Integrating the Healthcare Enterprise

IHE Patient Care Device (PCD)
White Paper

Medical Equipment Management (MEM):
Cyber Security

Date: May 27, 2011
Author: PCD Technical Committee
Email: pcd@ihe.net

Contents

1 Objective

This document addresses the problem of increasing risk of cyber attacks, targeted or not, on medical devices, specifically the risks of malware outbreaks and breaches of Protected Health Information (PHI). The unique regulatory status, general use scenario, and patient care aspects make medical devices difficult to protect and manage. The following will review the problem and provide guidance on a risk management based approach to solving it.

This document will not be addressing the general requirements around security, safety, or accuracy of patient information or medical device operation within interconnected / interoperable healthcare network. It is focused on providing an overview and primer on the risks and mitigation strategies associated specifically with cyber attacks as a result of illegal and intentional activity. The broader medical device considerations involving, amongst others, security, accuracy, reliability, legal, staffing, training, outsourcing, network standards, equipment nomenclatures, ethical, and privacy issues are outside of the scope of this document.

Further, the main focus of this document is on network-connected medical devices. Many implantable devices have some similar risk factors, but due to the way they are accessed and the risk to the patient, they add their own specific aspects to the problem. They are a unique type of equipment and require unique considerations, which are beyond the scope of this document.

2 IHE Role

IHE PCD (Patient Care Device) Domain is concerned with enabling interoperable communications of regulated patient-centric point of care medical devices. With these new capabilities there is a strong movement for devices to be incorporated into the enterprise data network of healthcare delivery organizations. Unfortunately, many of these devices have not been designed or implemented with cyber security best practices. For IHE-PCD to continue to provide solutions for interoperable communications we need to make sure that the infrastructure is safe and secure. This whitepaper will address device manufacturers as well as clinical end users and educate them about today’s threats and risks. It will provide guidance on how medical devices should be managed and protected in order to minimize their exposure by examining the current state of standards. Lastly it will explore opportunities for IHE to profile these standards to meet the security needs of medical devices.

3 Why is cyber security an issue for medical devices?

Numerous current trends within the healthcare delivery system, but also outside forces, are making the topic of cyber security of medical devices highly relevant.

As economic pressures on healthcare providers are increasing and they need to provide care for more patients with less staff and within budget constraints, the integration of data across the care infrastructure is one obvious opportunity to create efficiencies. Combined with government initiatives to encourage the adoption of electronic record systems, this is leading to an increasing number of medical devices being connected to hospital networks and tightly integrated with administrative and clinical IT systems, like HIS (Hospital Information System) or EMR (Electronic Medical Record).

Further, both, providers and device manufacturers are increasingly utilizing commercial off-the-shelf (OTS) components, like operating systems, and build on open infrastructure standards, like the use of a general Internet Protocol (IP) network.

On the other hand, we are seeing some very concerning trends with regards to what is commonly referred to as the “cyber underground economy”. The motivation of cyber criminals is changing and therefore the threat landscape is evolving at an unprecedented rate. Hacking is turning from “fame to fortune” or from “dorms to dollars” and the production of malware is now largely in the hands of international criminal organizations (Symantec Corp., 2010).

As a consequence, we are seeing:

- The number of new malware and variants is increasing exponentially with literally millions of new pieces of malicious software released every year. In fact, it is estimated that by now (2010) malicious code is exceeding the commercial software being produced.
- Hacking (supported by malware) is changing from a “big bang” splash to a much more stealthy approach where the goal is not to announce ones success of penetrating a system. Rather, the approach is to penetrate unnoticed, infiltrate the larger infrastructure, discover the relevant assets, and capture the most valuable information.
- This has led to a new type of malware which, rather than trying to spread to as many systems as possible, is targeted and very limited in its distribution. The use of automated tools to write viruses is now common, and rather than thousands of viruses targeting millions of systems, we now see millions of viruses but each only targeting a limited number of specific systems, a trend also referred to as “micro distribution”.
- In addition to the abovementioned exponential increase of malware and variants, we are also seeing an increasing sophistication with malware being able to systematically penetrate a security weakness of a particular infrastructure, morph and replicate itself, as well as the ability to receive instructions from the outside.

