Global Information Assurance Certification Paper

Securing Medical Devices in the Healthcare Environments

SANS Security Essential

GSEC Practical Assignment

Version 1.3 (amended December 12, 2001)

March 1, 2002

Cuong Le

TABLE OF CONTENTS

1 ABSTRACT

In the United States (U.S.) Healthcare industry, medical devices* are equipment that consists of software, hardware or a combination of both. The Food and Drug Administration (FDA) subjects medical devices to regulatory requirements. At this time, these FDA regulatory mandates have resulted in conflicts to the security policies set forth by many individual healthcare institutions. This paper discusses the security for medical devices within healthcare environments.

* For more information regarding medical devices and FDA regulatory requirements please refer to appendix A – Medical Devices and FDA Regulatory Requirements.

2 INTRODUCTION

The fast changing pace of today's business landscape and increasing financial pressures is influencing moves toward more sophisticated and connected business models. The Internet is seen as the universal network, the Holy Grail to every problem. It brings unique opportunities, challenges as well as threats to any systems connected to it. The Internet allows the U.S. Healthcare industry to be more efficient, lower transactional and operational costs while providing better presence and service to its customers, partners, and physicians. Yet, leveraging an open network such as the Internet also raises concerns about the privacy, integrity, and availability of patient information. As healthcare organizations strive to leverage the Internet, they need to deploy security architectures to meet government regulations and ensure the trust of patients.

The U.S. Healthcare industry is large and complex. Its organizations are diverse and the technology gaps between organizations are vast, from proprietary solutions to limited standardization. In addition, it is both cost and time prohibitive for the manufacturers of healthcare systems and medical devices to incorporate the constantly changing security updates as well as meet the FDA's rigorous regulatory requirements. These coupled with the fact- that there are limited regulatory pressures for information security, has left U.S. Healthcare far behind other industries.

This paper discusses the security for the medical devices as defined in appendix A. However, due to time constraints and the vast number of systems and medical devices used in the U.S. Healthcare industry, this paper will be focused on the software related medical devices and their security within the U.S. Healthcare industry.

3 Problem Statement

Studies by the FDA indicate that:

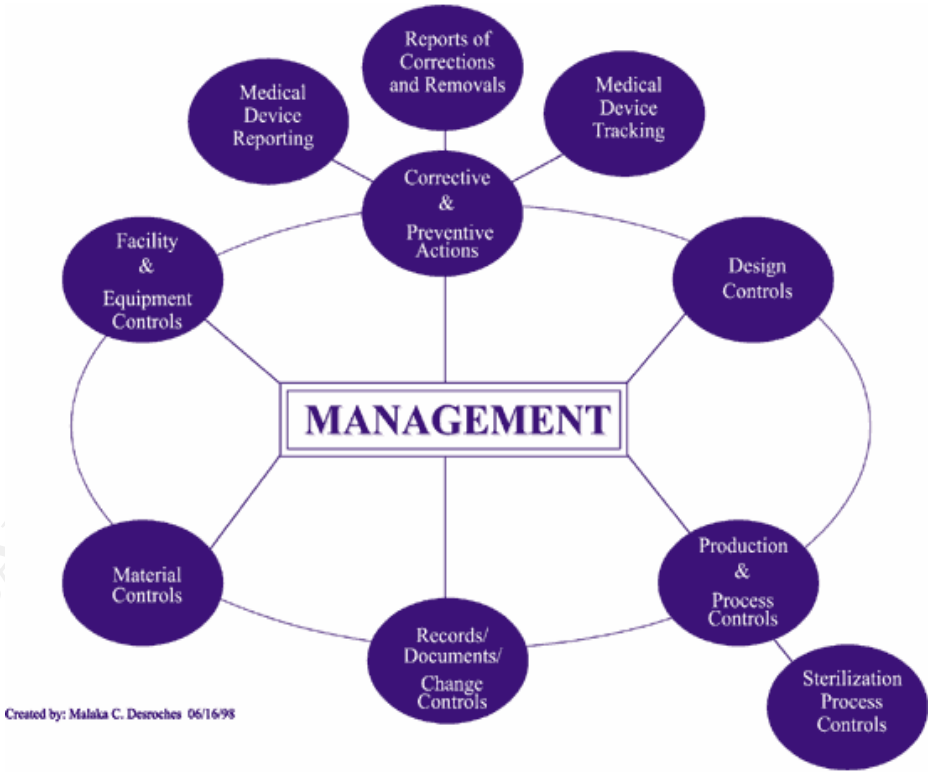
"A subsequent study of software-related recalls for the period of fiscal year (FY) 1983 through FY 1991 indicated that over 90 percent of all software-

