National Cybersecurity and Communications Integration Center

BULLETIN 201205040900

Attack Surface: Healthcare and Public Health Sector

Executive Overview

(U) The Healthcare and Public Health (HPH) sector is a multi-trillion dollar industry employing over 13 million personnel, including approximately five million first-responders with at least some emergency medical training, three million registered nurses, and more than 800,000 physicians.[1] This robust sector has led the way with medical based technology options for both patient care and data handling.

(U) A significant portion of products used in patient care and management including diagnosis and treatment are Medical Devices (MD). These MDs are designed to monitor changes to a patient's health and may be implanted or external. The Food and Drug Administration (FDA) regulates devices from design to sale and some aspects of the relationship between manufacturers and the MDs after sale. However, the FDA cannot regulate MD use or users, which includes how they are linked to or configured within networks. Typically, modern MDs are not designed to be accessed remotely; instead they are intended to be networked at their point of use. However, the flexibility and scalability of wireless networking makes wireless access a convenient option for organizations deploying MDs within their facilities.

(U) The expanded use of wireless technology on the enterprise network of medical facilities and the wireless utilization of MDs opens up both new opportunities and new vulnerabilities to patients and medical facilities. Since wireless MDs are now connected to Medical information technology (IT) networks, IT networks are now remotely accessible through the MD. This may be a desirable development, but the communications security of MDs to protect against theft of medical information and malicious intrusion is now becoming a major concern. In addition, many HPH organizations are leveraging mobile technologies to enhance operations. The storage capacity, fast computing speeds, ease of use, and portability render mobile devices an optimal solution.

(U) This Bulletin highlights how the portability and remote connectivity of MDs introduce additional risk into Medical IT networks and failure to implement a robust security program will impact the organization's ability to protect patients and their medical information from intentional and unintentional loss or damage.

Background

(U) According to Health and Human Services (HHS), a major concern to the Healthcare and Public Health (HPH) Sector is exploitation of potential vulnerabilities of medical devices on Medical IT networks (public, private and domestic). These vulnerabilities may result in possible risks to patient safety and theft or loss of medical information due to the inadequate incorporation of IT products, patient management products and medical devices onto Medical IT Networks. Misconfigured networks or poor security practices may increase the risk of compromised medical devices. HHS states there are four factors which further complicate security resilience within a medical organization.

1. (U) There are legacy medical devices deployed prior to enactment of the Medical Device Law in 1976, that are still in use today.[2] Prior to enactment of the law, the FDA required minimal testing before placing on the market. It is challenging to localize and mitigate threats within this group of legacy equipment.
2. (U) Many newer devices have undergone rigorous FDA testing procedures and come equipped with design features which facilitate their safe incorporation onto Medical IT networks. However, these secure design features may not be implemented during the deployment phase due to complexity of the technology or the lack of knowledge about the capabilities. Because the technology is so new, there may not be an authoritative understanding of how to properly secure it, leaving open the possibilities for exploitation through zero-day vulnerabilities or insecure deployment configurations. In addition, new or robust features, such as custom applications, may also mean an increased amount of third party code development which may create vulnerabilities, if not evaluated properly.
3. (U) In an era of budgetary restraints, healthcare facilities frequently prioritize more traditional programs and operational considerations over network security.
4. (U) Because these medical devices may contain sensitive or privacy information, system owners may be reluctant to allow manufactures access for upgrades or updates. Failure to install updates lays a foundation for increasingly ineffective threat mitigation as time passes.