Unfortunately, we have to assume that these trends will continue and that protecting our personal and commercial IT infrastructure will become a much more complex task. This will be especially a challenge for embedded systems and their unique platforms and given design restrictions. The appearance of the Stuxnet worm (Markoff, 2010) is an indication that highly sophisticated attacks on targeted systems is indeed a reality we need to live with.

Sidebar: A Quick "Who is Who" of Malware

Virus: A piece of self-replicating software code that appends itself to a program file or a sector of a disk.

Trojan: A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can obtain control and do its chosen form of damage.

Worm: A program that duplicates itself from one directory, drive, computer, or network to another through electronic communication (e-mail, instant messaging) or Local Area Networks.

Backdoor: A method of bypassing normal authentication, securing remote access to a computer and data while attempting to remain undetected. It may take the form of an installed program or could be a modification to an existing program or hardware device.

Rootkit: Techniques to allow concealment by modifying the host operating system so that the malware is hidden from the user or removal tools. The term originated based on its initial appearance in the UNIX environment (administrator = root access), but is now used generically for any concealed malware.

Spyware: A type of malware that can be installed on computers with the purpose of collecting information about users without their knowledge. The presence of spyware is typically hidden from the user and can be difficult to detect.

Botnet: Network of software agents (bots or robots) that run autonomously and automatically, most commonly for malicious purposes, but it can also refer to a network of computers using legit distributed computing software. The purpose of a botnet can vary, (e.g., distribution of spam or malware, coordinated denial of service attacks, and similar).

Threats and breaches can be external as well as internal in nature. A malicious insider could be used to aide an attack or even execute it on their own. This threat should be of concern especially since due to the economic pressures as a result of the most recent global recession. But also well meaning insiders can pose a risk, a simple example could be a nurse transferring a virus from her personal digital picture frame to a central monitoring station via a USB flash drive.

4 Regulatory Environment and the Role of Regulation

In most countries the sale and use of medical devices is highly regulated. For example, in the U.S. the definition of what is a medical device, how it is used, and how it is being manufactured and distributed is controlled by the FDA (FDA, 2010). Although minor variations exist between regions, similar controls are in place in other countries, e.g., through CE regulation in Europe. Commonly, these regulations mandate that the responsibility for validation and control of an approved configuration lies with the device manufacturer.

Although these strict controls assure the safety and reliable function of the device, they do make it more difficult to protect these devices against cyber attacks:

- Configuration controlled by manufacturer – prevents providers from installing after-market cyber security solutions.
- Controlled release process – long validation cycles make it difficult to deploy up-to-date security patches to operating systems and other OTS software.
- Need to predict behavior – limits the usefulness of traditional cyber security technologies, like Antivirus, as their behavior over the lifetime of the product cannot be predicted. Also, with traditional antivirus solutions, there is always the risk of false positive detections which, with a medical device, can have severe consequences.

The regulatory status of medical devices typically prevents healthcare providers from having access to the device or deploying security related software patches without consulting the manufacturer. Consequently, manufacturers are expected to provide patch releases or updates to the approved configuration in a timely manner.

For the U.S. market, the Food and Drug Administration (FDA) has stated that patching of off-the-shelf (OTS) software for medical devices is regulated by the design control portion of the existing Quality System Regulation 21 CFR 820 (FDA, April 2005). If determined by the manufacturer that the patch would not alter the intended use of the device or would not introduce new elements of risk, it would require validation as part of the manufacturer’s software maintenance activity, but it would not require renewal of the device’s existing premarket or other approval.

The FDA recommends that healthcare providers demonstrate device compliance as part of a quality assurance process and that proper management of the manufacturer’s released patches is part of the risk management program. However, providers should not make changes or apply patches without manufacturer advice or recommendation.

Any patch or security update strategy, whether implemented by the manufacturer or by the provider, needs to take the criticality of the respective system in consideration. Mission critical systems (e.g., surgery, ICU) will require a greater degree of attention. It is important that manufacturers and providers cooperate proactively in establishing such strategy, rather than reactively responding to the individual events.

5 Medical Device Types and Risk Considerations

Today’s medical devices are quickly moving from propriety hardware and software platforms to commercial off-the-shelf (OTS) hardware and software platforms and everything in between. While it is true that it has been some time since devices have been analog and processes purely paper-based, it was not that long ago when medical device manufacturers designed and produced all their own hardware and software components in house.