related device failures were due to design-related errors, generally, the failure to validate software prior to routine production" [4].

Consequently, the FDA uses its own quality control inspection process to review and approve medical devices. Figure 3-1 depicts the high-level inspection process flow that the FDA field staff may use to assess a medical device manufacturer's compliance with the Quality System Regulation and related regulations. The new inspection process is known as the "Quality System Inspection Technique" or "QSIT". Field investigators may conduct an efficient and effective comprehensive inspection using this guidance material that will help them focus on key elements of a firm's quality system.

As illustrated in Figure 3-1 and in the Guide to Inspections of Quality Systems, device manufacturers are subjected to a vigorous control process to ensure compliance to FDA regulatory requirements as they introduce new medical devices or alter existing ones. As a result, these FDA requirements would prohibit the manufacturers to release new and/or revised medical devices in a timely manner.

Figure 3-1: Quality Control Inspection Process



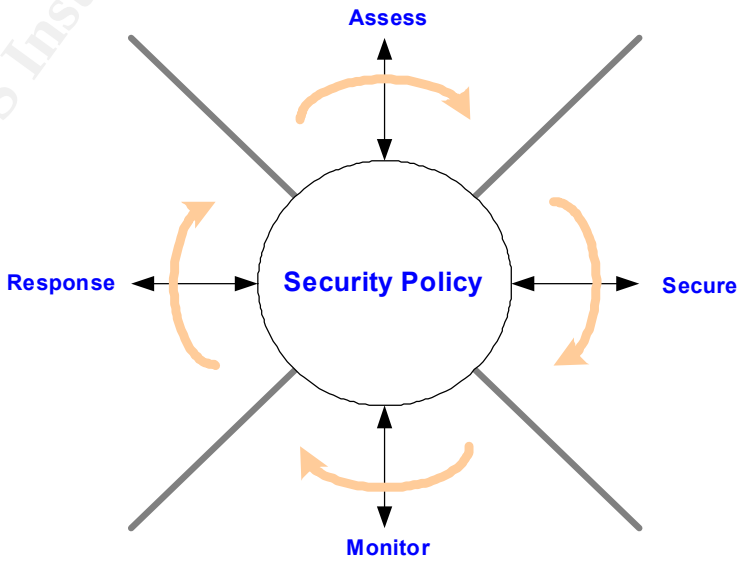
Hardware and operating systems such as Unix, Windows NT, or others typically host software components of medical devices. The release cycles for the operating system patches, security patches, and anti-virus software patches are measured in terms of days and/or months. The anti-virus definition files are rolled out in a matter of day(s). While it would take the medical device manufactures months to perform verification and validation on their products to ensure compliance with the FDA regulatory requirements and - undergo its review and approval process. It is not economical, practical nor possible for the device manufactures to keep up with the fast changing pace of the IT security environments and still comply with the FDA.

So, what are the issues here? It is clear that we have a healthcare IT security policy vs. government regulatory dilemma. If the medical device manufacturers violate the FDA regulatory requirements, their products can be pulled off the market. In this case, it would be a financial impact for the manufacturers resulting in a lack of medical devices for the healthcare institutions, and further resulting in the possible reduction of the best care for their patients. On the other hand, if the medical device manufacturers do not meet healthcare institutions' security policies, their products can also be pulled out; thus creating similar consequences.

4 A Fundamental Approach

The fundamental approach to resolve the identified problems is to follow a risk management methodology. According to Network Computing [12], risk management should be an ongoing activity that includes phases for assessing risk, implementing controls, promoting awareness and monitoring effectiveness. Each healthcare organization will have to assess its own risks to best fit its requirements and needs. The risk management life cycle is depicted in the following diagram:

Figure 4.1: Risk Management Life Cycle



Each step in the risk management life cycle will be discussed as follows:

4.1 Security Policy

Every organization should have a security policy to protect its resources: people, information, and assets. It's even more of a reason to have security policy when connecting your business to the Internet. However, it is not the scope of this paper to discuss how to develop a security policy, but rather assume that a security policy exists for healthcare organizations. Although, when evaluating medical devices' compliance against the organization's security policy, it is important to understand the various types of policies available within one's organization so that the appropriate policy can be amended, revised, or developed if it does not exist:

- Program policy that sets the overall tone of an organization's security approach
- Issue-specific policy is intended to address specific needs within an organization
- System-specific policy that addresses system(s) with specific functions that can't be governed by an umbrella policy [9].

In the context of this discussion, if the issue-specific policy calls for all systems connected to the network to install anti-virus software with frequent updates of the virus definition files, and the medical devices may not be able to comply with this particular policy. Each organization will have to determine whether to revise the issue-specific policy to exclude the medical devices or develop a system-specific policy to allow the medical devices to function within a segregate protected network environment.

4.2 Assess

At the heart of risk management is the evaluation of the potential impact of threats on the ability of a company to continue providing products or services to customers. This evaluation phase of the process is risk assessment. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. SANS' risk analysis consists of the following steps:

1. Threat Assessment and Analysis. (Protected against what?)
2. Assets Identification and Valuation. (What must be protected?)
3. Vulnerability Analysis. (What are the potential ways in which threats can be realized?)
4. Risk Evaluation. (What is the probability of vulnerability?)
5. Interim Report

1. Threat Assessment and Analysis

Once connected to the Internet, the medical devices in the hospitals or the like will be subjected to all threat vectors: outsider attack from network and

telephone, insider attack from local network and local system, and attack from malicious code. Once medical devices are compromised, they can become insider threats to other systems on the same network.

2. Asset Identification and Valuation

To the hospital administrators, the assets include employees, clinicians, patient information, IT infrastructures, and physical buildings. Most of the assets are tangible items that the hospitals can associate values to them with the exception of the patient information. To the clinicians, the assets would be the patient information in which patient's confidentiality, integrity, and availability are important. These are intangible items that are subjected to the clinicians and hospital administration's interpretation. Each organization will have to decide how to assign value to a person's life or his/her confidentiality.

3. Vulnerability Analysis

Medical devices are especially vulnerable since it's not currently possible for them to be kept updated as frequently as new OS and security patches to counter new hacks and new malicious code that appear on the Internet on the daily basis. Their vulnerability can be accounted in details by running a vulnerability-scanning tool or manually inspected by using checklist(s) from best practices.

Today, there are many tools available to assist organizations in identifying their vulnerability. A list of ***free and commercial vulnerability scanners and their detection results*** can be found at http://img.cmpnet.com/nc/1201/ graphics/ f1-detect-results.pdf. Free benchmark and scoring tools for Windows 2000, Solaris, and other systems can be found at www.cisecurity.org. Microsoft Personal Security Advisor (MPSA) is an easy to use Web application that will help you secure your Windows NT 4.0 or Windows 2000. MPSA will scan your system and build a customized report on items such as: missing security patches, weak passwords, Internet Explorer and Outlook Express security settings, and Office macro protection settings.

Organizations can also use best practices for vulnerability analysis such as:

- Those at the Naval Surface Warfare Center web site [7]. Some specific risk assessment forms are: Windows NT, Windows 2000 , Unix Accreditation Form Part 2, Generic Accreditation Form Part 2 (for architectures not covered elsewhere), Network Risk Assessment Form Part 2.
- Microsoft offers free baseline security checklist for Windows products at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/content.asp
- NSA Guideline for Securing Windows NT [13].
- SANS offers Windows 2000, NT, and Unix security checklist and guides at its store, www.sanstore.org

There are many other vulnerability scanners and benchmarking tools on the Internet. However, it is not the intention of this paper to provide an exhaustive list of vulnerability scanner tools.

4. Risk Evaluation

It is up to each organization to decide whether they will accept, mitigate, or transfer each risk. If the organizations are not willing to accept the risks, then they can remove those medical devices from their environments and there is no need to discuss further. In the context of medical devices and patient care, the integrity of patient data is probably the most important factor as it may result in a life or death situation. Hospitals typically have good processes and procedures for dealing with patient data's confidentiality (celebrities have to deal with this all the time) and availability (good backup processes and procedures help).

Risk = (Threats * Vulnerability) / Countermeasures

To reduce risk, one has to both diminish the threats by increasing countermeasures and reduce the vulnerability by way of vulnerability patching* or reduce the vulnerability by way of OS and security patches, which is more of a problematic approach due to FDA regulatory requirements.

*Vulnerability patching is the process of turning off all unused services.

5. Interim Report

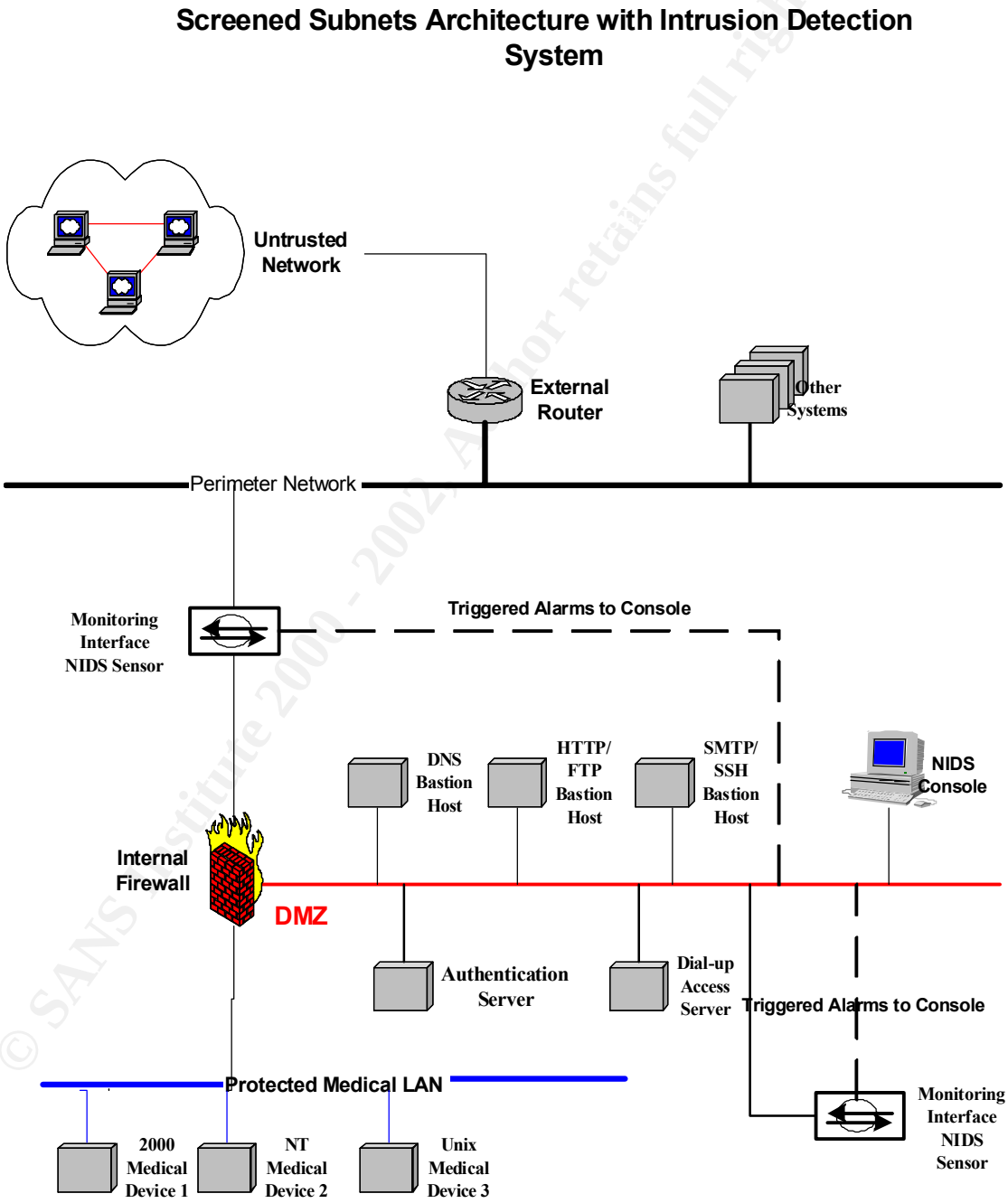
The interim report should consist of the information learned from step 1-4. It should also include a preliminary plan for short and long term solutions. Each of the alternatives should have pro and con with associated cost benefit analysis. In this scenario, the preliminary plan for the short-term solution could be either to remove the medical devices from the network, or to introduce some countermeasures that would reduce the risks while waiting for a longer-term solution to be developed. The long-term solutions could be either to revise the security policy to make special provisions for medical devices and/or to work with the device manufactures and FDA to improve the product release cycles.

4.3 Secure

As identified in the previous section, the medical devices are subjected to all kinds of threats. The focus of this section is to design a secured infrastructure for medical devices within hospitals or the like, by ways of prevention and negation. Several countermeasures that are used, as part of the overall solution, will be described following Figure 4-2 below:

Figure 4-2 is based on the screen-subnet architecture from Building Internet Firewall [10], and the network intrusion detection concepts from Cisco Secure Intrusion Detection System [8].

Figure 4-2:



Legend: — — — · **= special communication to NIDS console**

1. **External Router**

   To protect both the perimeter net and the internal net from the Internet, a router or firewall can be used. The router needs to block any incoming packets from the Internet that have forged source address. Another task for the router is to prevent IP packets containing inappropriate addresses from leaving the hospital networks. All traffic leaving the hospital networks should come from one of their valid addresses. Otherwise, either the hospitals have serious configuration problems or somebody is forging source addresses. This does not provide additional network protection, but as a good network citizen one needs to filter inappropriate outbound source addresses to prevent one's system from being used by intruders to launch attacks on other sites. This is countermeasure number 1.

2. **Network Intrusion Detection System (NIDS)**

   Since medical devices are vulnerable due to the lack of latest OS and security patches, the NIDS is suggested here to locate attacks on the network in a preventive manner. The NIDS sniffs the network packets and compares the traffic against signatures for known intrusive activity. The NIDS solution considered here is a signature-based hardware and software combined solution. A sensor performs real-time monitoring of network traffic. It will reassemble network packets, if necessary, and compare against a signature indicating typical intrusion activity. If an attack is detected, the sensor logs the attack and notifies a central Console. The Console displays the alarms, logs the data, and takes proper action on attacks detected by a sensor. Sensor(s) can be programmed for automatic responses such as TCP reset, IP blocking and logging. Since the NIDS runs on its own hardware and software, new signatures can be updated to prevent new attacks.

   Similar offering of a signature-base NIDS can be found at ISS RealSecure IDS [14]. NIDS solution is countermeasure number 2.

3. **Internal Firewall**

   In the Screen Subnet Architecture the internal firewall protects the internal Medical LAN both from the Internet and from the perimeter network. This is where each hospital will have to determine its policy for inbound and outbound traffic base on its own needs, capabilities, and constraints; there is no one answer for all sites. The internal firewall should also be configured to prevent the internal LAN from the perimeter net in the event that the internal LAN is compromised. Considerations must be given to the services between the internal net and the perimeter net, the internal net and the DMZ where bastion hosts reside. This is countermeasure number 3.

4. **Bastion Hosts**

The bastion hosts recommended here are intended to function as proxy servers. Proxying provides the Internet access or access from the perimeter net to a small number of hosts, while appearing to provide access to all of medical devices behind the internal firewall. In an ideal world, one would run one service per bastion host. Each host has one clear purpose, it's difficult for problems to propagate from one service to another, and each service can be managed independently. In the real world, things are rarely the same due to financial, administration, and physical constraints as the number of hosts increases. Bastion host is countermeasure number 4.

5. Host-Based Security

Many medical devices are I/O (both disk I/O and network I/O) and CPU intensive. Installing any kind of host-based security software that may take away the CPU cycle and slowing down the I/O processing will impact the predictability of the results. Manufactures should investigate those Host Intrusion Detection System (HIDS), Host Firewall, and Anti-Virus software as long as they can be setup to run as a background process with a low priority and won't interfere with the primary purpose of the medical devices. Host-based software can be considered as countermeasure number 5.

Host Operating Lockdown such as shutdown unnecessary services, password requirements, system backups, and physical security will certain minimize the risks and can be considered as countermeasure number 6.

6. Remote Access

To support users and support staff remotely, remote access is required. Several options are available:

- **Login into a DMZ authentication server**. The user logs into a server that is adjacent (DMZ) to the firewall using some authentication technique such as password-based authentication or one-time password product such as Security Dynamics' SecurID. The user then uses the SSH to provide an encrypted and authenticated channel without exposing passwords to the network.
- **Dial-up Access**. The users dials up the modem pools at the Dial-up Access server on the DMZ. Once connected they will need to authenticate again using one of the more secure techniques such as SSH. An additional NIDS sensor is connected to the same LAN segment to monitor network activity.
- **VPN Access**. The user has a virtual private connection to the network using a combination of software and hardware that utilizes strong cryptography.
- **Citrix or Terminal Server Access.** The user login to the Citrix or Terminal server that authorizes user to access appropriate systems.

Again, this is not meant to be an exhaustive list of options.

4.4 Monitor

To improve network security, IT will need to establish procedures to continuously gather and analyze information through network monitoring, security news, periodically review configuration files and verify security configurations.

- **Monitoring the network.** Once the security policy and a secured infrastructure are in place, the next step is to monitor the network to ensure compliance to the security policy. Manual monitoring is usually accomplished by reviewing audit and log files. Automatic monitoring can be accomplished by using NIDS.

- **Monitoring the security news.** IT can subscribe to security mailing lists or web sites to learn of the latest news, tools, exploits, and countermeasure.

  Some of the mailing lists are:

  - Bugtraq at http://www.securityfocus.com
  - NTBugtraq at http://www.ntbugtrak.com
  - The SANS Institute at http://www.sans.org
  - Security Focus newsletter at http://www.securityfocus.com

  Some of the web sites are:

  - http://www.sans.org
  - http://www.incidents.org
  - http://securityfocus.com
  - http://www.cisecurity.org
  - http://www.microsoft.com/security
  - http://www.symantec.com

- **Periodically review configuration files** to ensure that routers, firewalls and other network devices are up-to-date and validate against the security policy.

- **Test network security** by using automated scanners (See section 4.2, subsection 3 for various scanners) or conducting professional security evaluations to ensure compliance to the security policy.

4.5 Response

According to SANS Security Essentials II, incident handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. The incident handling process, whether it is automated or manual,

should include 6 steps: preparation, identification, containment, eradication, recovery, and lesson learned. More details can be found at http://www.sans.org.

5 Conclusion

This problem impacts all device manufacturers and healthcare organizations. This is not an isolated situation and there is no silver bullet to this problem. The device manufacturers will have to re-evaluate their design control process to expedite the release cycle in order to be competitive, and ultimately stay in business. They should have process and procedures to lock down their medical devices as much as possible. They should work with their customers to arrive at a compromised solution or waiver, if possible. At the same time, device manufacturers should also work with the FDA to streamline its review and approval process.

Healthcare organizations will have to perform risk assessments in their own environments to determine their level of risk tolerance, based upon existing security measures put in place for their medical devices. System specific policy** may have to be put in place or adjusted to accommodate the release cycles of the medical devices. At the end of the day, it's the healthcare organizations' choices to not have the functionality needed to provide care to their customers, the patients, or to accept the risk and put in place the best possible defense-in-depth for their medical devices.

** As defined in SANS Security Essentials II, p. 2-4, system-specific policy should be developed when there are several systems that perform various functions and the use of one policy governing all of them may not be appropriate. It may be necessary to develop a policy directed toward each system individually.

