



University HealthSystem Consortium

University HealthSystem Consortium Medical Device Security

January 2005

THE POWER OF COLLABORATION

Table of Contents

Contributors and Reviewers	1
Section 1. Overview	
Introduction	3
Executive Summary	3
Section 2. The U.S. Food and Drug Administration	
Background.....	7
Myth vs. Reality	7
The Future	9
Section 3. Contract Language	
Mitigation Responsibilities	11
Device Design—A Preemptive Approach	13
Recommendations for UHC Members	15
Section 4. Device Security Overview	
Overview	16
Best Practices	18
Section 5. UHC Member Approaches to Medical Device Security	
Member Stories	21
Section 6. Resources and Current Initiatives	
Industry Groups	24
Vendors	26
Section 7. Conclusion	28
Appendix A	
FDA Medical Device Reporting	29
References	32

Contributors and Reviewers

Anteon Corporation

Elizabeth Spangler
Information Assurance Manager (IAM)
Army PACS Program Management Office
Elizabeth.spangler@us.army.mil

Emory Healthcare

Matt Simon
Manager, Security & Client Services
Matt_Simon@emoryhealthcare.org

First Health

David Dillehunt
Vice President and Chief Information Officer
ddillehunt@firsthealth.org

GE Healthcare

John Moehrke
Enterprise Systems Architect: Security and
Privacy in Healthcare
John.Moehrke@med.ge.com

Angelo Calvache
Legal - Privacy
angelo.calvache@med.ge.com

Scott Bolte
Product Security Program Manager
Scott.Bolte@ge.com

Loyola University Health System

Ron Price
Associate Dean, Office of Information Systems
Loyola University Chicago Stritch School of
Medicine
Chief Technologist, Loyola University Health
System
rprice@lumc.edu

North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)

W. Holt Anderson
Executive Director
holt@NCHICA.org

Novation

Bob Benson
Senior Director, Contract Development
BBENSON@novationco.com

Oregon Health & Science University

John Kenagy
CIO, Information Technology
kenagyj@ohsu.edu

Thomas Drury
Manager, Healthcare Systems
drury@ohsu.edu

Philips Medical Systems

Nick Mankovich
Director Product IT Security
nick.mankovich@philips.com

SEC Associates, Inc.

Lisa Olson
Principal Consultant
lolson@secassociates.com

Siemens Medical Solutions

Mollie Beaver
Mollie.Beaver@siemens.com

Section 1. Overview

Introduction

Protecting systems against viruses, worms, and other threats has unfortunately become a way of life in today's networked environment, resulting in solutions such as antivirus software and firewalls. There are many ways of compromising a system including e-mail, Internet access, disks, and even network-connected medical devices, potentially causing a breakdown not only in the device, but the entire clinical information system as well. Clearly, all potential entry points should be protected in a robust fashion; however, there are issues associated with vulnerability management for medical devices.

One of the biggest problems relates to accountability. For example, virus protection primarily lives in the software, not the actual device. Device vendors are reluctant to expose their equipment to outside software and many have strict rules about adding or modifying software on their devices (even antivirus software), often citing lack of Food and Drug Administration (FDA) approval as the main reason. In actuality, the FDA rules address the safe performance of the device, putting the responsibility on the manufacturer for both the device and any off-the-shelf (OTS) software that is part of the device. There is much confusion as to who does and should own medical device security.

This paper examines the question of accountability and responsibility as well as investigating various approaches and solutions to medical device security. Recommendations of best practices and measures that both providers and manufacturers can take are also presented. Although this paper has a technology focus, it is intended to provide a good foundation for any individual interested in the topic of medical device security.

Executive Summary

The U.S. Food and Drug Administration

There is a misconception fostered by some medical device manufacturers that manufacturers cannot install security patches without prior FDA approval. While it is true that the FDA's requirements are aimed almost exclusively at the medical device manufacturer, the FDA's regulations do not necessarily prevent manufacturers from installing security patches without prior approval. Rather, the regulations allow (if not require) the manufacturers themselves to determine the safety and effectiveness of any patch using the maintenance plan that should have been developed and submitted as part of the initial premarket submission. The only real constraint imposed by the FDA's regulations is the additional time required to thoroughly test patches, something that the manufacturers should be doing regardless.

Contract Language

Because there is so much confusion surrounding the FDA's regulations, health care providers are taking their own measures to define and/or ensure vendor responsibilities related to medical device security by modifying contract and request for proposal (RFP) language. Two general approaches are being taken. The first approach is to better define mitigation responsibilities once a vulnerability has been identified. This language addresses 4 areas:

- The HIPAA Security regulation—Invoking the vendor’s responsibility to comply by protecting electronic patient information from any reasonably anticipated threat
- Urgency—Defining what constitutes “urgent,” as well as associated actions and time frames for dealing with urgent issues
- Liability—Determining the best balance between the vendors who can better determine the impact of a patch on the design of a device and the user who can (arguably) more accurately measure the impact of patching (or not patching) the device within their network
- Definition of party or parties responsible for testing and applying patches

The second is a preemptive approach that encourages manufacturers to build security components directly into the device. At best, this approach requires vendors to modify the device design to incorporate security. At the least, the approach includes a comprehensive questionnaire or worksheet that the vendor or manufacturer must complete so that an organization can make an informed decision about whether to purchase the product or at least know what the consequences might be in the case of an exploit.

Of the 2 approaches, the preemptive approach seems to have the better chance of success and has yielded several initiatives that can be tackled by UHC members, and may also be pursued in conjunction with other industry groups that have been formed to address this very important issue:

- Convene a forum of medical device vendors, security software vendors, and UHC members to determine if a standard can be created for security components that should be integrated into new medical devices going forward.
- Join discussions from the Department of Defense (DoD), National Electrical Manufacturers Association (NEMA), Healthcare Information and Management Systems Society (HIMSS), the Department of Veterans’ Affairs (VA), Novation, manufacturers, and other organizations to develop a template to be used to hold all parties accountable for evaluating security, and agree on a methodology and approach to securing the medical devices that exist today.
- Merge the forms being sent to the manufacturers to provide a common set of questions to which all vendors will be held accountable. This form will likely be used during an RFP process, but may also be used for renewals and upgrade planning.

Device Security

While defining contractual obligations for medical device vendors, including enforced hardening of devices, is a good long-term approach, a shorter-term solution is needed. Organizations need to be proactive about protecting their medical devices and networks. The first step is to understand the risk to the computing environment that is posed by networked medical devices. Risk may be evaluated using the following equation:

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$

Threats include malware such as viruses or worms. Vulnerabilities are weaknesses—for example, a remote buffer overflow or an administrative account with no password. Impact includes the cost of downtime for the device, cost of repair and remediation, and regulatory penalties incurred by the loss of or unauthorized access to electronic PHI (ePHI). The greatest potential cost—the compromise of patient safety—cannot be quantitatively measured but is certainly an important factor.

Quantifying the risk posed by each device makes it easier to prioritize where to place extra controls and aids in making a case to management for needed funds to minimize the risk posed by networked medical devices. There are a number of methods available to perform risk assessments, including OCTAVE,¹ a self-guided risk methodology developed by CERT² at Carnegie Mellon University, and the Microsoft methodology.³

There will always be risk introduced by network medical devices; the goal is to minimize the risk to an acceptable level. More important than having specific point solutions available to protect network medical devices is having a good security posture in general throughout the network. Best practices for securing medical devices that providers can implement themselves include:

- **Knowledge about both the network and the devices.** This may include running protocol and port scans against all networked devices, as well as the use of vulnerability analysis tools.
- **Risk assessment.** This requires a vigilant methodology to constantly assess and manage risk. Often this involves a multidisciplinary team that monitors the organization's network and exposure, as well as monitoring and reacting to vulnerabilities identified by such external organizations as CERT.
- **Virtual LANs (VLANs) to segregate devices that communicate with each other.** Understanding the communication relationships between devices is key to using VLANs as a security control for networked medical devices.
- **Firewalls.** For devices that pose the greatest risk, small firewalls or routers with access control lists (ACLs) are necessary to protect the device from compromise.
- **Intrusion detection systems/intrusion prevention systems (IDS/IPS).** IDS/IPS can be used to look for abnormal traffic and take action based on the event.
- **Change/configuration management.** It is critical that all changes to networked medical devices be recorded in detail.
- **Proxy servers for Internet connectivity.** A proxy for all Internet connections can significantly increase security posture, particularly if the proxy server also employs antivirus scanning technology.
- **Executive support.** If security is driven from the top down, the security program of the entire enterprise will be significantly stronger.