Each vendor created their own workstation hardware, operating system and sometimes even network protocols. This design combined with private network architecture created a fairly robust system in which all aspects of operation could be controlled, including release and security management.

However, this propriety approach and communication isolation did not allow for easy integration with other systems and caused the medical device manufactures to spend an increasing amount of time keeping up with advancements in technology and developing customized interfaces. Because of this most manufacturers today rely on commercial hardware and software components for their platform (hardware/operating system) and instead focus their efforts on the medical software applications. With these changes come increasing vulnerabilities and cyber risks. These vulnerabilities can impact the safe and effective operation of the medical devices.

For the purpose of discussion, we will focus on the current and next generation of medical devices that are a mixture of custom-build hardware and medical device application software, and OTS components like operating systems, network communication, or workstations. When a medical device manufacturer chooses to use OTS software as part of their device design, under FDA regulation that software becomes a component of the device and therefore falls under the existing regulations for the entire device.

A unique class of medical devices is purely software based, i.e. without individualized hardware components. These software-based medical devices are installed on standard workstation or server platforms but still within the manufacturer’s specified requirements. Operating system patching or third-party cyber security software (e.g., antivirus) still needs to be assessed against exiting regulations and as part of the approved device configuration.

The Role of Software in Medical Devices

Most patient monitoring systems are now networked together for alarm transmission, information sharing, and results reporting. These networked systems usually incorporate workstations that allow the clinical staff to view patient data in real time, while also providing reporting and documentation capability. Due to operational and real-time requirements, these central stations are typically provided by the manufacturer and are considered medical devices. However, a peek under the cover and what is really sitting at the nurses’ station may be nothing more than a personal computer (PC) running an OTS operating system such as Microsoft Windows or a Linux variant combined with specific custom software applications.

While most can easily identify the risks and vulnerabilities associated with such PC-based central stations, often times these same risks are not realized for the actual networked patient monitoring devices. Because of its often proprietary or locked down operating system it is easy to believe that the monitor is not vulnerable to the same threats as the more “commercial” devices. While this may be true with today’s state of operation and threat landscape, we must still understand the possible threats and include every device in the risk management plan for tomorrow.

Impact of Cyber Risks on Medical Devices

Medical devices that provide a life-sustaining service, such as a ventilator, a balloon pump or an infusion pump, must operate with the highest level of integrity and availability. However, with the shift toward commercial software and devices begin to become networked, it suddenly is more difficult for the manufacturer to maintain integrity and assure availability. In this situation, the manufacturer must coordinate their software releases with the OS vendor’s patches and updates. The OS vendor’s updates must also be validated to ensure that they do not impact the integrity of the medical device and it must be assured that they are reliably deployed to ensure maximum quality and up-to-date cyber protection of the larger installed base.

Network availability and utilization can also impact the operation of the device. Adverse conditions in either the operating system or the network have a negative impact that is directly related to the life-sustaining function of the device.

Patient safety is also a concern with diagnostic devices. If for instance the configuration of a CT scanner becomes corrupted because of a malware outbreak (or, as an example of a false positive, a virus misdiagnosis) improper treatment could result. Many real-time diagnostic or monitoring systems have zero margins for loss of availability or integrity.

Device Infrastructure Homogeneity

One of the challenges of managing medical devices is that there is a lack of homogeneous hardware and/or software across the enterprise. Most medical devices and systems are built based on the design specifications of the manufacturer but may not meet the business needs of the purchasing hospital. While it is true that most manufacturers are now going to a commercial platform and operating system, each is typically configured to support that vendor’s application. This, combined with the previously discussed regulatory restrictions, makes it very difficult to apply enterprise-wide security solutions to the medical devices.

However there are other instances where homogeneity is found and actually can have a negative impact. For instance, most hospitals typically purchase all of the infusion pumps from a single manufacturer to minimize training efforts, optimize maintenance, and maximize vendor discounts. While this is beneficial for the support of the devices, should a vulnerability exist it could be exploited by malware (e.g., as we have seen with Conficker (Keen, 2009 and Conficker

Working Group, 2010)) and shut down for the entire medication delivery system. This problem exists for any type of medical device, e.g., patient monitoring systems that utilize commercial operating systems and network infrastructure. Today’s sophisticated viruses have the capability to self-distribute (Symantec Corp., 2010), should a virus infect one device or workstation, it could easily propagate to like systems and compromise the monitoring of all the patients.