Appendix A - Medical Devices and FDA Regulatory Requirements

In order to fully appreciate how the medical devices are used in the healthcare environments as part of the care delivery process for patients and how it can create conflict within healthcare organizations' security policies, an introduction to the medical devices background and the FDA regulatory is warranted. This section attempts to provide some insights into the FDA regulatory requirements regarding medical devices.

1. Medical Devices

What is a Medical Device?
The definition of a device appears in section 201(h) of the FD&C Act. A device is:
"...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component, part, or accessory, which is:

- recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes..."

Software that is to be marketed to enhance the performance of a device is regulated as an accessory to that device. Software that enhances the performance of a group of different devices is regulated as an accessory to the device that poses the greatest risk to the patient. The manufacturer of accessories is subject to the medical device regulations when the accessory is labeled and marketed separately from the primary device for a health-related purpose to a hospital, physician, or other end user [3].

2. FDA Regulatory Requirements

The Safe Medical Devices Act of 1990, enacted on November 28, 1990, amended section 520(f) of the act, providing FDA with the authority to add preproduction design controls to the Current Good Manufacturing Practice (CGMP) regulation. This change in law was based on findings that a ***significant proportion of device recalls were attributed to faulty design of product***. Specifically, in January 1990, FDA published the results of an evaluation of device recalls that occurred from October 1983 through September 1989, in a report entitled ``Device Recalls: A Study of Quality Problems" (Ref. 1). (See 55 FR 21108, May 22, 1990, where FDA

announced the availability of the report.) ***FDA found that approximately 44 percent of the quality problems that led to voluntary recall actions during this 6-year period were attributed to errors or deficiencies that were designed into particular devices and may have been prevented by adequate design controls***. These design-related defects involved both noncritical devices (e.g., patient chair lifts, in vitro diagnostics, and administration sets) and critical devices (e.g., pacemakers and ventilators). Also in 1990, the Department of Health and Human Services' Inspector General conducted a study entitled ``FDA Medical Device Regulation From Premarket Review to Recall'' (Ref. 2), which reached similar conclusions. With respect to software used to operate medical devices, the data were even more striking. ***A subsequent study of software-related recalls for the period of fiscal year (FY) 1983 through FY 1991 indicated that over 90 percent of all software- related device failures were due to design-related errors, generally, the failure to validate software prior to routine production*** [4].

As such all medical device manufacturers are required to submit a premarket notification, also known as PMN or 510(k). This premarket notification [510(k)] submission requirements and basic regulatory requirements that all manufacturers and distributors must consider, when they intent to:

a) market a medical device into commercial distribution for the first time, or
b) reintroduce a device that will be significantly changed, or
c) modified to the extent that its safety or effectiveness could be affected [1].

Information on the 510K submission can be found in the Premarket Notification 510(k): Regulatory Requirements for Medical Devices, http://www.fda.gov/cdrh/manual/510kprt1.htm

To assist manufacturers in understanding the intent of the regulation, and to ensure consistency with quality system requirements worldwide, the FDA provides the Design Control Guidance for Medical Device Manufacturers document for the medical device manufacturers. Because the design controls must apply to a wide variety of devices, the regulation does not prescribe the practices that must be used. Instead, it establishes *a framework that manufacturers must use when developing and implementing design controls*. The framework provides manufacturers with the flexibility needed to develop design controls that both comply with the regulation and are most appropriate for their own design and development processes [5].

Appendix B - References

1. 510K Overview.

2. SANS Security Essentials Version 1.3(amended December 12, 2001). The SANS Institute, 2001.

3. Premarket Notification 510(k): Regulatory Requirements for Medical Devices.

4. Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation.

5. Design Control Guidance for Medical Device Manufactures.

6. Guide to Inspections of Quality Systems, August 1999.

7. Naval Surface Warfare Center.

8. Cisco Secure Intrusion Detection System.
   Carter. Cisco Press.

9. SANS Security Essential

10. Building Internet Firewall.
    Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman.

11. White-Hat Security Arsenal.
    Aviel D. Rubin

12. Network Computing.

13. NSA.

14. Internet Secure Systems - RealSecure.