Although providers can themselves, for the most part, safely implement these practices, if there is any doubt as to whether a particular practice or activity will effect the functioning of a medical device, it is best to check with the device manufacturer.

Member Approaches

UHC members have employed a variety of techniques to resolve the issues surrounding medical device security. These include many of the approaches that will be outlined in this paper, such as preemptive approaches, isolation techniques (e.g., virtual private networks [VPNs] and firewalls), and proactive measures (looking for potential problems by keeping abreast of industry-identified vulnerabilities and actively monitoring the network for intruders).

Conclusion

A number of approaches to ensure medical device security will be presented in this paper, including the definition and designation of responsibilities, potential changes to contract language, and actual system solutions that can be implemented either at the network or device level. No single solution stands out over the others and all have merit. The unfortunate truth is that as long as there are computers, there will be vulnerabilities and therefore potential security breaches. A combination of approaches is necessary to achieve the maximum level of security required for most medical devices and because of the ever-changing environment in which we live, the job will never be truly finished.

The real conclusion to be drawn from this paper is that it is ultimately up to the provider organization to make sure that the appropriate safeguards are in place. The FDA is limited in what it can enforce through regulation. Vendors are not indifferent to the issue but are arguably less vested than providers, meaning that medical device security is a lower priority for them. Industry groups can influence but not enforce policy. Providers need to keep doing what they are doing: implementing their own measures to the extent that they can and collaborating with each other to define industry standards and collectively influence vendors to take on more responsibility for medical device security.

Section 2. The U.S. Food and Drug Administration

Background

The U.S. FDA, specifically, the Center for Devices and Radiological Health (CDRH), is responsible for regulating firms that manufacture, repackage, relabel, and/or import medical devices sold in the United States. This includes emitting electronic products such as X-ray systems and ultrasound equipment. Medical devices are specifically subject to the general controls of the Federal Food Drug & Cosmetic (FD&C) Act, which contains the baseline requirements that apply to all medical devices necessary for marketing, proper labeling, and monitoring performance once the device is on the market. These general controls may be found in the final procedural regulations in Title 21 Code of Federal Regulations Part 800-1200.⁴

The FDA breaks down medical devices into 3 classifications: Class I, Class II, and Class III, which define the regulatory requirements for the general device type. With the exception of some Class I devices that are exempt, medical devices cannot be commercially distributed without authorization from the FDA. Authorization is obtained by submitting either a Premarket Notification 510(k) for devices that are substantially equivalent to FDA-approved devices that are already on the market, or a premarket approval for high-risk devices that do not fall under the premarket notification process. A list of exempt devices, as well as guidance on classifying a device and regulatory control are available through the FDA's Device Advice homepage.^{5,6}

A device, in and of itself, is basically considered to be safe once it goes through the comprehensive FDA approval process and reaches the market. Safety concerns arise once the device is in use and security vulnerabilities are discovered. Remediation of the vulnerabilities often requires an update to the operating system (O/S) in the form of a security patch. Questions about who is responsible for testing and installing a patch, the timeliness of the patch installation, and whether patching a system requires FDA approval have created much confusion and some contention between health care providers and medical device manufacturers and distributors.

Myth vs Reality

The Myths

There is a misconception, fostered by some medical device manufacturers, that manufacturers cannot install security patches without prior FDA approval. This has evolved into the general sentiment that FDA policy is degrading network security and performance by impeding the timely implementation of security and other maintenance patches in commercial off-the-shelf (COTS) software used in network-connected medical devices. In a Web conference presented to UHC members in June 2004, Brian Fitzgerald, Deputy Division Director, Division of Software and Electrical Engineering, FDA, addressed these concerns.

The Reality

While it is true that the FDA's requirements are aimed almost exclusively at the medical device manufacturer, the FDA's regulations do not necessarily prevent manufacturers from installing security

patches without prior FDA approval. There are 2 FDA rules that are applicable to software maintenance patches.

Regulation 21 CFR 807.81 part (a)(3),⁷ the section that addresses when a premarket notification is required, states that a change or modification in the device that could significantly affect the safety or effectiveness of the device requires a new premarket notification by the manufacturer:

[A premarket notification is required when]

(3) The device is one that the person currently has in commercial distribution or is reintroducing into commercial distribution, but that is about to be significantly changed or modified in design, components, method of manufacture, or intended use. The following constitute significant changes or modifications that require a premarket notification:

- (i) A change or modification in the device that could significantly affect the safety or effectiveness of the device, e.g., a significant change or modification in design, material, chemical composition, energy source, or manufacturing process.
- (ii) A major change or modification in the intended use of the device.

The quality system regulation 21 CFR 820.30(g)⁸ states that design changes must be validated by the manufacturer when the change cannot be verified by subsequent inspection and testing:

g) *Design validation.* Each manufacturer shall establish and maintain procedures for validating the device design. Design validation shall be performed under defined operating conditions on initial production units, lots, or batches, or their equivalents. Design validation shall ensure that devices conform to defined user needs and intended uses and shall include testing of production units under actual or simulated use conditions. Design validation shall include software validation and risk analysis, where appropriate. The results of the design validation, including identification of the design, method(s), the date, and the individual(s) performing the validation, shall be documented in the DHF.

The FDA offers guidance when applying these regulations to software (U.S. Department of Health, 1997). Therefore, a new premarket notification is needed if:

- The proposed design change (or patch) affects the indications for use, or
- Clinical data are necessary to evaluate safety and effectiveness of the change, or
- Evaluation of the change raises new issues about safety and effectiveness.

The first qualification is not applicable. Per regulation 21 CFR 814.20 (b)(3)(i),⁹ the definition of “indications for use” is as follows:

(i) *Indications for use.* A general description of the disease or condition the device will diagnose, treat, prevent, cure, or mitigate, including a description of the patient population for which the device is intended.

Application of security patches or other security configuration changes will never affect the indications for use.

The other 2 qualifications for submitting a new premarket submission relate to evaluating the safety and effectiveness of proposed changes. Quality system regulation 21 CFR 820.30(g) basically allows (and arguably requires) the manufacturer to make the determination regarding safety and effectiveness of changes. Manufacturers should develop a maintenance plan for the COTS software for their devices. The plan should be part of the initial premarket submission. The plan may delegate authority for carrying out aspects of the plan to user facilities, COTS vendors, third parties, and of course, the manufacturers themselves. Manufacturers adhering to the maintenance plan as described in the original premarket submission may test patches and more often than not are able to install them without any interaction with the FDA. Rarely will a patch require clinical data to test its effectiveness, nor will it usually compromise the safety or effectiveness of a device.

The Myth Dispelled

The FDA clearly does not prevent manufacturers from installing security patches without explicit approval; it only potentially limits those manufacturers that do not have clearly defined maintenance plans for COTS software in their devices. Provider organizations can address this issue by contractually requiring vendors to develop and implement maintenance plans for any devices being purchased; this is covered in greater detail in the next section.

By requiring thorough testing of any medical device software change, be it at the application level or the operating system level, regardless of whether the change is in the form of a patch or enhancement, and regardless of which entity performs the testing, the FDA policy imposes a time factor for installing patches. However, the added time does not “degrade network security,” nor should it be viewed as an impediment. Rather, it should be viewed as enhancing network security by ensuring the quality of a medical device. Patches are not infallible and they have the potential to cause more problems than they solve. It is critical to test a patch thoroughly before implementing it even if it means taking a medical device out of commission during the interim.

The Future

On November 12, 2004, UHC spoke with FDA’s Brian Fitzgerald to learn what plans, if any, the FDA has for the area of medical device safety in the future. According to Fitzgerald, the FDA policy “is what it is” and there are no specific plans to change the policy in the foreseeable future. The FDA is, however, working on several other initiatives:

- **Clarification of the current policy.** As illustrated, there is still much confusion regarding the FDA policy. The FDA recognized the need to clarify the regulations to both providers and device manufacturers and in January 2005 released a guidance document providing some clarification, “Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.”¹⁰ The FDA welcomes and encourages comments and suggestions on the guidance document; information on submitting comments can be found in the document itself.
- **Segmentation of networks.** Inspired by the VA’s approach to medical device security,¹¹ the FDA is recommending the segmentation of networks, which limits the exposure of medical devices and related software to the rest of the organization’s network and the Internet. This segmentation can be accomplished using tools such as VLANs and ACLs. The FDA is working on a guidance document that outlines this approach.

- **System integrators.** A system integrator is “an individual or company that specializes in building complete computer systems by putting together components from different vendors. Unlike software developers, systems integrators typically do not produce any original code. Instead they enable a company to use off-the-shelf hardware and software packages to meet the company's computing needs.”¹² From the FDA's point of view, system integrators best accomplish risk management for medical device safety. They are drafting a guidance document that outlines this philosophical approach.