6 Privacy vs. Security Problems

When looking at networked medical devices, there are two related areas of concern:

- Privacy, i.e. protection of PHI (Protected Health Information) and PII (Personally Identifiable Information) stored on or transmitted by the device
- Security, i.e. the protection of the device and the data on the device against cyber threats.

Those two are tightly related and a proper security posture is required to enable privacy.

In general, it is recommended to take a risk management based approach to assess and manage medical device inventory. Specific guidance is for example provided by IEC 80001-1 (Cooper, 2010).

Medical Device Privacy

When assessing privacy risks, one should consider what type of data is being stored or transmitted, whether it is encrypted or not, whether the data on the device pertains to a single or many patients, and whether storage of the data is temporary or permanent. Manufacturers can disclose this type of information for example via NEMA's MDS[2] form (National Electrical Manufacturers Association, 2008).

Although some privacy issues can be mitigated by device design, proper process and management of devices and their lifecycle is essential. Policies should be in place to manage everything from device procurement (e.g., request manufacturer MDS[2]), onboarding (e.g., device-specific risk analysis, training), maintenance (e.g., validate OS patch level), repair processes (e.g., sending device off premises, receiving device back), and end of life (e.g., erase all PHI/PII stored on the device).

Medical Device Security

From a security perspective we need to deal with a significant degree of complexities. Even though we have not seen any targeted attacks on medical devices (as we have seen it on embedded systems in other industries, for example through the Stuxnet virus), there are documented cases where medical devices became a casualty of a larger malware outbreak, or in some cases the medical device became the entry point for an attack.

Especially malware with highly sophisticated distribution capabilities, for example Conficker (also known as Downup or Downadup), can enter a medical device via USB flash drive (for example during an on-site support visit) and then spread to like devices on the network which show the same security vulnerability.

Cyber protection on the device itself, as it could for example be built in by the manufacturer, is an effective solution as it addresses the problem at its root. However, traditional Antivirus technology is less suited for this as it requires regular updates of virus definition, its behavior as well as performance impact is difficult to predict, and, although the chance is slim, there is always the risk of a false positive detection.

Alternative cyber security technologies, like Host Intrusion Prevention (HIPS), are much more suitable for embedded systems and have proven themselves in other industries, e.g., with ATM devices. In short, HIPS locks down device configuration and behavior, tightly control device configuration, and limit and monitor all processes as well as inbound and outbound traffic. This technology, combined with security-aware design and configuration, are very effective in protecting embedded systems.

Although HIPS is an established and effective technology (Robb, 2006), it has not been widely adopted to secure medical devices. This typically leaves us with a significant security vulnerability on the lowest level, the device itself.

It is critical for healthcare providers to understand device software in use, patch level, cyber protection in place, and configuration across their entire inventory of networked assets. This is the baseline for a thorough risk analysis and allow for decisions on how to implement additional, external cyber security measures like VLAN separation, Firewalls, or similar (see for example here: (Department of Veterans Affairs, 2004)). Although external measures can be costly, difficult to maintain, and may not protect against all attack vectors, they are essential as many devices in today’s hospital environment are not sufficiently protected.

7 Roles and Responsibilities

As we advance and leverage modern technology, these integrated systems are exposed to more risk. Because these risks originate from different sources and can manifest themselves on any component within a complex system, it is important that responsibilities are shared in the appropriate resources are allocated for effective management. This implies redefining the boundaries of technical support for medical devices, and has blurred the lines of responsibility between the manufacturer, biomedical engineering and IT support. Today’s complex problems cannot be solved by just one group, cooperation across boundaries is essential.

Biomedical Engineering

Since modifications to networked medical devices are tightly regulated (for example in the U.S. under FDA Quality System Requirements), health-care providers must assure problem identification and resolution is accomplished effectively, documented properly and complies with all standards. Since its inception, biomedical engineering has been maintaining devices to these standards. Biomedical engineering also plays a key role in asset management, has a frontline position in workflow analysis, system utilization, clinical integration, and remediation of device-specific problems.