(U) FDA regulation mandates that manufacturers ensure the safety and effectiveness of their MD that incorporates off-the-Shelf (OTS) software. Manufacturers are responsible for continuous safe and effective performance of an MD containing OTS software and performance of the OTS software used by the MD.[3] Secure deployment and management of the MD or related IT infrastructure is the responsibility of the purchasing organization. According to the HPH Sector Specific Plan (found on pg 31, section 3.10), most risk assessments performed in the HPH Sector are conducted to achieve compliance with safety, physical security, and information security regulations. Following are some examples:

- (U) Hospitals must conduct risk assessments to meet State regulations and achieve certification required for reimbursement by the Federal Medicare program.
- (U) Pharmaceutical manufacturers conduct risk assessments to meet regulations that ensure the efficacy of their products.
- (U) Sector health plans, healthcare providers, and healthcare clearing houses assess risks to systems that maintain health data to ensure compliance with security and privacy rules in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- (U) Federal partners conduct risk assessments as a component of the certification and accreditation process to comply with the Federal Information Security Management Act (FISMA) of 2002.
- (U) Beyond the need to meet regulatory requirements, HPH Sector organizations have a vested interest in conducting risk assessments to identify risks that could lead to negative financial consequences and damage to their reputations. The SSA will assist sector partners with this process by identifying and sharing risk assessment tools.[1]
- (U) Based on HHS reporting, until recently the primary focus of FDA's regulatory scrutiny on medical devices was their safety and effectiveness, but technological advancements in networking and communication have brought both benefits and risks. While increased interoperability and efficiency can be facilitated by modern networking and communication technologies, the way MDs are set up on communications networks by the purchaser determines how well protected they may be against cyber attacks.
- (U) As medical organizations transition from legacy, proprietary software to commercially available products, they run the risk of infection from traditional infection vectors like internet, email, removable media, mobile phones, etc.

Technical Details

(U) Technology developers are frequently creating and selling new technologies that change and expedite the way healthcare personnel carry out their mission essential functions. As a result, Healthcare and Public Health Sector owners and operators are consistently challenged to keep up with modern technology. Capable and accessible communications networks and technical devices are crucial for first responders, doctors, and patients. Financial constraints, personnel shortages, and a lack of risk awareness have resulted in proprietary computer operating systems that are not compatible with current antivirus software applications. Additionally, medical devices utilizing wireless technology are both implantable within the body and portable, adding to further concern and vulnerabilities. In a world in which communication networks and medical devices can dictate life or death, these systems, if compromised, pose a significant threat to the public and private sector. For example, a widespread malware infection may cause a network outage, impacting a hospital's ability to treat patients or relay critical information.

(U) The following provides a summary of types of computing devices within the healthcare industry:

1. (U) **Implantable Medical Devices (IMD):** Some medical computing devices are designed to be implanted within the body to collect, store, analyze and then act on large amounts of information. These IMDs have incorporated network communications capabilities to increase their usefulness. Legacy implanted medical devices still in use today were manufactured when security was not yet a priority. Some of these devices have older proprietary operating systems that are not vulnerable to common malware and so are not supported by newer antivirus software. However, many are vulnerable to cyber attacks by a malicious actor who can take advantage of routine software update capabilities to gain access and, thereafter, manipulate the implant.

    - (U) During an August 2011 Black Hat conference, a security researcher demonstrated how an outside actor can shut off or alter the settings of an insulin pump without the user's knowledge. The demonstration was given to show the audience that the pump's cyber vulnerabilities could lead to severe consequences. The researcher that provided the demonstration is a diabetic and personally aware of the implications of this activity. The researcher also found that a malicious actor can eavesdrop on a continuous glucose monitor's (CGM) transmission by using an oscilloscope, but device settings could not be reprogrammed. The researcher acknowledged that he was not able to completely assume remote control or modify the programming of the CGM, but he was able to disrupt and jam the device.[4]

2. (U) **External Medical Devices:** Older versions of non-implanted medical devices still in use were designed as embedded systems with little or no connectivity that have proprietary operating systems. Increasingly, medical devices are incorporating commercial operating systems that provide enriched feature sets such as connectivity and firmware updates. As these commercial operating systems displace traditional operating systems created by individual software developers, their vulnerabilities become better identified by hackers because of their widespread and public availability.

