types, it does not explicitly address the area of cybersecurity and its possible effect on patient safety.[13]

- The European Commission's ongoing project to unify data protection within the European Union (EU) under a single law, the General Data Protection Regulation (GDPR), with the goal to update and improve the current EU Data Protection Directive 95/46/EC to consider important aspects like globalization and technological developments like social networks and cloud computing. A proposal was released on 25 January 2012, with numerous amendments proposed since. Adoption is planned for late 2014 with a planned effective date after a transition period of 2 years.

- New rules are currently being drafted in Europe on the protection of personal data, which will perhaps add some further details to this generic requirement, by spelling out desirable outcomes such as confidentiality, availability, integrity and authenticity, as well as process elements around data security such as regular audits, personnel training and access control.

- The EU is also currently drafting new legislation on critical information infrastructure security, across all critical industries and including the healthcare sector. While none of these rules will apply to individual devices, hospitals and other health organizations will have to look to the cybersecurity of the communication infrastructure interconnecting their thousands of devices.

---

[12] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Strasbourg, 28.I.1981, URL: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[13] "Proposal for a Regulation of the European Parliament and of the Council on Medical Devices", URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0542:FIN:EN:PDF

5 Patch Management Challenges – Stakeholder Perspective

A common goal for both the manufacturer and the HDO is patient safety. To ensure the safe and effective use of their device the FDA has regulated the manufacturer via its Quality System Regulation. Historically the manufacturer ensured compliance by creating proprietary and physically and logically isolated products. Based on technology evolution, customer needs and requirements, the medical devices have moved into the IT mainstream by being networked and using Commercial-off-the-Shelf (COTS) components. This has changed the burden of securing the medical devices from the manufacturer alone to include the HDO and from securing the device by itself to securing it as part of a larger system (often referred to as "defense in depth"). Because COTS components have the unique risk of being exploited by a growing number of threats, they also require unique and specific consideration and chain of control from the COTS manufacturer to the end user of the device.

The manufacturer – HDO relationship is evolving into a partnership and close coordination of processes and technical decisions is of critical importance. The proliferation of connectivity and the increasing pace of malware development dictate a sense of urgency.

5.1 Manufacturers

The medical device manufacturer must consider the HDO's needs for management of the medical device's life cycle. It is very common for HDOs to use medical devices much longer than typical IT systems; for example, it is common for medical devices to be used for 10 years or more. This is a significant challenge for both the HDO and the manufacturer since the medical device's useful life often exceeds the support for the COTS Operating System or other commercial software, especially when considering security patches.

A common complaint from HDOs is that a manufacturer may hide behind the FDA when questioned on cybersecurity and delay release of patches because it is an FDA-regulated device. However, the FDA guidance is clear. Software security patches should be released in a timely manner and typically do not require resubmission to or re-approval by the FDA.[14] But any software changes that could impact the ability of the device to operate in a safe and effective manner need to be tested and approved by the manufacturer.

In case of a cybersecurity event with a medical device, the first priority is patient safety. All medical devices must include a built in fail safe mechanism and notifications to the intended user that a device or system failure is occurring. The user impact when a device fails can be significant. The best practice to restore a compromised device is to re-install the operating system environment, the application and all pertinent configuration data. This ensures the device integrity and patient safety.

[14] "Cybersecurity for Networked Medical Devices is a Shared Responsibility: FDA Safety Reminder", U.S. Food and Drug Administration, 2009, URL: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm

5.2 Healthcare Delivery Organization (HDO)

While most HDOs are able to protect and reliably manage IT assets, medical devices pose a very different challenge. Securely managing medical devices requires a very different approach over managing traditional IT assets such as servers, workstations and network gear. Medical devices offer the following challenges:

- The life of a medical device may exceed 10 years, where most IT managed assets have a life expectancy of 3-5 years.
- Due to FDA regulation, the HDO cannot install any software or components on the medical device that have not been validated and approved by the manufacturer. This includes, for example, anti-malware tools, intrusion detection/prevention, encryption, agents to support asset management, and software patches. This may be further enforced through contracts and warranty conditions and as a result, any change to the device without manufacturer approval can create substantial liability for the HDO. Further, the HDO typically does not understand functional, safety, or regulatory implications of any decisions regarding add-on software components.
- The complex logistics of patch distribution and installation on devices that may be in 24x7x365 operation.
- HDO Resources required to test and deploy patches.
- Organizational separation between healthcare IT and Biomed / Clinical Technologies department and responsibilities. Medical Device functional support is the domain of biomedical engineering while cybersecurity is the domain of IT. Manufacturer support agreements often span both aspects and clinical leaders are often responsible for access control. Unclear and inconsistent support matrix increases uncertainty of responsibility.

6 Other Regulatory Aspects

6.1 Regulatory Restrictions on Use of Third Party Software Agents

Indirectly related to the regulatory approval process are third party software agents and tools. IT Asset Management or similar systems may deploy such agents in order to provide more granular control of the IT asset itself.

In case of the asset in question being a medical device, the deployment of such agents typically falls under the same restrictions as stipulated by the FDA regulation and as discussed before; i.e., such agents should not be deployed without having undergone manufacturer testing or having received manufacturer approval.

The challenge many manufacturers face is to determine which are the common and appropriate management systems and agents. It is difficult to select which management systems and agents are commonly used by their customers and should be validated

Third party software agents placed on IT assets are typically deployed as part of:

- An IT Asset Management or CMDB (Configuration Management Database) System for the purpose of asset discovery and management of assets according to a corporate IT standard;
- Other maintenance and management systems as they may be deployed in and for the purpose of Biomedical Engineering or Operational management.
- Patch management systems to deploy patches and manage updates (may be included in above).
- IT Security Management Systems, which may automatically deploy anti-malware software and updates to virus definition files.

6.1.1 HDO Considerations

When utilizing any automated asset management system in a Medical Device environment, the following typically needs to be restricted and tightly controlled:

- Push deployment of agents to devices for which the respective agent has received manufacturer approval.
- Configuration of devices must be in line with manufacturer-approved configuration.
- Automatic deployment of operating system (or other COTS component) patches must be in line with the manufacturer-approved version of software.
- As a result, the patch process for medical devices, as compared to standard IT equipment, must be tightly controlled and may even need to be managed and executed separately.

There have been documented cases where IT Management Systems did a system-wide push of operating system patches, resulting in the interruption of patient exams because of system

messages or reboots.[15] Additionally, some of the devices that accepted the patch were now out of compliance relative to the manufacturer-approved configuration. The impact can vary from a regulatory violation with potential legal consequences over interruption of exams or treatment, to potential impact on patient safety.

6.2 Understanding the Latest (Oct. 2014) FDA Guidance Document

In Oct. 2014 the FDA issued guidance for manufacturers[16] on the risks of cybersecurity and their responsibility to provide a reliable and secure infrastructure. This communication explains issues such as unauthorized device access, component exploitation, and incident response and recovery. While the recent communication reiterates the three primary points of FDA's historical stance on patching, it also represents a change in thinking at the FDA and indicates a possible future emphasis on cybersecurity in the device approval process.

[15] "Birth monitor demands Windows restart as mom begins to push", URL: http://www.geek.com/geek-cetera/birth-monitor-demands-windows-restart-as-mom-begins-to-push-1342039/

[16] "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication", U.S. Food and Drug Administration, 2013, URL: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm?source=govdelivery