Hospital IT

Historically, most hospital IT personnel have not been responsible for Medical Devices. However, due to the shifting technology platforms, increasing interoperability, and the specific skill sets of IT personnel the scope of the IT department and their responsibilities is starting to change. It is important that hospital IT personnel are involved with Medical Systems starting at the evaluation level. Many times key components or prerequisites are missed without the proper IT individuals present. It is also important that IT risk assessments are performed prior to purchase and that safeguards and security architecture are a part of the medical device acquisition process.

Device Manufacturers

Device manufactures are in a unique position. It is their responsibility to manufacture and update their devices within the framework of medical device regulations and standards. However, once their devices are installed at a customer’s facility, manufacturers may find it difficult to perform software maintenance or install upgrades or patches. ". Devices that pass operational tests in a controlled environment can act unpredictably or fail when exposed to conditions that were not planned for in a real life environment. Many unexpected scenarios occur when the device configuration leverages existing hospital resources, such as desktop hardware and network infrastructure. Careful planning must be performed to foresee possible implications resulting from the use of commercial off the shelf hardware and software in a standard network environment and in conjunction with medical applications and systems. Additionally, medical device manufacturers must be prepared to react quickly to changes in the environment. This includes response to operating system vulnerability reports and subsequent patch distribution, fluctuations in network and radio frequency traffic and reliably interfacing communications with other systems.

8 Example Discussion / Threat Vectors

Looking at today's cyber threat landscape, there are a number of threats which are not relevant to embedded systems like medical devices. Any threat building on social engineering (e.g., phishing), utilizing attack vectors like email, and depending on user behavior (visiting an infected web site, downloading infected code, or similar) are of lesser concern.

However, what is of specific concern are any threats utilizing networks or "Sneakernet" based distribution mechanisms. Many medical devices are poorly protected and are vulnerable against threats introduced via portable media (USB, CD, etc.) or directly via the network.

Specifically the long useful life of medical devices can be a problem. Many devices still in use today were designed in times of a much simpler threat landscape. Also, they may be using older OS version which may be beyond their support horizon, which makes them particularly vulnerable to cyber attacks.

Further, users need to be aware of the risk of malware being introduced on a device itself, for example with devices returned from repair or loaner devices. This problem should be considered in the larger risk analysis and when planning device management process steps. To give an example, an external virus scan prior to network connection should be implemented for all devices entering premises (supply chain hardware component protection for new purchases, loaners, repairs).

A specific variation of a supply chain based risk is that of the introduction of a vulnerability via third party components. Manufacturers of medical devices may acquire software components or firmware embedded in hardware subsystems from a variety of sources. Supply chain attacks may be targeted or introduced via poor controls and processes on the side of the supplier. They may involve manipulating computing system hardware, software, or services at any point during the life cycle.

Introduction of malware into an infrastructure have been documented on a broad range of components, from software over USB flash drives to digital picture frames, to name a few examples. NISTIR 7622 (draft) provides an in depth discussion of the topic (Swanson, 2010).

Further, the increasing use of wireless technologies poses a unique problem for systems used in a mobile use case (ultrasounds, infusion pumps, handheld or body-attached systems). Obviously, all wireless communication should be securely encrypted to avoid "clear text" transmission of PHI. However, this raises the question of reliable key management to avoid a device losing connection due to loss of or invalid encryption or decryption keys. Respective standards define wireless encryption and key management (see: IEEE 802.11); automated key management systems are highly recommended to avoid communication disruption.

Lastly, with any device but especially with wireless devices, proper authentication is critical. This includes both, authentication of a user to access the device (e.g., for configuration or maintenance) as well as authentication of the device on the network (typically referred to as “network access control”). Again, the use of proper tools is essential to assure a reliable process and avoid accidentally blocking access.

9 Guidance on Counter-Measures

As discussed previously, taking a risk-management-based approach to managing complex medical device environments is essential for healthcare providers, but also for medical device manufacturers. Essentially, counter measures to protect medical devices from cyber threats and protect their PHI fall into three categories: device protection, network architecture, and lifecycle management.