3. (U) **Portable Devices:** Increased wireless interconnectivity introduces additional configuration challenges between portable devices, medical IT infrastructure, remote facilities, and partner IT infrastructure.[1] Portable medical devices are gaining popularity with the introduction of iPads, smart phones and laptops that use Windows and MAC operating systems. These devices are currently being used by healthcare professionals in direct patient care settings, including in hospitals to discuss healthcare information such as clinical tests, x-rays, and lab results with their patients in real time. The following examples highlight types of portable devices used by and in the HPH Sector:

   - (U) University of Chicago doctors use iPads to access patient information and to aid with dialogue with patients during consultations. McAfee released a report stating Apple's IOS devices were unaffected by the growing mobile malware attacks facing other platforms. However, a security software firm discovered malware, Backdoor. Bifrose.AADY, which affected iPad and iTunes users connecting through Windows operating systems. iPad users were sent an e-mail with a link for an iTunes update. Once the link was clicked a code injected itself into explorer.exe, a Windows background process, at which point a newly infected system could be accessed and controlled by a third party. The code also pulled serial numbers and read passwords for different programs including POP3 email and any protected storage.[5]

   - (U) A good example of a product Bluetooth wireless regulated medical devices is a wireless electrocardiogram. Each patient lead can be designed as a separate battery-powered Bluetooth device that communicates with a battery-powered Bluetooth-enabled patient monitor. The patient monitor communicates with the hospital's 802.11b network and continuously sends the electrocardiogram data to the network. Meanwhile, the doctor can monitor this data from anywhere and at anytime in the hospital using his or her handheld personal digital assistant, completing the entire electrocardiogram monitoring process without a single wire.
   - (U) Poor smartphone configuration increases malware related risks during the syncing and transferring of data with a personal computer and during unscanned downloads. Smartphones with poorly designed security protections are frequently connected to medical IT networks and provide a new vector for malware transmission.
   - (U) A Conficker working group official identified 300 medical devices from a single manufacturer had been infected with the Conficker Worm. These devices were used by doctors to view MRIs typically located in or near intensive care units and were connected to local area networks (LAN).[6] It was noted by the working group that the computers on the LAN were older computers running Windows NT and Windows 2000 that did not have updated anti-virus software and when connected to the internet became infected with the Conficker worm.[7]

4. **(U) Expanding Attack Surface:** The advances of MDs like smartphones, tablets and USB devices used in the healthcare sector have enabled patients to receive better care, track ever increasing volumes of electronic healthcare records and ultimately providing more time for patient and physician relations. Along with these advances are concerns;

instant connectivity of these devices to the internet or a Health Information System (HIS) that could be compromised if not protected with the latest anti-virus and spy-ware software. Due to the ease of portatbility, additional best practices to secure an MD is with encryption software or password protection to prevent sensitive information contained on the device from being accesses or used illegally. MDs like smartphones and tablets are mini computers with instant access to the internet or linked directly to a hospital's network. The device or the network could be infected with malware designed to steal medical information if not upgraded with the latest anti-virus and spy-ware software.

- (U) *Home healthcare:* In the future, elderly and infirm patients can be monitored by loved ones and medical professionals in their home, saving the cost and distress of institutionalization. This process may be threatened by the inadequacy of these home networks and their maintenance. Homeowners may not use proper password protections or maintaining the most current antivirus software. By definition the elderly and infirm may not be able to determine whether these domestic networks are safe or even operational.
- (U) *Physician group practices:* Most people have their primary healthcare provider in a small physician group practice and these may be the least able to properly configure and regularly maintain their networks.
- (U) *Health Insurance companies:* More than anyone else, health insurance companies handle the most sensitive data. This data is not just a patient's medical information but includes their financial history. This information is shared with multiple parties such as physicians, health plans and pharmacies and other third parties. Third party vendors are used by insurance companies to administer their program to include processing and collection of payments. The handling of medical information by so many entities has lead to the theft of patient medical records. Medical identity theft leads to fraudulent claims by the criminal entity to the patient's insurance company or may even involve dishonest pharmacists that write fraudulent prescriptions that are eventually sold on the black market.[8] One of the most effective efforts that health insurance companies can do to reduce their risk of compromised information would be to educate their employees on established security policies and processes. Education should include what the password policy is and how often it is suppose to be changed and that it should never be shared with others. Inform personnel on types of malware and Spearphising scams that may target them when they are at work and connected to the internet. Employees should know that these scams may be specifically targeting them and their knowledge of and access to medical information.
- (U) *Electronic Patient Records (EHR):* Patient records are at risk when stored on unencrypted laptops and portable drives. To process EHRs or send EHRs per a patient or physician's request, internet connectivity is a requirement. An EHR compromise can lead to loss of patient trust, a violation of the Health Insurance Portability and Accountability Act (HIPAA) and actual loss of the medical practice or business. A significant threat to an EHR system is unauthorized access by insiders. Access to records should only be given to those that actually need access. IT Administrators should routinely monitor personnel access to EHR through logs ensuring that employees are not misusing access privileges. IT Administrators should also verify that access rights are given based on need to know to prevent unrestricted access to EHRs.[9]

TACTICS, TECHNIQUES, AND PROCEURES

(U) **Disruption of Operations:** Continuity of healthcare services is one of the main objectives of the HPH Sector. Physical sabotage or natural disasters that damage or disrupt sector cyber infrastructure are the most likely threats that could negatively impact the sector's ability to provide continuous services.[1] Other manmade threats to the continuity of sector operations include a Denial of Service (DOS) attack, which may be the result of a physical or cyber action that causes an interruption of business operations by overwhelming a resource (web server, router, etc). DOS or Distributed Denial of Service (DDOS) attacks are achievable through technological means, typically a botnet.

(U) **Information Theft:** There are several points of entry for most adversaries targeting the HPH Sector: insider, web, email, or equipment loss.

- (U) *Insider:* Employee turnover, advances in portable media, and availability in massive cloud storage create an optimal environment for insiders seeking to steal data. Intellectual property (IP) and competitive knowledge can be transferred quickly, easily and relatively without detection using portable media devices or by uploading to the cloud. The most common method of data exfiltration by insiders involves network transfer (via email, remote access channel, or file transfer).[10]
- (U) *Malware:* Computers of HPH personnel may become infected by widely distributed malware variants designed to steal information. These malware families include keystroke loggers, remote access trojans, etc. While not designed to specifically target healthcare systems, the malware is capable of harvesting readily available information and documents for exfiltration to command and control (C2) servers. These C2 servers are used by attackers to stage information for collection.
- (U) *Spearphishing:* Spearphishing is an email based attack where tailored emails containing malicious attachments or links are sent to key personnel. These emails are especially convincing because they appear to be sent from a legitimate source. Criminals seeking detailed information on medical advancements or procedures will often use spearphishing to penetrate a network. When targeting management, attackers will craft an email related to a relevant current event or company policy. Attacks designed for other company members will have a different format and focus on topics like human resources actions (salaries, job openings, raises, etc.) or IT updates (patches, upgrades, etc). The highly customized nature of spearphishing emails make them extremely difficult to mitigate at the email gateway. In addition, advanced attackers understand how to bypass email filters and antivirus software so that malicious software can be delivered successfully.
- (U) *Web:* Silent redirection, obfuscated JavaScript and search engine optimization (SEO) poisoning are just a few of the ways an adversary can leverage web behaviors to penetrate a network. In addition web servers with injection flaws or broken authentication may expose an organization to information leakage or database

THREATS

INSIDER: Most insiders steal within 30 days of leaving an organization. (CERT)

WEB: During 2010, approximately 64% of websites had at least one Information Leakage vulnerability. (WhiteHat Security)

EMAIL: The number of targeted phishing attacks skyrocketed during the last quarter of 2010 averaging 70 per day. (Symantec)

compromises.

- (U) *Equipment Loss:* Theft or loss of equipment containing sensitive medical information of patients or organizations is a significant problem because of its frequency and severe consequences. The more that patient information is electronically stored, the more likely that when a security breach and or theft of electronic media is stolen, the number of people affected will increase. In a report submitted to congress by Health and Human Services (HHS) for the calendar years of 2009 and 2010, officials noted that in addition to the typical equipment stolen such as laptops and desktops, theft of backup tapes and network servers were also reported. Additional thefts reported included smartphones, flash drives, CDs and memory cards.[11] Poor physical security protective mechanisms or operational security awareness make it easy for thieves. In addition, lack of hardware encryption allows thieves direct access to all data stored on the device.

Vulnerabilities

(U) A benefit that medical devices, patient management applications and general hospital IT bring to the medical community, patients and manufacturers are the remote monitoring and treatment to patients with chronic conditions. Medical professionals and manufacturers are able to monitor devices in real time, provide case management, data downloads and software updates. These benefits require the use of MDs that unintentionally provide pathways for possible intrusions into a Medical IT networks that can result in risk to the patient or theft of medical information.

(U) Healthcare IT Administrators can reduce risk to the patient that relies on a MD and ensure that patient information is secure thru established policies and procedures. An overall strategy will be the foundation for securing MDs used by medical professionals and the patients that require them. The strategy should encompass all mobile devices used by the organization not just those connected to the network. Policy should include how MDs are connected to the HIS or if connected on a separate network and how device information is accessed and protected.[12] Employees should be provided training on all MD policies, what is acceptable and what is not. They should be aware of password requirements and if personal mobile devices are prohibited on the HIS. There should be an encryption policy for MDs to ensure that the device itself is protected and ensures another layer of security to the MD if lost or stolen. Encryption methods should include information that is transmitted to and from the MD.[13]

(U) During discussion with Veterans Administration(VA) Officials on this Healthcare Sector Product, the VA conveyed that during a recent exercise, MD manufacturers refused to allow their MDs to be encrypted because encryption software had not been tested. Manufacturers could not ensure that MDs would continue to operate as intended under FDA license if the VA installed encryption software onto a MD. To protect purchasers and users of MDs that may be subject to cyber vulnerabilities, prior to installation of new patches and or encryption software, MD manufacturers should be contacted for their recommended corrective action.[3]

(U) Kevin Fu is an Assistant Professor in Computer Science at the University of Massachusetts Amherst that conducts advanced research on implantable medical devices. In 2009, Kevin Fu demonstrated a proof of concept attack at an Emory Tech Conference on how to illicitly access an implanted medical device (IMD). Doctors are beginning to routinely access IMDs such as pacemakers and defibrillators over the Internet using a short range wireless link. This process enables doctors to manage the device, make software updates, and continuously monitor and even treat the patient remotely. The demonstration proved that once a device is hacked, it can be vandalized, reprogrammed, or have medical information stored on the device stolen.[14]

(U) Professor Fu also showed that a device could be built with off the shelf components allowing illicit communication with a device. The exploit was possible due to a communications feature left active in the device intended to be used during manufacturing quality control but had not been turned off. The only additional information needed to gain access to the device was the patient's name. This access could allow a malicious actor to reprogram the defibrillator, deliver a shock to the patient's heart, and/or disable the power saving mode causing the battery to run down in hours rather than years.[15] This demonstration shows that the design concepts for medical device immunity from cyber attack must include all phases of the medical device lifecycle including inception,design, manufacturing, the deployment environment, maintenance, and finally support.

(U) While proprietary operating systems provide little external visibility to design flaws which might enable external unauthorized access, the operating system only provides this protection against less sophisticated intruders. More robust measures like encryption and authentication would act as a deterrent to more advanced attackers.

Impact of Mobile Devices in the Healthcare Sector

(U) The recent increase of mobile devices and their availability to consumers for private and professional use pose a challenge for IT Administrators. Mobile devices have evolved how healthcare professionals implement healthcare by adding flexibility and provide immediate access to patient records leading to more time spent with patients by a healthcare professional. If IT Administrators don't implement the correct mobile device for the right job or are slow to integrate an MD into the work place, they run the risk that employees may use their personal mobile devices to perform their duties. If a healthcare professional uses a personal device such as a smart phone, tablet or USB device to access patient information, at risk for theft or accidental loss of the device is patient information on an unencrypted or protected device that is not password protected.[16]

(U) Hospitals are held liable if an employee loses a patient's information. USB drives can hold approximately 25,000 patient records that if lost due to an actual theft or loss of the USB, the cost to the hospital in penalties can be six million dollars or more. Penalties may include legal fees, notification to affected patients and cost for ID monitoring services.[17]

(U) Healthcare and Public Health Sector IT Administrators need to address the gap between security and mobile device use. Areas of concern include unmanaged mobile device access, authentication of users requesting access to a hospital's web server, how to secure mobile devices with health information, unsecured wireless connectivity or cellular networks and protection against unauthorized breach of lost and/or stolen devices.

(U) The following example is a example of an attack that can impact medical MDs and mitigation steps taken to minimize risk to the patient, theft of medical information, and ultimately the Health Information System:

- (U) In reaction to more than 181 cyber attacks against MDs used by the VA, MDs were placed on separate networks, isolating them from the main network in order to protect both clinical information and devices. This was done using a modern technique of network configuration called Virtual Local Area Networking (VLAN) with access control lists (ACLs). This technique allows a networked device to remain available on the network while only permitting positively authorized users to log in to it.[18]
- (U) The VA, which has long been a champion of better practice in network security, has in excess 50,000 MDs which they categorized by function and manufacturer and group them on individual Virtual Local area networks (VLANS). This allowed the devices to be

disconnected from other parts of the VA network and from external intrusion but enabled their healthcare professionals to continue maintaining the treatment and monitoring functions of the devices.[19] This defense-in-depth strategy was well described in their Isolation Architecture publication. [20]

- (U) In general, a suitable firewall configuration should be maintained for those medical devices connected to medical IT networks. Since many existing medical devices were designed with embedded operating systems, the majority of current cyber attacks cannot affect them but significant and growing numbers of devices are now configured with some kind of commercial OS, and if allowed unprotected connectivity, they can become susceptible to malware and or viruses.

(U) Some devices that are very sensitive to battery life, such as those which are implanted, may be vulnerable to Denial of Service (DOS) attacks. The side effect of these DOS attacks may be to continually awaken the device it from its battery preserving “sleep” state, thus reducing its lifetime and provoking the patient to an earlier surgery for its exchange than would otherwise be needed. Only internal design measures, specifically tailored to DOS attacks, can prevent this threat vector. It is important that engineers keep this threat in mind and design devices to withstand DOS attacks.

(U) Another danger in medical devices, patient management application and general hospital IT is the potential theft of personally identifiable medical information that could be provided to unauthorized agents such as the press, insurance companies, private investigators, lawyers, etc. which might cause embarrassment to the patient or interested parties. This sensitive information could also be used for illegal purposes, such as profit on underground forums or identity theft. The protection of networked MDs can best be implemented in a layered security approach using the suggested following best practices:

- (U) Purchasing only those networkable medical devices which have well documented and fine-grained security features available, and which the Medical IT network engineers can configure safely on their networks.
- (U) Including in purchasing vehicles vendor support for ongoing firmware, patch, and antivirus updates where they are a suitable risk mitigation strategy.
- (U) Operating well maintained external facing firewalls, network monitoring techniques, intrusion detection techniques, and internal network segmentation, containing the medical devices, to the extent practical.
- (U) Configuring access control lists (ACL) on these network segments so only positively authorized accounts can access them.
- (U) Establishing strict policies for the connection of any networked devices, particularly wireless devices, to Health Information Network (HIN) including; laptops, tablets, USB devices, PDAs, smartphones, etc. such that no access to networked resources is provided to unsecured and/or unrecognized devices.
- (U) Establishing policies to maintain, review, and audit network configurations as routine activities when the Medical IT network is changed.
- (U) Using the principle of least privilege to decide which accounts need access to specific medical device segments, rather than providing access to the whole network.
- (U) Implementing safe and effective, but legal patch and software upgrade policies for Medical IT networks which contain regulated medical devices.
- (U) Securing communications channels, particularly wireless ones, by the use of encryption and authentication at both ends of a communication channel.
- (U) Having and enforcing password policies to protect patient information.

Points of Contact

(U) This product was produced as a collaborative effort between NCCIC components and our partners: National Cyber Security Division-Critical Infratructure Cyber Protection and Awareness (CICPA), Health and Human Services, Veterans Administration and DHS Office of Intelligence and analysis (I&A). We would also like to acknowledge the Sector Specific Agency and private industry sector partners for their contribution.

(U) Please direct questions to the NCCIC Duty Officer (NDO) via email at NCCIC@hq.dhs.gov or by phone at (703) 235-8831. The NCCIC will continue to coordinate with the appropriate component organizations.

References

1. Healthcare & Public Health Sector Specific Plan. http://www.phe.gov/Preparedness/planning/cip/Documents/2010-cip-ssp.pdf, website last accessed 27 March 2012.
2. F.D.A. to Check Safety of Old Devices. http://ww w.nytimes.com/2009/04/09/business/09device.html, website last accessed 27 March 2012.
3. FDA Guidance for Industry Cybersecurity for Networked Medical Devices Containing off the Shelf Software. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/
4. Getting Root on the Human Body. http://www.darkreading.com/security/vulnerabilities/231300312/getting-root-on-the-human- body.html, website last accessed 27 March 2012.
5. iPhone,iPad untouched by mobile Malware Attacks. http://www.imore.com/2011/08/24/iphone-ipad-untouched-mobile-malware-attacks/, website last accessed 27 March 2012.
6. Red tape keep conficker on medical devices, http://www.zdnet.com/news/red-tape-keeps-conficker- on-medical-devices/295270, website last accessed 27 March 2012.
7. Conficker infected critical hospital equipment hospital. http://news.cnet.com/8301-1009_3-10226448-83.html, http://news.cnet.com/8301-1009_3-10226448-83.html
8. How to keep your health insurance information safe from thieves, http://www.insureme.com/health-insurance/keeping-your-health-insurance-information-safe, website last accessed 27 March 2012.
9. 5 Steps To Access Health Data Breatch Risks, http://www.informationweek. com/news/healthcare/security-privacy/232602025,
10. CERT Guide to insider Threats. http://www.sei.cmu.edu/library/abstracts/books/9780321812575.cfm, website last accessed 27 March 2012.
11. HHS: Patient Data Breaches Have more than Doubled. http://www.informationweek.com/news/healthcare/security-privacy/231601760, website last accessed 27 March 2012.
12. How Secure Are Your Clinicians'' Mobile Devices. http://www.informationweek.com/news/healthcare/mobile-wireless/231903089, website last accessed 27 March 2012.
13. IBID. website last accessed 27 March 2012.
14. Killer hackers could target cardiac inplants. http://www.theinquirer.net/inquirer/news/1556846/killer-hackers-target-cardiac-implants, website last accessed 27 March 2012.
15. IBID. website last accessed 27 March 2012.
16. HHS: Patient Data Breaches Have More Than Doubled. http://www.informationweek.com/news/healthcare/security-privacy/231601760
17. Doing More with Mobile Devices In Healthcare: Eliminating the Security Compromise. http://www.forbes.com/sites/dell/2011/09/22/mobile-devices-in-healthcare/, website last accessed 27 March 2012.
18. VA Addresses Medical Device Security. http://www.healthcareinfosecurity.com/interviews.php?interviewID=1163, website last accessed 27 March 2012.
19. Providers Scramble to Protect Medical Devices from Cyber-Attackers. http://scrubsandsuits.com/news/providers-scramble-to-protect-medical-devices-from-cyber-attackers, website last accessed 27 March 2012.
20. Medical Device Isolation Architecture Guide. http://www.himss.org/content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf, website last accessed 27 March 2012.