Key Guidance for Manufacturers
• **Develop a set of security controls to assure medical device cybersecurity to maintain confidentiality, integrity and availability.** • **Manufacturers should consider cybersecurity during the design phase, as this can result in more robust and efficient mitigation of cybersecurity risks.** • **Manufacturers should define and document components of their cybersecurity risk analysis and management plan as part of the risk analysis.**
Security Capabilities
• **Security controls will depend on the medical device type and use, probability of risks, and potential impact on patients. Devices capable of connecting to other devices, networks, or to portable media (**e.g., **USB or CD) are more vulnerable to cybersecurity threats.** • **Providing justification in the premarket submission for the security features chosen and consider appropriate security control methods for their medical devices including, but not limited to, the following:** o **Limit Access to Trusted Users Only: User authentication, timed user sessions, role-based authorization, avoid "hardcoded" passwords, minimize risk of tampering, and controlled software or firmware updates.** o **Ensure Trusted Content: Restrict software or firmware updates to authenticated code, implement version control, secure data transfer** o **Use Fail Safe and Recovery Features: Implement fail-safe device features, protect critical functionality, allow for security compromises to be recognized, provide methods for retention and recovery of device configuration**
Cybersecurity Documentation
• **Recommended documentation to provide with the device's premarket submission and in accordance with the Quality System Regulation, including Design Controls.** • **Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated, including:** o **List of all cybersecurity risks that were considered.** o **List and justification for cybersecurity controls for the device.** • **Traceability matrix linking cybersecurity controls to cybersecurity risks.** • **Plans for providing updates and patches to operating systems or device software.** • **Demonstrating that the device will be provided to purchasers free of malware.** • **Instructions related to recommended anti-virus software and/or firewall use appropriate for the environment of use.**

6.2.1 Confusion Surrounding Circumstances that Require Resubmission of Premarket Review

In addition to the requirement of a review before a device is brought to market, there are two other conditions that require submission of a 510(k) or PMA. A new submission "is required for changes or modifications to an existing device where the modifications could significantly affect the safety or effectiveness of the device, or the device is to be marketed for a new or different indication for use".[17] Some manufacturers and HDOs misinterpret this language from the FDA to mean that security maintenance activities, such as patching or updating antivirus signature files, cross the threshold that requires a new 510(k) or PMA submission.

The confusion surrounding circumstances that require resubmission is a major driver of the difficulties in the patch management workflow for medical devices. Many manufacturers may not patch due to their misinterpretation of this rule. Many HDOs are unsure what responsibilities they have and when or when not to deploy patches. To clarify, the FDA has stated that it does not typically categorize patching as something that requires resubmission of a 510(k) or PMA. Patching will need to be managed under the manufacturer's quality system processes and will have to undergo formal verification and validation prior to release to the HDO.

[17] "Premarket Notification 510(k)", U.S. Food and Drug Administration, 2014, URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm

7 The Medical Device Patch Process

7.1 Manufacturer

Medical Device Manufacturers support their device life cycle with formal processes in line with FDA regulations (and/or other applicable regional authority). Historically, security patches were included with each release and were typically provided as a cumulative package since the last release. If the patches do not affect or change the intended use of the device, there is no requirement for notification or filing with the primary regulator (e.g., FDA). There is, however, a requirement for the manufacturer to test and validate the change to assure no adverse impact on the device.

Many manufacturers have adopted the practice of providing major releases (feature enhancements and rolled up patches), minor updates to the application, and fixes addressing specific, limited issues. These may include a set of cumulative COTS patches.

Some manufacturers and HDOs misinterpret this language from the FDA to mean that security maintenance activities, such as patching or updating antivirus signature files, require a new 510(k) or PMA submission. The quality system and patch process, whether it is an upgrade, update or fix, typically follow the same steps: Testing, Verification and Validation process and finally documentation, customer notification and distribution. The testing process duration and timing is dependent on the manufacturer quality system as appropriate for the medical device. Manufacturers are required to have a customer notification process. Delivery options for the patches range from a manufactured patch, which is deployable (executable), to a notification that is published, indicating the patches have been tested and released. Customers can then deploy the patches following the manufacturer recommendations.

To assure only authenticated software (including upgrades, updates, patches and fixes) are being installed, manufacturers may utilize what is known as code signing process, which digitally signs the software with a cryptographic hash or checksum. Code signing assures that the software is not altered and that its security posture is maintained, as well as to maintain compatibility and reliability. It also assures only licensed users install the software.

7.1.1 Time to Validate Patches / Cost of Release

Historically, manufacturers used their release or revision cycle to include software patches and updates, including security. The manufacturer's quality system, a required component of FDA regulation developed to ensure product and patient safety, was developed to support this model of distribution of updates and patches. This model worked for both the HDO and the manufacturer until the security environment changed and more frequent patching was required. The manufacturer’s quality system and processes are challenged today to keep pace with the required release frequency (monthly or even weekly).

Manufacturer quality systems are required to test and verify any change that may impact the intended use and the safe and effective use of the device. These requirements do impact the ability of the manufacturer provide security patches at sufficiently frequent intervals. Operationally impacting a medical device can have impact on multiple levels, be it financial or patient safety.

Noted medical device researcher, Kevin Fu, sums it up well:

> *"Regression testing, validation, and other good manufacturing practices are non-trivial. It can take a lot of work to perform testing. The last thing a manufacturer wants to do is accidentally brick a medical device with an errant update. How do you automatically validate things that connect to non-deterministic patients? Moreover, how do you perform testing on a component that will interoperate with other unknown components from different manufacturers?"*[18]

The following table summarizes the key aspects of patch release and management:

DOs	DON'Ts
1. DO patch in a timely manner based on criticality 2. DO obtain manufacturer approval 3. DO validate before deploying 4. DO know your inventory (type, configuration, location, use, etc.)	1. DON'T push out patches without considering device type (e.g., IT vs. Medical Device) and current utilization (patient care impact) 2. DON'T unnecessarily delay the deployment of patches.

7.1.2 General Lifecycle Management Challenges

The device manufacturer typically releases new revisions of software and systems every 18-24 months, with minor updates and fixes more frequently. These releases may include new operating systems, service packs, security patches, new application features and application updates. With any system using COTS components, this process needs to be carefully planned for and aligned with the COTS components' lifecycle.

A common conflict is that the medical device's useful life and expected support may exceed the life expectancy of many COTS components. Further, in this day and age, COTS security patches are being released so frequently that many medical device manufacturers are challenged to test and validate them and to provide timely releases. Even if the manufacturer no longer supports a device or release, the HDO can still enter a complaint. The complaint may prompt the manufacturer service organization to provide discounted service or fix, or the HDO may use the complaint as leverage for a purchase discount.

7.1.3 Software Certification and Code Signing

In order to assure that software or firmware installed on medical devices is authentic and an approved version, manufacturers may deploy software certification or code signing technologies.

[18] "False: FDA Does not Allow Software Security Patches", Kevin Fu, Secure-medicine.org, Oct. 17, 2012, URL: http://blog.secure-medicine.org/2012/10/false-fda-does-not-allow-software.html

Code signing can assure that:

- The manufacturer authorizes the installation of the respective software.
- The software is technically sound and has been validated and verified to assure safe and effective operation of the device.
- The chances of alteration or corruption of the software (be it intentional or on purpose) is largely reduced.
- Tampering with the device software is prevented and integrity is assured, providing another layer of protection against malware.

Different technologies are utilized depending on device architecture, capabilities, and platform. Typically, code signing requires some form of external certificate service which can be mutually accessed by the manufacturer when the software is “signed” and used for confirmation by the HDO when the software is installed. Ideally, this confirmation should happen automatically in the background and impose no additional workflow steps on the HDO staff.

Software certification can be deployed to the manufacturer's application / proprietary software as well as for COTS components (for which it may be provided as a native feature of the COTS package). Device capabilities or platform may limit to what extent code signing can be implemented.

7.2 HDO Related Concerns

Similar to the manufacturer side, there are significant logistical and practical challenges for an HDO to implement an efficient and up-to-date patch management process. One obvious priority is the communication between manufacturer and HDO so that the latter is alerted to the availability of the upgrade or patch and understands criticality as well as priority and effort required to deploy.

Typically, the number of medical devices to be managed is large, potentially several thousand or ten thousands devices of hundreds of different types and supplied by dozens of different manufacturers. This requires the support of numerous platforms and management of interdependencies between the devices themselves as well as their associated servers and workstations and the respective software packages, databases, etc. running on them.

In addition, the deployment needs to be coordinated with device utilization, clinical care delivery, and business priorities. Simple patches may be deployed relatively quickly, but more complex upgrades may require a coordination of firmware or even hardware upgrades to maintain compatibility and an approved configuration. This may result in device reboot, reconfiguration, or re-testing as appropriate for the task at hand.

Even though the manufacturer has already tested and approved a patch or upgrade, many HDOs have formal processes to approve it in their specific configuration and in a safe test environment. They are able to evaluate the reliability of the entire process, including its delivery method (network, data carrier, etc.), technical and clinical training, documentation, tracking and ticketing, etc.

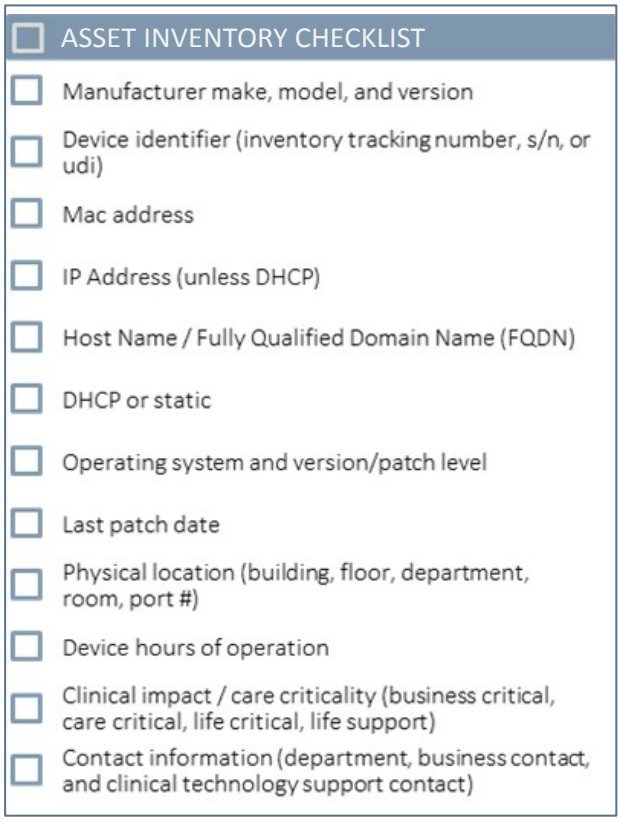
From a business and care delivery perspective HDOs need to be concerned of the impact of the patch process. What, for example, if over the next week I take 10% of one particular device out

of service due to upgrade? To address all of the above complexities and to assure a reliable and rollout with minimal interruption and risk, a careful impact analysis and project and staffing plan may be required.

7.2.1 Asset Management

Whether an HDO utilizes a manual or automated process (with the limitations as discussed before), the basic requirements for proper asset and maintenance management (for example with the help of a Computerized Maintenance Management System (CMMS)), are the same. Important pre-requisites to a mature patch management process include knowing your inventory of clinical technology devices. This includes asset management information and IT metadata.

In reality, HDOs need to find on the one hand the right balance between deploying patches too infrequently (or not at all) and on the other hand the operational and resource impact of providing patches in a highly complex and critical environment where patching requires substantial deployment resources and results in devices not being available while being processed. It is balancing cybersecurity and patient safety against operational priorities that makes it a difficult problem for HDOs to solve.



7.3 Security Measures to support Patching

Due to the complexities of patching, both the healthcare organizations and the manufacturers have to assess if there are any alternatives to patching or address situations where patching is not possible (e.g., end of support) or practical. As discussed, even the most rigorous patch process will deliver patches with a delay and leave a certain vulnerability gap between the time new malware is created and the respective patch is deployed. It is highly recommended that HDOs support the patch process with additional security measures.

7.3.1 System Security Hardening

If a medical device can be secured by disabling unnecessary ports, services and making appropriate configuration changes, the attack footprint becomes much smaller. This hardening of the device significantly reduces the risk of exploitation by an attacker or malware agent. System security hardening may also include implementing least privilege or role-based access control to a system.

There are several guidelines for implementing system hardening. Among them are the Department of Defense Security Technical Implementation Guides (STIG) and the Center for Internet Security Benchmarks (CIS).

7.3.2 Intrusion Detection and Protection Systems

Network Intrusion Detection and Protection Systems (NIDS / NIPS) or Host Based Intrusion Detection and Protection Systems (HIDS / HIPS) can be implemented to detect and even prevent intrusions on the level of the network (NIDS/PS) or the device (HIDS/PS). Implementation on the device level typically falls under the same restrictions of having to be tested and certified by the manufacturer due to FDA regulation. Some HIDS/HIPS solutions in the market are very effective in locking down a system and restricting undesired behavior and therefore may allow a relatively relaxed patch deployment process.

7.3.3 Network Segmentation

Segmenting networks into individual layers does provide a certain level of protection from network-based attacks. However, it does not protect individual devices from media-based attacks. In both cases, segmenting contains an attack or outbreak, and makes it more difficult for these attacks to spread widely. Network segmentation is, in a sense, an additional layer of security and provides a degree of damage control. Network Access Control (NAC) can be used in support of network architecture-based measures.

Technologies utilized to create separate network segments -- e.g., a biomedical network for medical devices, or a department-specific network -- include the creation of Virtual Local Area Networks (VLAN) and the use of properly configured routers and firewalls. Determining how to segment the network, and which devices to place on these network segments, includes an evaluation of security risks of the respective devices, an analysis of the impact of a security event (including financial, operational, and patient safety considerations), and the value of the respective device or group of devices. A good example for this type of assessment and architecture has been provided by the Department of Veterans Affairs.[19]

As patient needs and device technology evolves, cybersecurity measures to protect medical devices need to advance with the industry. Innovated solutions that will enable the following are necessary:

- Ease of management / segregation
- Improved on-device security
- Ability to allow separate management responsibilities from different components
- Easier patch deployment and upgrade process

[19] "Medical Device Isolation Architecture Guide 2009", URL: http://www.himss.org/files/HIMSSorg/content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf

However, it has to be understood that any of the discussed measures may include more or less of a residual risk and decisions need to be made carefully and in the context of the organization's overall security risk analysis and management process.

8 Conclusion

The importance of a timely and well-executed patch process to maintain the device's security posture is vital in preventing compromise of device availability, integrity, and confidentiality and ultimately improving patient safety.

Agencies like the US FDA, FBI, Homeland Security, and US CERT, have issued specific warnings and guidance on cybersecurity for medical devices in recent months. However, regulators such as the FDA mandate that medical device manufacturers produce and sell safe and effective medical devices, which include a formal product development, test, and release process. As a result, product updates including patches are not deployed as frequently as they are in the normal IT environment. As a consequence healthcare delivery organizations (HDOs) have medical devices that are not patched.

FDA has been consistent in their position on patching for nearly a decade. However, some manufacturers and HDOs still misinterpret the language from the FDA to mean that security maintenance activities, such as patching or updating antivirus signature files, require a new 510(k) or PMA submission. That is not true. If the software change does not impact performance features or functionality of the device the FDA does not typically need to review or re-approve the medical device software.

HDOs will rarely be in a position to decide on their own whether to patch a medical device. It has to be assumed that in most cases they do not have the detailed knowledge to assess a patch's impact on the medical device's safety and effectiveness. Therefor software security patches from the manufacturer should be released in a timely manner and typically do not require re-submission to or re-approval by the FDA. COTS patches only require resubmission to the FDA in the exceptional case where they would change the device's features or use; i.e., in most cases re-validation is required, but not re-submission or re-approval.

Due to the complexities of patching, both the healthcare organizations and the manufacturers have to assess if there are any alternatives to patching, or to address situations where patching is not possible (e.g., end of support) or practical. As discussed, even the most rigorous patch process will deliver patches with a delay and leave a certain vulnerability gap between the time new malware is created and the respective patch is deployed. It is highly recommended to support the patch process with additional security measures.