Device Protection

Typically, any protection implemented on the device itself should be implemented by the manufacturer in compliance with regulatory mandates and to assure that the device functions within specification. As previously discussed, traditional antivirus is less suitable to be used in embedded systems, especially medical devices. However, other technologies exist and can be employed very effectively:

- Host Intrusion Prevention Systems (HIPS): a software-based technology which monitors a system's behavior on operating system level and against a known good configuration (system configuration and registry, port usage, program and process execution and behavior, and similar). Any system behavior which does not conform to this definition will not be allowed, therefore very effectively preventing outbreak of malwares or penetration by a hacker (Robb, 2006).
- Boot or software verification: a similar approach, although typically implemented at a deeper system level and compares system resources (e.g., BIOS settings) and executables against a known standard, e.g., by comparing a file's hash signature against its reference. Although this implementation is typically very specific to a given system, it is especially suitable for low-complexity devices with limited resources.
- Network and I/O monitoring: implemented as an ongoing process to monitor any data entering the system via network or ports and preventing any non-conforming data from entering.
- Device configuration: it is critical that any device used on today's complex networks is configured so that the risk to it is minimal. As examples, this includes to restrict the devices port (internet as well as physical) usage to only what is necessary, or elimination of the standard OS's administrator account.
  The requirement for configuration control may extend beyond the actual device itself and may include components of the immediate device infrastructure as they may pose a vulnerability to the device. For example, in case of a pure software based medical device, this would include the operating system of the host hardware.

Network Architecture

Use of proper network architecture allows reducing the risk of a malware outbreak or system penetration and also can contain the impact should such event occur. However, maintenance complexities may make it difficult to guarantee tight protection over time and it is not recommended to use any network architectural approach as the sole measure.

Key network architectures are:

- Use of VLAN segments specific to groups of devices, organizational entities, or functional groups. VLAN's will protect the respective segments against penetration, will contain any outbreak should it occur, and allow for the restriction of risk factors by for example eliminating email or internet traffic on a segment dedicated to medical devices.
- Firewalls can be used to separate off critical or valuable devices or groups thereof, thus reducing the risk of them being attacked or accessed. They can be implemented as a software-based firewall in the device itself, or external firewalls can be used.

However, implementing security via network architecture should be considered a secondary and supportive measure. Many providers find it challenging to balance the trade-off between security on one hand and connectivity/interoperability on the other. Such trade-off is a key factor that network segmentation is a short-term rather than long-term security measure and may be difficult to maintain reliably and over time.

Lifecycle Management

In addition to the technical measures described above, effective lifecycle management can also help to improve device reliability as well as security. These processes and policies can be implemented manually or via automated workflow management tools.

- Asset and inventory management: As a first and most important step it is essential to obtain a complete list of networked assets and their key configuration, for example OS type and version, including patch level, or network and port settings. Even though with medical devices any detected deficiency will typically require manual intervention and cooperation with the manufacturer, having a complete list of assets and defining the high risk items is a key first step.
- Purchasing process: a provider's security requirements should be clearly spelled when purchasing new equipment. This should include a manufacturer's disclosure the devices security and privacy parameters as well as the presence of any cyber protection (and the potential need for maintaining it) on the device, for example through the use of the NEMA MDS[2] form (National Electrical Manufacturers Association, 2008).
- Devices entering premises: any device which is being introduced (new purchase or loaner) or reintroduced (return from repair) into an environment should be assessed for: configuration changes (e.g., OS level or configuration) as well as the presence of malware which may have been introduced outside of the controlled environment. Tools and technologies exist (at least for standard platforms) to a) obtain device configuration, and b) perform an external virus scan, both prior to (re-)connecting the device to the provider network.

- Similar considerations apply to devices leaving premises. With any device the presence of PHI or PII on the device should be assessed (or known) and any critical data should be removed prior to it leaving the environment (e.g., for repair, return of a loaner, or to end-of-life it).
- Configuration validation and security check after 3rd party access: Any access to the device by a third party (manufacturer or service contractor) should be logged and the device should be checked for configuration changes and cyber security risks after each access. The risk of introducing malware or altering device configuration (intentional or unintentional) can lead to a compromised security posture of the device (e.g., open ports) or can introduce malware to the enterprise via the device itself.

Security Best Practices

In addition it is highly recommended to follow general IT Security Best Practices; auditing, logging, authentication, and encryption should be applied wherever possible. Device design or regulatory restrictions may pose some practical limitations but standards, like IEC 80001-1 provide the appropriate framework (Eagles, 2008; Cooper, 2010).