In the meantime, the FDA encourages health care organizations to report all problems. Product problems should be reported to the FDA when there is *any* concern about the quality, authenticity, performance, or safety of a medication or device, not just in the case of an adverse event. This includes problems related to vulnerability management. Although there is much anecdotal evidence that malicious software has compromised the performance of medical devices, as well as the networks they reside on, there is a notable lack of formal reporting. Without formal evidence, the FDA is limited in its ability to intervene with the device manufacturers. Information on how to report medical device problems can be found in Appendix A.

Section 3. Contract Language

Because there is still much confusion regarding the FDA's regulations, organizations are taking other measures to secure medical devices. One area of security hardening has been focused on strengthening the security requirements asked for in the RFP process and enhancing the contract language incorporated into purchase agreements to define the responsibility and accountability for device security between the vendor and the provider organization. This approach is currently being tested. Although many organizations are working on the contractual security support language and when it should be inserted into the process, most parties that UHC interviewed are still struggling.

Proposed contract language addresses medical device security from 2 different angles. The first is mitigation responsibilities following the identification of vulnerability. Draft text has included resolving issues such as the length of time to patch a known security vulnerability and defining who is responsible for patching, as well as other vulnerability management issues. The second angle takes a preemptive approach and focuses on defining the responsibility the vendor has for designing the device. This approach is centered on the functionality that vendors should build in, and what can be added to the device during and after installation. Considerations for each of these 2 approaches are discussed in the following sections.

Mitigation Responsibilities

The mitigation responsibilities following the identification of vulnerability are not easy to address because there are several hurdles and distractions. These include the rapidly approaching HIPAA Security deadline of April 2005, defining the urgency and liability issues of a vulnerable or compromised device, and identifying the source of the compromise.

The following excerpt is from a current bid for an imaging contract by UHC's Service Delivery team. It reflects some of the problems with language surrounding vulnerability identification. It does not account for urgency, level of threat, level of risk, the criticality of the device function, or the potential for compromise. It only barely addresses the HIPAA implications. It may also have the potential to place technical restrictions on the environment and contains metrics that which may be counterproductive in executing a required patch.

2.10 Access, Service Packs, and Patches. When accessing the Member's devices remotely, the Supplier shall utilize VPN connectivity via a VPN client, a site-to-site VPN or via a secure sockets layer (SSL) VPN connection. At all times Supplier must comply with the Member's remote administration guidelines. Supplier must have a current Business Associates Agreement (BAA) on file with the Member as required by HIPAA, and require all Supplier staff to comply with this agreement. Supplier shall have a Web page that Members can access that reports OS and application vulnerabilities, patches or remediation instructions, and patch status. Access to this page will be free to Members that have purchased the Supplier's equipment regardless of maintenance status. All vulnerabilities shall be posted to this Web page within 2 days of the vulnerability being discovered. The remediation instructions shall be posted to the Web page within 2 days of the vulnerability being discovered for high-severity incidents as defined by the U.S. Circuit Court (USCIRC) and within 2 weeks for moderate- and low-severity incidents.

The HIPAA cloud is looming over the entire industry. The confusion about what the industry best practice is continues to bring groups together for dialogue. The HIPAA Privacy Rule Section 164 Privacy and Security¹³ is driving many of the proposed changes to legal text. The section discusses addressable items around ePHI, protection from any reasonably anticipated threats or hazards of such information, and protection against uses or disclosure of such information.

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

Section 164.308 (administrative safeguards) comes closest to the issue, focusing on protection from malicious software. It defines this protection as:

(B) *Protection from malicious software (Addressable).*

Procedures for guarding against, detecting, and reporting malicious software.

Because this is focused on ePHI, devices that do not contain identifiable patient information fall outside of the approaching regulation. Additionally, because the HIPAA focus is primarily on securing patient information, satisfying HIPAA requirements only partially meets enterprise concerns and responsibilities.

The second issue with mitigation of responsibilities is identifying the liability. Should the vendor be accountable for recognizing the need for a patch or should the provider organization? Microsoft claims no responsibility for the damage done by a virus, but market factors have driven it to push XP Service Pack 2, a release focused on security. The issue of liability must be balanced between the vendors, who can better determine the impact of a patch on the design of a device, and the user, who arguably can more accurately measure the impact of patching (or not patching) the device within that network. The contract language should attempt to define this balance.

The third challenge is to define the level or urgency of the threat. For example, although Microsoft rates the different vulnerabilities for its operating systems, these ratings are likely based on different criteria than medical device manufacturers or users would use. The relevant parties must agree upon metrics with which to rate the level of threat, as well as on subsequent actions. The formula of Risk = Threat × Vulnerability × Impact, discussed later in this paper, is a good methodology for weighting different vendor and user concerns. It is critical to implement a formal risk assessment methodology to validate the residual risk presented by the device vs the mission of the health care organization.

Assuming that HIPAA, urgency, and the risk metric are adequately defined, the final hurdle is to define the process of who should test and apply the update. The problems that have been encountered by installing Windows XP Service Pack 2¹⁴ illustrate that installing a patch that is not thoroughly tested can

cause more problems than the threat itself. Should the vendor test and install the patch on the device or should the user, in order to identify the impact on the actual environment? The best solution is probably a combination of the vendor and the user, with the specific responsibilities dependant on the particular device. Regardless, the “who(s)” must be defined and included as part of the contract language.

Mitigation—Postvulnerability Identification Summary

In summary, contract language surrounding postvulnerability identification responsibilities should address 4 areas:

- The HIPAA security regulation
- Liability
- Urgency
- Definition of party or parties responsible for testing and applying patches

The HIPAA issue can be dealt with through best practices. UHC is sponsoring an ongoing dialogue with its members to determine what academic medical centers (AMCs) consider best practices and come to a consensus; this should meet the “reasonable” portion of the HIPAA regulations.

Urgency and liability issues have already been resolved within the finance industries and should be resolved by the health care industry using the same risk analysis approach. NEMA and HIMSS have also created workgroups to identify how to determine urgency.

The remaining issue is the responsibility for testing and execution of the fix. There are fewer resources to draw on when crafting this portion of the contract; however, the maintenance plan that the device manufacturer was required to submit to the FDA before being authorized to market the device should provide guidance in helping the parties determine how the patch should be tested and implemented and who is responsible for these tasks.

Device Design—A Preemptive Approach

Another approach to medical device security that is driving changes to the traditional contract language is the idea that medical device manufacturers should build security components directly into the device. This approach stems from the recognition that users have varied and complex environments in which devices will be deployed, coupled with the idea that any organization with Internet-facing applications or devices should have a layered defense strategy.

Some UHC members have suggested that having security components on the device that are both installed and supported by the manufacturer would make the responsibility clearer. Providing that the user maintains the device as required, all risk is transferred directly onto the vendor.

This approach has several drawbacks. These drawbacks include:

- Identifying the best security strategy and supporting software
- Identifying how the security component impacts the function of the device itself
- The impact of mixing devices and components within a single environment;

- The compatibility with the users' enterprise layered defense strategy
- The length of time required to develop a medical device from inception to FDA approval—5 to 7 years—which makes this a long-term solution

Any security or quality assurance involves a cross-validation component. Having Symantec go head-to-head with McAfee is an example of this. As long as there are at least 2 options, there will be subtle differences that make them not entirely compatible. Standards may help, but an enforced policy on methodology and methods of implementation is unlikely.

If the organization's strategy is to use a single-vendor solution within an environment, the design of the medical device may not be compatible with the chosen vendor security software. For example, some devices open all ports for dynamic use, while other devices force the use of a specific port. The impact of dynamic ports may be critical to one device, but cannot be used if the vendor of another device does not use the same port usage scheme.

Most devices today have a proprietary design. Some of these devices use proprietary software and will not accept any add-on security component. Given the quantity and variations among devices, the potential for a common security component that would work with all devices is very unlikely.

While building security components directly into a device may introduce compatibility issues with the myriad of complex system environments deployed today, contract language can require that certain security components and/or procedures be in place. An example of this approach is demonstrated by the University of Virginia's use of the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)¹⁵ vendor RFP template¹⁶ for meeting HIPAA security requirements.

The NCHICA is a nonprofit consortium of more than 250 organizations dedicated to improving health care by accelerating the adoption of information technology. The template covers 4 areas, including password control, security administration, activity logging, and networking and compatibilities. This works well for the University of Virginia because the security group has "veto-like" authority for purchases. The answers given on the NCHICA worksheet clearly show what security a device contains and/or is missing.

Another example is the Manufacturer Disclosure Statement for Medical Device Security (MDS²)¹⁷ developed by the HIMSS Medical Device Security Workgroup¹⁸ and endorsed by HIMSS, the American College of Clinical Engineering (ACCE),¹⁹ ECRI (formerly the Emergency Care Research Institute),²⁰ and NEMA.²⁰ As noted in the instructions for MDS², a manufacturer-completed document should be useful to health care provider organizations worldwide and should include device-specific information addressing the technical security-related attributes of the individual device model. The statement is adapted from several sources, including *Information Security for Biomedical Technology: A HIPAA Compliance Guide*,²² jointly developed by the ACCE and ECRI. In addition to the ePHI, administrative, and physical and technical safeguard questions, the 9-page form includes a section for the manufacturer to recommend security practices. The form can be downloaded from <http://www.himss.org/content/files/MDS2FormInstructions.pdf>.

The DoD has also tried the preemptive approach. It has spent the last 2 years asking medical vendors to apply O/S hardening to their systems before deployment. With some success, it has directed them to use recommended guides from the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), as well as implement simple changes such as disabling unused ports and

services, uninstalling unnecessary programs that are installed with the O/S as default, using stronger passwords, and having a computer emergency response team apply security patches.

The DoD also requires vendors to comply with the Mission Assurance Category (MAC) (DOD 8500.2) policy.²³ This extensive document defines 3 levels, MAC I through MAC III, with MAC I being the most stringent. MAC I requires high integrity and high availability, MAC II requires high integrity and medium availability, and MAC III requires basic integrity and availability. MAC II requires additional safeguards beyond best practices while MAC III requires protective measures, techniques, and procedures generally commensurate with commercial best practices. RFPs must include components and subcomponents of this regulation. Current DoD regulations require MAC III compliance for medical devices.

Preemptive Device Design Summary

The preemptive approach seems to have the best chance of succeeding. Despite the long design and life cycle of medical devices, manufacturers can use the questions on a common form to see where the users are focused and reduce the number of similar inquiries about RFPs. MDS² seems to have the most support with its acceptance by the NEMA, ACCE, and ECRI. Although this form provides an excellent starting point, it should be expanded to include non-ePHI devices and provide an indication of how the device security strategy blends with the user's layers of defense strategy.

Recommendations for UHC members

- Convene a forum of medical device vendors, security software vendors, and UHC members to determine if a standard can be created for security components that should be integrated into new medical devices going forward.
- Join discussions with the DoD, NEMA, HIMSS, VA, Novation, manufacturers, and other organizations to develop a template to be used to hold all parties accountable for evaluating security and agree on a methodology for securing the medical devices that exist today.
- Merge the forms being sent to the manufacturers to provide a common set of questions to which all vendors will be held. This form will likely be used during an RFP process, but may also be used for renewals and upgrade planning.

Section 4. Device Security Overview

Overview

Working with the device manufacturers to contractually define responsibilities and harden devices has much potential; however, it is a long-term solution. Today's volatile and often hostile environment requires that organizations take immediate measures to secure their devices. Although there are some restrictions imposed by the manufacturer, there are steps that an organization can legally take to secure its own systems, as outlined below.

Networked medical devices use a variety of operating systems, often from vastly different computing eras. Moreover, they have varying levels of hardening, configurability, manageability, and contain information ranging from basic clinical data to ePHI. Many networked devices, when compromised, can endanger the health of a patient—for example, when a medical device used in the emergency department (ED) is not available because it has been compromised.

To help understand the risk posed by networked medical devices to the AMC computing environment, it is helpful to examine the devices from a risk assessment perspective. Essentially, Risk is the product of the Threats to the device, the Vulnerabilities of the device, and the Impact associated with a breach of the device. The basic equation is:

$$R = T \times V \times I$$

Threats are defined as a potential cause of an unwanted impact on a system or organization. For instance, viruses that use e-mail as their infection vector have a high threat value because of the frequency of their occurrence. In terms of networked medical devices, the threats posed to them are similar to those posed to the other networked devices in the environment. These threats include viruses and worms as well as compromise of the device by an individual.

Vulnerability is defined as a weakness that makes an asset susceptible to exploitation by a threat. For instance, a Windows-based device with no antivirus protection has a high vulnerability value, whereas a Linux-based device would have a correspondingly lower vulnerability value since the vast majority of viruses and worms are written to exploit vulnerabilities in Windows programs. Other examples of vulnerabilities include a remote buffer overflow or an administrative account with no password.

Impact includes items such as the cost of downtime for the device, the cost of repair and remediation, regulatory penalties incurred by the loss of ePHI, and legal costs associated with the failure of the device. Although patient safety is not an easily quantifiable cost, it needs to be included in the equation because of the sensitive nature of networked devices in a clinical environment. The asset cost may be different depending on the device. For instance, it is possible that if a device was compromised the organization could live without that device for 2 or 3 days until the vendor made repairs. That would certainly not be true of a device that is used in the ED, for instance. Thus, it is imperative to perform a risk assessment on each device individually since the exposure for each asset is different based on its place in the patient care continuum.

The importance of performing an effective risk assessment on each networked medical device cannot be overemphasized. By understanding and quantifying the risk posed by each device it becomes easier to prioritize where to place extra controls and aids in making a case to management for needed funds to minimize the risk posed by networked medical devices. Since each device is different in terms of its operating system, manageability, antivirus posture, and level of vendor support for security, it is important to perform a risk analysis for each device individually.

There are a number of methods available to perform risk assessments. CERT at Carnegie Mellon University has developed OCTAVE, which is a self-guided risk methodology. Information on OCTAVE can be found at <http://www.cert.org/octave>. Microsoft also has developed a risk assessment methodology based on OCTAVE and other methods. The advantage of Microsoft's methodology is that it uses an intuitive scoring system and comes with predefined templates to assist in the assessment process. Detailed information on Microsoft's methodology can be found at <http://www.microsoft.com/technet/security/guidance/secrisk/default.mspx>.

The Role of the Operating System

There is good reason to believe that Windows operating systems are less secure than other operating systems because of a multitude of factors. These include the dominance of the market by Microsoft and, until recently, the lack of attention given to securing Windows operating systems. Since Windows devices are arguably more vulnerable to compromise than devices that use embedded operating systems or an O/S that is based on some version of Linux/Unix, they should consequently receive a higher risk rating than a device running on a proprietary or Linux/Unix O/S. Any modern day O/S can be hardened if configured properly.

The Role of Antivirus

The ever-present, ever-changing variety of worms and viruses that are in proliferation pose a major threat to all networked devices causing the need for antivirus software. While almost all organizations have antivirus measures in place on networked devices, often, networked medical devices do not have antivirus software. There are several reasons for this:

- Antivirus software running on the device may affect accuracy
- It may also affect the performance of the device
- Vendors may not allow the installation of antivirus protection

On occasion, antivirus software may be on the device, but it needs manual intervention, or worse, Internet connectivity to retrieve signature updates, rather than using an internally managed update process. Antivirus software that is not regularly maintained quickly becomes out-of-date and of little use.

Ideally a networked medical device will have a managed antivirus solution in place that is equivalent to the other fully managed devices on the network. Unfortunately, many, if not most, networked medical devices that support antivirus software (i.e., Windows-based) do not have any installed.

The Role of Hardening

By hardening a device, an attempt is made to make it more secure from attack by performing actions that limit the vulnerability presented by the device. For instance, turning off unnecessary services or daemons,

restricting unnecessary operating system access, and thorough patch management are all factors in how resilient a device is to attack.

The manufacturer distinctly influences the degree of hardening in networked medical devices. Unlike other computing devices where the information services team has complete control over the configuration and management, networked medical devices run the gamut from completely unhardened, unmanaged Windows machines that run unsupported operating systems to Linux/Unix-based machines that have been hardened by the manufacturer.

Patch management has been a topic of conversation regarding network medical devices for some time. As noted in the first section of this paper, rumors and speculation regarding the FDA certification status of a patched device exist everywhere. While there are advocates of strong contractual language stating that medical device manufacturers must patch devices within a certain number of days of release of the patch, experience has shown that may not be the wisest route. There have been occurrences where patches have broken existing software applications, or the O/S itself. Proper and thorough testing is essential to any patch management program. Another important point to note is that many vulnerabilities that are fixed by released patches require some significant user interaction for an exploit to occur. With that in mind, it is far more important that the medical device manufacturer have a methodology for patch management, rather than a hard deadline for patching of devices.

Therefore, while regular patch updates are very important to the security of networked medical devices, they must be applied only after careful and methodical testing, lest the patch do more harm than good. Additionally, if even minimal hardening can be done on the device to limit user interaction, the associated vulnerability of the device declines significantly.

There will always be risk introduced by network medical devices, but the goal is to minimize the risk to an acceptable level. More important than the point solutions available to protect network medical devices is having a good security posture in general throughout the network. This includes hardened and managed desktops, servers, regular patch management, layered antivirus protection, and intrusion detection /intrusion prevention systems. An effective incident management plan can minimize the damage caused by a security event and provide important lessons for improving the enterprise security posture. Incident response plans must include network medical devices to ensure consistent follow-up and to provide feedback to regulatory agencies and the device manufacturers.

Best Practices

Best practices in securing medical devices include:

- **Knowledge about both the network and the devices.** It cannot be emphasized enough that knowledge is power when it comes to securing networked medical devices. During the course of our research, we often found that the engineers at the institution know as much or more about the ins and outs of the communications of the device than the manufacturer.
 - Running protocol and port scans against all networked devices is essential to understanding the vulnerability cross-section presented by the device. Questions such as what other devices a medical device talks to and what protocols or ports it uses are essential to understanding how the device communicates on the network. That information should be

used to create network maps that encompass all networked medical devices. Free utilities like NMap (<http://www.insecure.org>)²⁴ can be used for scanning, and sniffers that listen to network traffic, such as Ethereal (<http://www.ethereal.com/>),²⁵ can be used to examine what the devices are doing during normal operation.

- A vulnerability analysis tool should also be run against all networked medical devices. Nessus (<http://www.nessus.org>)²⁶ is a freeware tool that scans devices for known vulnerabilities. Commercial solutions also exist—if an organization has such tools, they should definitely be used to scan the networked medical devices to better understand their security posture. It is important, however, to understand the type of scan being performed. Some more intrusive scans can actually cause system interruption and should be scheduled to run during off-hours.
- **Risk Assessment.** This requires a vigilant methodology to constantly assess and manage risk. Often this involves a multidisciplinary team that monitors the organization's network and exposure, as well as monitoring and reacting to vulnerabilities identified by such external organizations as CERT.
- **VLANs** should be used to segregate devices that communicate with each other if possible, and limit the access of one group of devices to another, the Internet, or other network devices such as domain controllers with ACLs. Other similar methods include using routed boundaries between networks that contain medical devices and other segments and using ACLs to control traffic. As already noted, the VA has an excellent document that describes its methodology of assessing how systems communicate,¹¹ which can be used by an organization as a starting point. Some institutions have not had much luck in using VLANs, because of either infrastructure limitations or the complexity of the network communications involved with medical devices. Understanding the communication relationships between devices is key to using VLANs as a security control for networked medical devices.
- **Firewalls.** For devices that pose the greatest risk, firewalls or routers with ACLs are necessary to protect the device from compromise. In particular, if the device is critical to life safety, or the device stores ePHI, then it should have some type of firewall, either software or hardware, appropriately configured to restrict traffic to and from the device to only what is absolutely necessary.
- **IDS/IPS.** If the device's means of communicating with the network have been quantified, IDS/IPS can be used to look for abnormal traffic and take action based on the event. For instance, if a medical device only communicates with a small number of hosts, the IDS/IPS sensors should be programmed to look for attempts by the device to contact hosts outside of its normal traffic pattern. Combining IDS/IPS at the edge of a VLAN medical device architecture can provide significant protection and management at a relatively low cost.
- **Change/configuration management.** It is critical that all changes to networked medical devices be recorded in detail. Network maps showing the detailed communications paths, protocols, and ports used by the device are essential to understanding the device's security profile.
- **Proxy servers for Internet connectivity.** A proxy for all Internet connections can significantly improve the security posture, particularly if the proxy server also employs antivirus scanning technology.

- **Executive support.** Executive support for security initiatives is one of the most important factors in being a “best in class” institution. If security is driven from the top down, the security program of the entire enterprise will be significantly stronger. A security-conscious culture goes a long way towards defending against attack.
- **A sound vulnerability management plan is key to defending against attack.** Typically the source of infection is not the medical device, but is instead a compromised workstation or server. Ensuring that the other devices on the network are protected and meet a secure baseline configuration standard will go a long way towards limiting the exposure of the network.

Although providers themselves can, for the most part, safely implement these practices, if there is any doubt as to whether a particular practice or activity will effect the functioning of a medical device, it is best to check with the device manufacturer. Better safe than sorry!

Section 5. UHC Member Approaches to Medical Device Security

Member Stories

As has been illustrated thus far, medical device security is a very important topic for UHC members, and indeed for most of the health care community, yet there is no single, comprehensive solution to the problem. UHC's quest for such a solution included a call to several UHC members to learn what measures they have taken and how well they have succeeded. The response was good, with members anxious to share what has worked for them, learn what has worked for others, and, perhaps most importantly, determine how to work together to develop and work towards a common industry solution. The following stories describe a variety of approaches that have met with varying degrees of success.

Emory Healthcare

Emory Healthcare, like many organizations, is "constantly trying to keep up." Although it has a centralized, well-managed environment, it has thousands of devices running on MS servers and thus is perpetually patching the associated software. Even so, it has had problems with viruses and considers medical devices to be one of the "biggest holes."

Emory employs a risk assessment method to determine where and how to best focus its security efforts. Its devices are broken down into 3 categories: (1) devices for which Emory Healthcare IS owns and controls all aspects, (2) devices that are departmentally owned but with security managed by IS, and (3) vendor-supported medical devices. For the vendor-supported medical devices, Emory mandates security controls but must find creative ways to enforce them.

The Emory Computer Security Incident Response Team plays an important role in Emory's security strategy. One of the team's primary roles is to review industry sources on a daily basis to stay abreast of the current vulnerability and exploit information. Each new potential threat is evaluated and when necessary, a plan is developed to address the threat in the most efficient, least disruptive manner. In addition to checking industry resources daily, Emory also uses the Nessus Vulnerability Scanner to passively scan for vulnerabilities, which, when detected, are promptly reported to the vendor.

Regarding the longer-term industry response to the issue of medical device security, Emory Healthcare would like to focus on exploit prevention. It feels that the best solution is to use host-based intrusion prevention on the medical devices as part of a whole intrusion prevention strategy. Such a strategy would also include network-based intrusion prevention at key network segments.

Loyola University Health System

Loyola University Health System has taken a preemptive approach to medical device security. It has been working with vendors to structure an RFP that puts the onus for device hardening onto the vendor. This includes making sure that the vendor has a timely and robust patch management procedure, as well as ensuring that they include firewalls on their devices. Loyola has even decided that it will not allow unprotected equipment in the door. This strategy has had mixed success with the vendors. Kodak has been the most receptive, even providing an engineer to help the Loyola team evaluate all the ports used by the picture archiving and communication system (PACS) and eliminate unnecessary ports.

Loyola has also employed isolation as a strategy using various methods. It has created a VLAN specifically for PACS. It has locked down the desktops using Citrix thin-client Win terminals, which are less prone to infection. It has implemented an SSL-based VPN, a limited conduit that allows physicians to dial in remotely and invoke a Citrix session. Loyola uses proxy servers to filter or limit Internet access, using a 3-tier system of nonclinical users, clinical users, and academic users. The Internet access rules are very strict for the clinical Computers on Wheels (COWS), and slightly less strict for the nursing stations.

University of Colorado

The University of Colorado also uses a preemptive approach to securing medical devices. In its experience, it often finds server operating systems running on desktop class hardware in medical devices, as well as out-of-date or unsupported software such as NT 4.0.

The University of Colorado risk rates all the devices in its network using the O/S as the first cut. If the device is Windows based, it receives more scrutiny than a Unix or proprietary device. For Windows-based devices it analyzes what version of Windows is used, whether the devices use antivirus protection, and the amount of hardening the manufacturer has performed. Its last resort is to firewall the device from the rest of the network and only allow necessary traffic to and from the device. Unix-based devices are also rated based on the hardening level; however, because the Unix O/S is less vulnerable than Windows, the University of Colorado is more concerned with unnecessary services than the threat of malware compromise.

Overall, the University of Colorado has found that the major vendors are willing to work with them on securing devices, but the smaller “mom and pop” shops are more reluctant to engage in security discussions. If a firewall is deemed necessary, the University of Colorado requires the vendor to pay the cost of the equipment.

University of Virginia Health System

The University of Virginia Health System feels that “information is our biggest weapon.” It makes a point of knowing as much as it can about every device on its network, starting with the RFP, which includes a hospital security survey that is based on the NCHICA vendor RFP template for meeting HIPAA security requirements. Devices that do not conform to standard security practices require an exception form describing the deviation and are put on a special watch list. One example includes a system that cannot run standard antivirus software because the vendor-modified core operating system dynamic link libraries (DLLs) and the antivirus software are no longer compatible. If a problem is detected with any of these devices, the device is immediately shut down until the appropriate remedy can be applied. Approximately 60 devices (out of more than 200) are currently on the watch list.

In keeping with its “information is knowledge” belief, the University of Virginia is constantly scanning the system for rogue devices (devices outside the control of the enterprise). These may include unauthorized devices or devices that do not conform to expectations (such as when a vendor unplugs a device and puts it in a new port). Again, in these cases the intervention is to shut down the port until the appropriate security measures can be taken.

Member Approaches Summary

UHC members have employed a variety of approaches to resolve the issues surrounding medical device security. These include preemptive approaches (working with the vendor to understand and harden the device); isolation techniques (using firewalls and VPNs); and proactive measures (looking for potential problems by keeping abreast of industry-identified vulnerabilities and actively scanning the network for intruders).

No one approach is distinctly better than another and all are probably necessary to ensure maximum security for medical devices. The single common theme is that health care organizations cannot rely on medical device manufacturers and vendors to fully own or resolve the issue; they must assume the responsibility themselves.

Section 6. Resources and Current Initiatives

Although arguably more vested in it, health care organizations are not alone in the struggle to secure medical devices. Several industry groups have attempted to address the problem. Following is a list of industry groups that offer reporting mechanisms and/or white papers. Health care vendors also are not indifferent to the problem. Several offer informative Web pages citing vulnerabilities and potential solutions; these are also highlighted in this section.

Industry Groups

ECRI (formerly the Emergency Care Research Institute)

<http://www.ecri.org/>

ECRI is a nonprofit health services research agency whose mission is to improve the safety, quality, and cost effectiveness of health care. ECRI's services alert readers to technology-related hazards; disseminate the results of medical product evaluations and technology assessments; provide expert advice on technology acquisitions, staffing, and management; report on hazardous materials management policy and practices; and supply authoritative information on risk control in health care facilities and on clinical practice guidelines and standards.

For more than 30 years, ECRI has gathered and investigated reports of incidents involving medical devices from health care providers, patients, and manufacturers. As a result of ECRI's investigations, many manufacturers have recalled or modified their devices. Although membership is required to access some of ECRI's more sophisticated alert and reporting capabilities, ECRI provides a vehicle where nonmembers can report medical device problems at http://www.ecri.org/Problem_Reporting/Reporting_Options.aspx.

Healthcare Information and Management Systems Society (HIMSS)

http://www.himss.org/ASP/topics_medicalDevice.asp

HIMSS has formed a Medical Device Security Workgroup whose purpose is to:

- Identify both the security issues associated with medical devices and systems and the *best practices* for addressing those issues
- Evaluate the issues of security threats and vulnerabilities that affect medical devices, the provider's and the equipment manufacturer's responses and responsibilities, and the legal and regulatory framework in which these issues must be addressed
- Coordinate with similar groups and committees to capitalize on existing efforts and realize the economies of collaboration
- Prepare and endorse white papers, guidance documents, comments, and recommendations on medical device security issues and practices for addressing those issues
- Educate HIMSS membership and the industry about the implications of medical device security through publications, tools, resources, and educational programs

The workgroup has created a standard Manufacturer Disclosure Statement for Medical Device Security (MDS²). The intent of the MDS² is to supply health care providers with important information that can help them assess the vulnerability and risks associated with ePHI transmitted or maintained by medical devices. The form is endorsed by the HIMSS, ACCE, ECRI, and NEMA, and is available at <http://www.himss.org/content/files/MDS2FormInstructions.pdf>.

National Electrical Manufacturers Association (NEMA)

<http://www.nema.org/>

NEMA provides a forum for the:

- Development of technical standards that are in the best interests of the industry and the users of its products
- Establishment and advocacy of industry policies on legislative and regulatory matters that might affect the industry and those it serves
- Collection, analysis, and dissemination of industry data

NEMA, along with the European Coordination Committee of the Radiological and Electromedical Industry (COCIR), and the Japanese Industries Association of Radiological Systems (JIRA), are part of an international committee of industry representatives that are taking a more holistic approach to security and privacy enforcement in the increasingly digital world of medical imaging. The joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)²⁷ is charged with examining all systems, devices, components, and accessories related to medical imaging informatics that access, contain, and/or process patient information. Committee members must devise ways of ensuring that these devices maintain certain basic security rules. In December 2003, the committee released a paper entitled *Defending Medical Information Systems Against Malicious Software*²⁸ which is available at <http://www.nema.org/prod/med/upload/medical-defending.pdf>.

The workgroup also developed a white paper entitled, *Patching Off-the-Shelf Software Used in Medical Information Systems*,²⁹ which is available at http://www.himss.org/content/files/Patching_OffTheShelfSoftware_Used_in_MedIS_October_2004.pdf.

Finally, the workgroup recently sent a memo to the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality regarding the impact of the HIPAA Security Rule regulations on medical device security.³⁰ The memo contains recommendations for (1) an immediate education action by the government, and (2) an adjustment to the HIPAA Security Rule to use a phased enforcement to:

- Require all covered entities to complete risk management planning on all devices that contain PHI
- Demonstrate completion of first-round mitigations and the establishment of subsequent targets
- Demonstrate progress in meeting or exceeding security targets
- Provide continuing evidence of the growth and sustainability of security programs for device compliance

North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)

<http://www.nchica.org/>

NCHICA is a nonprofit consortium of more than 250 organizations dedicated to improving health care by accelerating the adoption of information technology. The NCHICA's Board of Directors formed a HIPAA Implementation Planning Task Force in 1999 to develop an overall strategy to help the health care community reach compliance with the HIPAA regulations. Among the workgroups formed by this task force is a security workgroup that has developed the NCHICA Vendor RFP Template for Meeting HIPAA Security Requirements. Although designed with HIPAA specifications in mind, this form provides a good prototype for a medical device security checklist and is used by the University of Virginia Health System as part of its RFP process for medical device vendors. This form may be downloaded from <http://www.nchica.org/HIPAAResources/Samples/VendorSecurityMatrix.doc>.

Vendors

GE Healthcare

http://apps.gehealthcare.com/product_security/protection/prod_sec_home.html

GE Healthcare offers a Web site that contains a matrix of technically significant operating system vulnerabilities for all GE Healthcare-delivered operating systems. Each vulnerability has an associated response. The responses vary between vulnerabilities and in most cases require no immediate action. The site also contains a matrix of potential product vulnerabilities along with update procedures and remediation timelines, if available. If the fix is relatively easy, such as requiring only a simple load of software, customers are allowed to apply the fix themselves. Some patches are more involved and require direct GE Healthcare assistance. Patches requiring additional on-site assistance are installed at hourly-billed service rates for all customers. The GE vulnerability matrix may be viewed at http://apps.gehealthcare.com/product_security/protection/vulnerability_updates.html.

GE Healthcare performs rigorous testing to ensure that systems meet stringent reliability and performance standards and will not be accountable for any issues caused by any patches loaded from a "non-GE" source. Additionally, GE does not allow antivirus software to be loaded on its products without explicit approval. GE encourages its customers to use a "defense in depth" philosophy by applying external controls such as firewalls, layer 3 switches, and VLANs to restrict network access to medical equipment.

Kodak

<http://www.kodak.com/global/en/health/privacy/priSecMain.jhtml?pq-path=5371#wht>

Kodak has been identified by UHC members as one of the more proactive vendors regarding medical device security. Kodak's interpretation of FDA regulations notes that "medical systems are FDA regulated to assure patient safety and system performance. This requires Kodak to qualify changes to them following our QA process before we can install or recommend changes for installation for medical systems in the field. This includes all system changes, patches, updates, and enhancements."

Kodak health imaging staff monitors, analyzes, and provides security updates based on US-CERT alerts, Microsoft security bulletins, and the DoD information assurance vulnerability alert (IAVA) for Kodak's digital capture, digital output, and health care information systems. This is managed by Kodak's network vulnerability process (NVP) to provide a timely risk analysis. The Kodak Malware Quick Action Teams

(MQAT) provide predictable software updates to resolve security vulnerabilities (e.g., viruses and hacker attacks) for Kodak systems. Kodak's health imaging security bulletins can be viewed at <http://www.kodak.com/global/en/health/malware/malwareMain.jhtml>.

Philips Medical Systems

<http://www.medical.philips.com/us>

Philips Medical Systems' approach to medical device security is driven by customer need and the application of governmental (e.g., FDA) regulations. To that end, it has created a global network of Product Security Incident Response Teams to collect and manage information and address vulnerabilities that affect Philips' products and solutions. Philips' goal is for the appropriate team to evaluate each real or potential breach with an explicit threat/vulnerability/risk assessment and develop and implement vulnerability response plans.

Most Philips equipment does not permit any third-party software installation of any kind by the customer—for example, virus scanners, systems patches, or on-platform firewalls—without prior written consent. When it does authorize the use of virus scanners, system patches, or upgrades on a particular system, installation is carried out either by Philips Medical Systems at the time of manufacture or by a qualified Philips field service engineer.

Section 7. Conclusion

Medical device security is a significant issue for health care organizations. Medical devices have been breached by malware such as worms and viruses and continue to risk exposure because of a variety of factors. These factors, contrary to popular belief, are not the direct result of FDA regulations and red tape, but rather are related to the complex and sensitive nature of the devices themselves.

Simply put, medical devices deal with critical data that can directly influence patient care. The very nature of the data imposes a higher degree of caution when modifying the medical device software or the associated operating system. As a result, any security patches that must be applied should be accompanied by thorough testing of the device to make sure that it still functions correctly. Although the FDA regulations impose this requirement on manufacturers, it is something that vendors and providers alike should insist on regardless. The primary issues therefore relate not to who is imposing the testing requirement, but to what testing should be performed, how quickly the testing can be accomplished, who is actually responsible for testing, and who is responsible for implementing the patch. These are questions that can and should be resolved through contract language.

Securing medical devices involves much more than patch management, which, although important, is a reactive measure. There are a variety of system techniques and mechanisms that can be employed to harden devices and minimize exposure to malware. Likewise, there are utilities that can be used to detect breaches and actively look for rogue devices. Not all of these solutions require vendor permission and/or intervention and therefore can (and should) be implemented by the provider. In other cases, providers should work closely with the manufacturers, pushing them to make the changes necessary to secure their devices (this too can be done contractually). When in doubt about the impact of a security tool or intervention on a medical device, consult the manufacturer.

Regardless of what the solutions are or who actually implements them, an organization needs to have a strong commitment to security, starting with senior management. Policies, procedures, and contingency plans need to be thoroughly defined and documented. A strong communication mechanism also needs to be in place to keep all of the stakeholders apprised of a situation or potential problem.

A variety of approaches to medical device security have been presented in this paper including the definition and designation of responsibilities, potential points within contract language, and actual system solutions that can be implemented either at the network or at the device level. No single solution stands out over the others and all the solutions have merit. The unfortunate truth is that as long as there are computers, there will be potential for compromise. A combination of approaches is necessary to achieve the maximum level of security required for most medical devices and because of the ever-changing environment in which we live, the job will never be truly finished.

The real conclusion to be drawn from this paper is that it is ultimately up to the provider organization to make sure that the appropriate safeguards are in place. The FDA is limited in what it can enforce through regulation. Vendors are not indifferent to the issue but arguably have less invested than providers, making medical device security a lower priority for them. Industry groups can influence but not enforce policy. Providers need to keep doing what they are doing: implementing their own measures to the extent that they can and collaborating with each other to define industry standards and collectively influence vendors to take on more responsibility for medical device security.

Appendix A. FDA Medical Device Reporting

Mandatory Reporting

The medical device reporting (MDR) regulation³¹ became effective on July 31, 1996. The MDR regulation provides a mechanism for the FDA to identify and monitor significant adverse events involving medical devices. The goals are to detect and correct problems in a timely manner.³² The statutory authority for the MDR regulation is section 519 of the FD&C Act as amended by the Safe Medical Devices Act (SMDA) of 1990.

User facilities such as hospitals and nursing homes are legally required to report suspected medical device-related deaths to both the FDA and the manufacturer, if known, and serious injuries to the manufacturer, or to the FDA if the manufacturer is unknown. The reports must be made on the MedWatch³³ 3500A Mandatory Reporting Form.³⁴ The form, unfortunately, cannot be submitted electronically.

Voluntary Reporting

The problem with mandatory reporting is that it is limited. Reports are required only if a medical device is suspected of causing a death or serious injury (i.e., it is more reactive than proactive). The mandatory mechanism also applies to manufacturers and institutions, rather than to consumers and health care professionals (the distinction in reporting being between an institution versus an individual).

The FDA offers a means through MedWatch to voluntarily report serious adverse events, product problems, and medication errors that are suspected to be associated with use of an FDA-regulated drug, biologic, device, or dietary supplement. In fact, to keep effective drugs and devices on the market, the FDA relies on the voluntary reporting of these events. The FDA uses the data to maintain a safety surveillance of all FDA-regulated products. A voluntary report may be the action that prompts a modification in the use or design of a product, improving its safety profile and leading to increased patient safety. In the case of medical device security, a sufficient quantity of reports related to the effect of malware on medical devices will encourage, if not empower, the FDA to take affirmative action with the device manufacturers regarding the implementation of security measures.

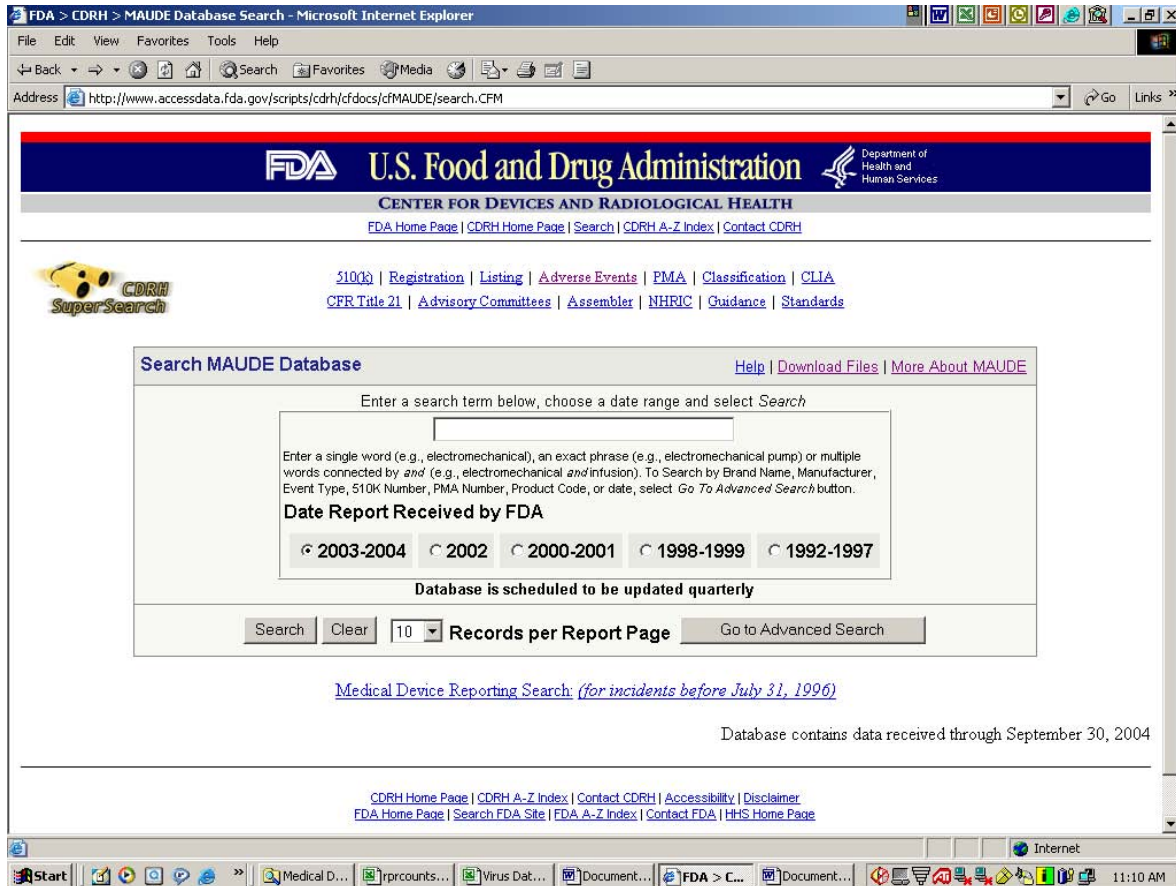
There are 3 ways to submit a voluntary report to MedWatch:

- The form may be completed online (<https://www.accessdata.fda.gov/scripts/medwatch/>)
- The report may be submitted by telephone: 1-800-FDA-1088
- The form may be downloaded, completed, and faxed or mailed to the FDA (<http://www.fda.gov/medwatch/getforms.htm>)

Reporting Databases

The FDA's Center for Devices and Radiological Health Web site offers 2 online databases that contain medical device reports.³⁶ The MDR data include mandatory manufacturer reports on devices that may have malfunctioned or caused a death or serious injury. These reports were received under both the mandatory MDR Program from 1984 to 1996, and voluntary reports up to June 1993. There are more

than 600,000 reports. The Manufacturer User Facility and Distributor Experience database (MAUDE) consists of all voluntary reports since June 1993, user facility reports since 1991, distributor reports since 1993, and manufacturer reports since August 1996. Both databases are searchable by key words, phrases, brand name, manufacturer, event type, 510K number, PMA number, product code, or date. A search for "SASSER" in the MAUDE database yielded the following results:



New Search			Help Download Files More About MAUDE
Manufacturer	Brand Name	Date Report Received	
PHILIPS MEDICAL SYST	XCELERA IM WORKSTATI	05/26/2004	
EASTMAN KODAK CO.	DIRECTVIEW CR SYSTEM	05/26/2004	
EASTMAN KODAK CO.	DIRECTVIEW CR SYSTEM	05/26/2004	

Although there is much anecdotal evidence that suggests that the SASSER worm adversely affected many organizations and a variety of medical devices, only 3 reports were submitted to the FDA.

Medical Product Surveillance Network (MedSun)

The Medical Product Surveillance Network (MedSun)³⁷ is a pilot program launched in 2002 by the U.S. FDA's CDRH. The primary goals of MedSun are to identify, understand, and share information about problems regarding medical devices. MedSun plays an important role in the FDA's post market surveillance effort.

As already noted, hospitals, nursing homes, and other health care facilities are required to report medical device problems under the SMDA using the MedWatch 3500A form. MedSun provides a secure, Internet-based data entry system that automates this process and helps gather other additional data that can help FDA, device manufacturers, and clinical facilities proactively address safety concerns before serious injuries or deaths occur.

Currently, 280 hospitals and nursing homes participate in the MedSun. The selection of these facilities was based on a number of factors including the size and location of the organizations, as well as their willingness to participate by submitting reports to the MedSun system. In 2005, the project will expand to more than 300 facilities throughout the continental United States. More information on program participation can be found on the MedSun Web site at <https://www.medsun.net/about.html>.

References

1. Carnegie Mellon Software Engineering Institute CERT Coordination Center OCTAVE Web site. Available at: <http://www.cert.org/octave/>.
2. Carnegie Mellon Software Engineering Institute CERT Coordination Center Web site. Available at: <http://www.cert.org/>.
3. Microsoft TechNet. The security risk management guide. October 15, 2004. Available at: <http://www.microsoft.com/technet/security/guidance/secrisk/default.aspx>. Accessed December 1, 2004.
4. Food and Drug Administration Web site. Code of federal regulations: title 21, volume 8. April 1, 2004. Available at: <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=820&showFR=1>. Accessed November 2, 2004.
5. Medical device exemptions 510(k) and GMP requirements. Available at: <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpd/315.cfm>. Accessed November 14, 2004.
6. Food and Drug Administration Web site. Classify your medical device. Available at: <http://www.fda.gov/cdrh/devadvice/313.html>. Accessed November 14, 2004.
7. Code of federal regulations. When a premarket notification is required. Available at: http://a257.g.akamaitech.net/7/257/2422/12feb20041500/edocket.access.gpo.gov/cfr_2004/aprqr/pdf/21cfr807.81.pdf. Accessed November 14, 2004.
8. Code of federal regulations. Quality system regulation. Available at: http://a257.g.akamaitech.net/7/257/2422/12feb20041500/edocket.access.gpo.gov/cfr_2004/aprqr/pdf/21cfr820.30.pdf. Accessed November 14, 2004.
9. Code of federal regulations. Indications for Use. Available at: http://a257.g.akamaitech.net/7/257/2422/12feb20041500/edocket.access.gpo.gov/cfr_2004/aprqr/pdf/21cfr814.20.pdf. Accessed November 14, 2004.
10. Food and Drug Administration Web site. Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. January 14, 2005. Available at: <http://www.fda.gov/cdrh/comp/guidance/1553.html>. Accessed January 26, 2005.
11. Department of Veterans Affairs. Medical device isolation architecture guide. April 30, 2004. Published by Center for Engineering & Occupational Safety and Health (CEOSH), St. Louis, MO in conjunction with the Department of Veterans Affairs and Veterans Health Administration, Washington, DC. Available at: http://www.nwfusion.com/news/2004/VA_VLAN_Guide_040430.pdf. Accessed November 15, 2004.
12. Webopedia Web site. Available at: <http://www.webopedia.com>.

13. Department of Health and Human Services' Web site. 45 CFR parts 160, 162, and 164. Health insurance reform: security standards; final rule. February 20, 2003. Available at: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf>. Accessed November 20, 2004.
14. Ohlhorst FJ, Randazzese VA. Windows XP Service Pack 2: install with care. July 23, 2004. CRN. Available at: <http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=23905071>. Accessed November 17, 2004.
15. NCHICA Web site. Available at: <http://www.nchica.org>.
16. NCHICA Privacy & Security Officials Work Group. NCHICA vendor RFP template for meeting HIPAA security requirements. August 8, 2003 Available at: <http://www.nchica.org/HIPAAResources/Samples/VendorSecurityMatrix.doc>. Accessed November 20, 2004.
17. Manufacturer disclosure statement for medical device security–MDS². Available at: <http://www.himss.org/content/files/MDS2FormInstructions.pdf>. Accessed December 27, 2004.
18. HIMSS Medical Device Security Workgroup Web site. Available at: http://www.himss.org/ASP/topics_medicalDevice.asp.
19. American College of Clinical Engineering (ACCE) Web site. Available at: <http://www.accenet.org/>.
20. ECRI Web site. Available at: <http://www.ecri.org/>.
21. National Electrical Manufacturers Association (NEMA) Web site. Available at: <http://www.nema.org/>.
22. ECRI Web site. Order form for Information Security for Biomedical Technology: A HIPAA Compliance Guide. Available at http://www.ecri.org/Products_and_Services/Products/HIPAA_Compliance_Guide/HIPAAcdromBROpdf.pdf. Accessed November 16, 2004.
23. Department of Defense Web site. Instruction number 8500.2 subject: information assurance (IA) implementation. February 6, 2003. Available at: http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf. Accessed November 2, 2004.
24. Insecure.org Nmap Security Web site. Available at: <http://www.insecure.org/>.
25. Ethereal Web site. Available at: <http://www.ethereal.com/>.
26. Nessus Open Source Web site: Available at: <http://www.nessus.org/>.
27. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC) Web site. Available at: <http://www.nema.org/prod/med/security/>.
28. Joint NEMA/COCIR/JIRA SPC. Defending medical information systems against malicious software. December 2003. Available at: <http://www.nema.org/prod/med/upload/medical-defending.pdf>. Accessed December 5, 2004.

29. Joint NEMA/COCIR/JIRA SPC. Patching off-the-shelf software used in medical information systems. October 2004. Available at: http://www.himss.org/content/files/Patching_OffTheShelfSoftware_Used_in_MedIS_October_2004.pdf. Accessed December 29, 2004.
30. Joint NEMA/COCIR/JIRA SPC Memo to the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality regarding Impact of the HIPAA Security Rule regulations on medical device security. Available at: <http://www.ncvhs.hhs.gov/041119p3.pdf>. Accessed January 26, 2005.
31. Code of federal regulations. Part 803 Medical device report. Available at: <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcr/CFRSearch.cfm?CFRPart=803&showFR=1>. Accessed December 15, 2004.
32. Division of Small Manufacturers Assistance Office of Health and Industry Programs. Medical device reporting for manufacturers. March 1997. Available at: <http://www.fda.gov/cdrh/manual/mdrman.pdf>. Accessed December 10, 2004.
33. MedWatch–The FDA Safety Information and Adverse Event Reporting Program Home Page. Available at: <http://www.fda.gov/medwatch/index.html>. Accessed December 10, 2004.
34. U.S. Department of Health and Human Services–FDA CDRH. MedWatch reporting forms. Available at: <http://www.fda.gov/medwatch/getforms.htm>. Accessed December 10, 2004.
35. U.S. Department of Health and Human Services–FDA CDRH. MedWatch online voluntary reporting form (3500). Available at: <https://www.accessdata.fda.gov/scripts/medwatch/>. Accessed December 10, 2004.
36. U.S. Department of Health and Human Services–FDA CDRH. Adverse event reporting data files. Available at: <http://www.fda.gov/cdrh/mdr/mdr-file-general.html>. Accessed November 2, 2004.
37. Medical Product Surveillance Network (MedSun) Web site. Available at: <https://www.medsun.net/about.html>.