A Risk Management based approach in a medical device environment needs to be complete and holistic in nature to include not only of the device itself, but also the supporting technologies, the existing IT infrastructure, and the organization around it).

10 IHE's Role in the Framework of existing Guidance and Standards

A number of existing guidance documents and standards already exist and can be used to define a path forward. Although the referenced documents leave some gaps, combined they provide the best guidance available today. IHE and other organizations are actively addressing this topic and are moving towards providing a more comprehensive and secure future.

IEC 80001-1

"In 2006, the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) determined there was a need for a standard to define the requirements of a process for addressing the new problems that might emerge when medical devices are connected to a network. This proposed standard is IEC 80001, Application of Risk Management for IT-Networks Incorporating Medical Devices." (Eagles, 2008) (Note: IEC 80001-1 is now an approved and released standard)

This process standard covers activities, particularly risk management, required of both the health-care organization and equipment manufacturer when medical devices are integrated into a network, or when such integrations are changed. According to the ISO subcommittee, this standard also will cover the handover of information from the manufacturer to the responsible organization, sufficient to allow the health-care organization to manage risk.

NEMA MDS2

In preparation for compliance with the HIPAA Security Rule deadline in 2005 and the increased focus on medical device security, the HIMSS Medical Device Security Workgroup created a standard Manufacturer Disclosure Statement for Medical Device Security (MDS^2) form. The intent of the MDS^2 was to supply healthcare providers with a form that would allow them to gather the information needed to assess the vulnerability and risks associated with electronic Protected Health Information (ePHI) transmitted or maintained by medical devices.

This is a simple document that focuses on only the elements of the risk assessment process associated with medical devices and systems that maintain or transmit ePHI. This was the first step in creating a standard to allow manufacturers to quickly respond to a potentially large volume of requests regarding the security-related features of the medical devices they manufacture. (National Electrical Manufacturers Association, 2008)

Medical Device Integration Matrix

The Clinical Engineering/Information Technology (CE-IT) Community has created a matrix of potential questions facilities should ask manufacturers with respect to medical device integration. The Matrix has been developed into nine functional sections including: Manufacturer

Information, Decision Chart, Security, Network, Hardware, Software & Interface, Human Factors, Service Support, Training and Documentation. (CE-IT Community, n.d.)

DICOM Security Guidance

Specifically to imaging data, the DICOM committee has developed guidance around the secure exchange of information (DICOM supplement 31); authentication, confidentiality and integrity (DICOM supplement 55); and de-identification of patient data (DICOM supplement 142).

FDA Guidance

Understanding the a growing number of medical devices were being designed to be connected to computer networks and incorporate off-the-shelf software the FDA created a guidance document in 2005 to address how the possible vulnerabilities should be handled (FDA, January 2005). The findings of the initial document were reiterated in a reminder publication on the same topic (FDA, 2009).

While these documents do not provide any further regulation or enforceable responsibilities, they do provide a careful review of the topic and the regulatory requirements associated with the issue.

The Joint Commission Guidance

Although The Joint Commission does not provide direct guidance on the topic of cyber risks, it provides discussion of the issues resulting from the integration of information systems as part of its Sentinel Event Alert, Issue 42: Safely Implementing Health Information and Converging Technology (The Joint Commission, 2008)

VA Guidance on Network-Based Security

The Department of Veterans Affairs has recognized the problem of securing networked medical devices through proper network architecture, thus reducing risk and minimizing impact of an outbreak should it occur (Department of Veterans Affairs, 2004).

NIST Standards, Guidelines, and Technical Resources

NIST information security standards (Federal Information Processing Standards [FIPS]), guidelines (Special Publications in the 800 series), and technical resources may be used by organizations to help provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in information systems and technologies. While the original intent of many NIST information security resources was not specifically targeted toward medical devices, many of the concepts and security controls can be applied to the underlying medical device technology.

Specific NIST standards, like SP 800-82, although written for industrial control systems, can also provide valuable guidance for addressing the embedded system security issues in the healthcare environment.

HITSP TN 905

“This Technical Note is intended to act as a framing document to provide a high-level perspective on device connectivity requirements, to propose a roadmap for how HITSP might address these requirements, and to indicate how it might work with other external organizations to resolve standardization gaps. The specific requirements to be addressed in the roadmap are only those arising from the Harmonization Requests assigned to HITSP that include device connectivity elements, especially the Common Device Connectivity (CDC) AHIC Extension/Gap December, 2008. This includes the generic types of devices that shall be considered (e.g., ventilators or infusion pumps).” (HITSP, 2010)

11 Conclusion

The increasing integration of medical devices with hospital networks as well as use of off-the-shelf technologies exposes devices and the PHI stored on them to cyber risks. This can lead to compromised devices, breach of PHI, or even open the door to a larger attack on the enterprise network, all of which putting patient data and lives at risk.

A lot of work is being done to address these vulnerabilities to the underlying technology, but practical limitations as well as regulatory complexities within the medical devices standards are resulting in a less than satisfactory status quo. Healthcare providers are faced with the reality of having to protect their medical devices within the given realities.

This document provides guidance and suggestions on how Biomedical Engineers, IT professionals, manufacturers, and security experts can collaborate to minimize the risks associated with networked medical devices.

IHE and others are working on driving and refining the standards and protocols with the goal to reduce both, the burden on as well as the risk to our healthcare system. A comprehensive approach will combine aspects of process and workflow, system management, device and network architecture, and cyber security measures.

12 References

CE-IT Community. (n.d.). *Medical Device Integration Matrix*. Retrieved November 24, 2010, from CE-IT Community: http://www.ceitcollaboration.org

Conficker Working Group (June 2010, published January 2011). *Lessons Learned.* Retrieved February 9, 2011, from confickerworkinggroup.org: http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

Cooper, T. a. (2010). *Aiming for Patient Safety in the Networked Healthcare Environment*. Retrieved December 7, 2010, from AAMI.org: http://www.aami.org/publications/ITHorizons/2010/18-20_StandardsRegs_Cooper.pdf

Department of Veterans Affairs. (2004, April 30). *Medical Device Isolation Architecture Guide*. Retrieved December 7, 2010, from HIMSS.org: http://www.himss.org/Content/files/VA_VLAN_Guide_040430.pdf

Eagles, S. (2008). An Introduction to IEC 80001. *IT Horizons* , 15-19.

FDA. (2005, January 14). *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*. Retrieved December 7, 2010, from U.S. Food and Drug Administration: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

FDA. (2005, April 12). *Clinical Engineering Topic Discussion Series: Cybersecurity of Medical Devices*. Retrieved January 6, 2011, from U.S. Food and Drug Administration: http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ucm127816.htm

FDA. (2009, November 4). *Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility*. Retrieved December 7, 2010, from U.S. Food and Drug Administration: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm

FDA. (2010, March 1). *Medical Device Classification*. Retrieved December 7, 2010, from U.S. Food and Drug Administration: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm

HITSP. (2010). *Technical Note TN 905 - Device Connectivity*. Retrieved December 7, 2010, from www.hitsp.org: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=5&PrefixNumeric=905

Keen, C. E. (2009, June 2). *Conficker worm highlights PACS cybersecurity issues*. Retrieved December 7, 2010, from AuntMinnie.com: http://www.auntminnie.com/index.asp?Sec=sup&Sub=ris&Pag=dis&ItemId=86009

Markoff, J. (2010, November 19). *Worm Can Deal Double Blow to Nuclear Program*. Retrieved December 7, 2010, from The New York Times: http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html

National Electrical Manufacturers Association. (2008, September 29). *NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2)*. Retrieved December 7, 2010, from http://www.nema.org/stds/hn1.cfm

Robb, D. (2006, February 1). *New HIPS Technology Takes on Zero-Day Attacks.* Retrieved May 3, 2011 from eSecurityPlanet.com: http://www.esecurityplanet.com/trends/article.php/3582221/New-HIPS-Technology-Takes-on-Zero-Day-Attacks.htm

Swanson, M.; Bartol, N.; Moorthy, R. (2010, June). *NISTIR 7622: Piloting Supply Chain Risk Management Practices for Federal Information Systems*

Symantec Corp. (2010, April). *Symantec Global Internet Security Threat Report, Volume XV: Trends for 2009*. Retrieved December 7, 2010, from Symantec Security Response: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

The Joint Commission. (2008, December 11). *Safely Implementing Health Information and Converging Technologies*. Retrieved December 7, 2011, from The Joint Commission: Sentinel Event Alert, Issue 42: http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies/