Are Hospital Networks Really Secure

Carl Brackett

East Carolina University

Abstract

Medical care comes in various forms of treatment; they have one thing in common no matter which medical facility in which treatment was obtained, they all start a patient record. Patient records are no longer recorded on paper; they are stored in a digital format. The question is, do medical facilities like hospitals really have their networks secure to protect patients and their confidential information?

Patients are under the impression that the personal information they share with a hospital will be kept confidential and used internally as necessary for their care. The patient signs HIPPA and consent forms that are suppose to protect their information from being accessed by unauthorized individuals that are not listed on these forms. Hospitals are being breached by the various devices that are designed to help the patient recover during their stay at the facility.

This paper is going to research if hospitals are keeping their patient information secure on their network. This research will provide multiple examples of how devices in different hospitals have been compromised allowing sensitive patient information vulnerable for theft. This paper will also discuss what security measures are in place at hospitals that failed to stop the information from being stolen.

Conclusions will be drawn from the findings found in this research and examples discussed to see if breaches can be avoided in the future.

Keywords: *digital records, hospitals, HIPPA, security, medical*, firewall

Introduction

Medical care for patients has evolved over the years as new technology has been made available for doctors to care for their patients. With this growth in technology, medical records for patients have also seen a change in the way they are kept when checking into a doctor's office or hospital for treatment. These patient records are not stored in a folder and put away until the patients next visit, but they are stored in a digital format that can be shared between medical facilities automatically with the patient's consent.

This new digital age of record keeping may simplify keeping patient records up to date in a timely fashion, but it also brings up some new issues in regards to security. The patient information is collected and distributed with electronic devices that may contain vulnerabilities that can be exploited by unauthorized users (Niccolai, 2015). These persons do not need a key or a sign out log as in years past, they may not even be in the same vicinity as the patient being treated (Harman, Flite, & Bond, 2012).

Security measures on hospital networks should be considered and implemented since the information flowing through the network contains confidential information for patients. Security breaches for hospitals has risen over the years due to attackers figuring out ways they can get into the network quickly by simply hacking a device that may already be connected to the network. Devices like drug infusion pumps, defibrillators and temperature controls can be manipulated by an attacker remotely just by gaining access to the hospital network (Zetter, 2014).

Specific device examples will be discussed in how an attacker may gain access to the network or start manipulating devices attached to the network. Security measures that

are in place will be discussed showing how easy an attack can be carried out against a hospital network. Conclusions will be based from research findings and specific examples of how a device can be easily accessed and controlled remotely. The discussion on these topics may lead to avoiding future breaches on the network.

Literature Review

As technology advances and grows, medical facilities like hospitals embrace the new technology in hopes to provide better care for their patients. Changes in technology can be good or bad depending on the circumstances in which the technology is used. Hospitals not only deal with patient care, but they are also obligated to protect the patient's confidential information. Hospital networks were designed to interconnect the different departments to share patient information easily and for faster diagnosis of patients. Before hospital networks, patient information was filled out in paper form and was hard to keep the information updated in a timely fashion (Harman, Flite, & Bond, 2012).

Networking boomed in places like hospitals allowing them to start keeping digital records of their patients. Even though hospitals could now keep their information digitally, issues regarding security have become a concern. Devices like MRI scanners and X-ray machines can now connect to the network, but may come at a cost of a security breach (Niccolai, 2015). These type of devices may contain vulnerabilities that may allow an attacker to gain access to the network and steal patient information (Niccolai, 2015).

In a report done by TrapX Security, two specific attacks are given showing how easy it is for an attacker to gain access to a hospital network using the same equipment

used to save patient lives. This equipment has become the target for attackers since most of the devices do not have any security applications installed on them (Munro, 2015). Any device with internet connectivity is a potential target for an intruder to gain access to the network (TrapX Labs, 2015).

In the first attack found by TrapX, blood gas analyzers were used to penetrate the network. An attacker infected the systems with malicious software to gain access to the network (TrapX Labs, 2015). Sensors installed by TrapX detected the activity coming from the blood gas analyzers and sent out alerts regarding the activity detected (TrapX Labs, 2015).

The second attack discussed in the TrapX report, involved the picture archive and communications system (PACS). PACS is used as a central storage system for images from the radiology department (TrapX Labs, 2015). An end-user from the hospital clicked on a malicious website that ended up using a java exploit allowing the attacker to run remote commands to gain access to the network (TrapX Labs, 2015). Even though the hospital was running applications to defend against cyber attacks, it could not detect this attack against the PACS environment (TrapX Labs, 2015). TrapX concluded in their report that they thought that the majority of hospitals were infected with some type of malware not being detected with their current infrastructure and cyber attack procedures (Ragan, 2015).

Accessing a hospital network may not be as complicated as one may think, since access does not have to be gained by hooking into a RJ-45 jack on the wall. Most care facilities including hospitals are putting in wireless access points for network access since some of the equipment used by the doctors and nurses run off of wireless connections.

Connecting these devices wirelessly or by bluetooth is suppose to make communication for staff more efficient, but the problem with these devices is that they do not get configured properly or have default username/passwords configured on them (Arsene, 2015).

Securing patches for these devices from the manufacturer or installing security software on them prove to be difficult since most of the devices are proprietary and contain individual operating systems for each device. If a security patch is written for one of these devices, it has to be approved by the FDA before officially getting released to the customer (Arsene, 2015). With lagging security updates these devices may already be infected with some type of malware even though the hospital network does not have any issues being detected with current cyber security techniques.

In a two-year study conducted by Scott Erven, an IT security specialist for Essentia Health, on different medical facilities in the Midwest he found numerous devices on the network that could be manipulated very easily (Zetter, 2014). He found that drug infusion pumps could be controlled remotely to change the dosages being distributed to a patient like a nurse would do if physically in the room with the patient (Zetter, 2014). Bluetooth-enabled defibrillators could be manipulated into giving false shocks when not needed or stopping a shock that could save a patient's life (Zetter, 2014). Refrigerators that are connected to the network for monitoring temperatures could be accessed and have the temperatures changed remotely causing damage to the goods being cooled inside (Zetter, 2014).

Research has been done on these type of devices, but health care facilities are not taking them into consideration before purchasing them (Zetter, 2014). Health care

facilities are not evaluating and performing tests on the equipment prior to purchasing and putting the equipment into official use (Zetter, 2014). The vulnerabilities if any should be found in the testing phase so requests can be made to the manufacturer to have them corrected before completing a transaction for the equipment. Erven states that one of the main problems found in many of the devices that could be hacked was due to embedded web services in the devices that allows communication to other devices on the network (Zetter, 2014).

Hospitals need to invest more time and money into their security infrastructure to protect their patients and staff from attacks (Arsene, 2015). They need to have policies in place to have stricter passwords and access for staff (Arsene, 2015). Firewalls are great appliances for stopping unwanted traffic from getting inside the network from the outside, but this is not always the case. A good example of this occurring from inside the hospital, was a contractor for the hospital being able to download patient information to a laptop and ended up having the laptop stolen from their vehicle (Schultz, 2012). 34,000 patients had to be notified that their personal information which was suppose to be secure on the hospitals network were stolen and could be compromised by an unknown individual (Schultz, 2012). Policies should have been in place for the hospital that would have never allowed the patient information to be downloaded to a laptop and be taken off the network.

Hackers can manipulate exploits in medical devices in a variety of ways causing havoc for hospitals and medical facilities. The attack may be targeting a medical device like a pacemaker that could potentially be deadly for a patient (Battelle, 2015). In 2007, Dick Cheney had the wireless functionality disabled on his pacemaker to eliminate any

concerns of being assassinated by his pacemaker being hacked (Battelle, 2015). Hackers may not be wanting to injure anyone, but instead they may be wanting to disrupt the services at the hospital by causing a Denial of Service attack on the network (Battelle, 2015). They could also be gaining access to the network for financial gain by encrypting and holding patient information for ransom until their demands are met to their satisfaction (Battelle, 2015).

Hospitals need to take security seriously and be proactive instead of reactive when such an attack occurs on their network. A plan needs to be in place to deal with security breaches so the necessary actions can be performed immediately after an attack. HIPPA compliance needs to be taken seriously by all staff to protect secure information and patient records (Berger & Manos, 2014). Any device that leaves the network, will need to have the data encrypted in case the device is stolen while off premises (Berger & Manos, 2014). Following simple guidelines like the ones just mentioned will provide some basic security to protect the information flowing on the network.

Research has shown that security investments after an attack are not as effective as investments for preventing future attacks (Johnson, 2011). Four steps that healthcare facilities can follow to help strengthen their network security are to take inventory, control access, use simple technology and educate end users (Johnson, 2011). Taking an inventory of how information flows and where is it stored within the network can help build countermeasures to secure the information properly (Johnson, 2011). Controlling access to sensitive information is important, since it does not need to fall in the wrong hands. By limiting who has access to certain information, it is not likely to be viewed by an unauthorized individual (Johnson, 2011). Use technology that is user friendly and

makes sense to the end user, if not they may be prone to trying to go around the technology implemented causing bigger security concerns for the facility (Johnson, 2011). Educating end users about security is very vital, some users may not understand the ramifications of a decision they make could compromise the integrity of the network allowing a potential breach to steal sensitive information (Johnson, 2011).

Not all breaches are caused by devices on the network, some are from human error (Horowitz, 2012). From a Healthcare Information and Management Systems Society (HIMSS) Report, human error was identified as a major factor in healthcare security breaches with 79 percent of respondents stating that the breaches were initiated by the employee and 56 percent responded that employees had unauthorized access to data on the network causing the breach (Horowitz, 2012). Even though security policies are updated regularly, it is best to start at the source and make sure all staff are properly educated on security for the facility (Horowitz, 2012).

The majority of healthcare facilities already have certain security practices that they have in place to protect the information on the network. In most instances any facility that is connected to the internet or other facilities that are at a different location will have a firewall or multiple firewalls in place to keep unauthorized individuals gaining access to the network. This does not stop unauthorized access from inside the network, like if an individual gains access to the network from inside the facility with a wireless connection. Access is granted only to individuals that need access to certain information related to their job (HRSA, n.d.). Logs are recorded and audited to make sure there is not any unauthorized access to information on the network (HRSA, n.d.). Information flowing across the network is encrypted in case there is an unauthorized

capture of information obtained by an authorized or unauthorized user (HRSA, n.d.). Even though these measures and policies are in place, breaches are still occurring randomly throughout healthcare facilities exposing private and confidential data (HIPPA Journal, 2015).

Conclusion

Technology has made the exchange of information between healthcare facilities faster and more up to date in the past years. Paper records are in the past and have been replaced with digital copies for patient records. This digital age in medical facilities has presented some new concerns in security. In the past, the paper records would be on a shelving system behind a locked door where today this is not the case. The information on the network can be retrieved by all authorized personnel in the facility, but can also be at risk of getting stolen by unauthorized individuals as well.

Hackers do not need to break into the healthcare facilities physically, but find other means of accessing the network by using the very devices already onsite. Devices that are critical for patient care and that cannot have updates installed on them regularly poses security issues for the network. Security flaws in devices like drug infusion pumps and defibrillators not only put the safety of patients at risk, but it can also allow an attacker to gain access to the network. These type of devices need to be evaluated and fixed by the manufacturer before selling them to a healthcare facility. Healthcare facilities need to test and evaluate the equipment before purchasing them to make sure these type of vulnerabilities do not exist. Not all the blame can be placed on vulnerable devices, since human error was also found to be a cause for security breaches.

Healthcare facilities have policies and procedures in place for protecting the network, but sometimes do not detect malicious activity running on devices like drug infusion pumps or defibrillators. Proactive precautions need to be taken before a breach occurs to make sure patient's data is stored and secured correctly. Active monitoring and access controls need to be implemented correctly and evaluated monthly to make sure no suspicious activity is occurring on the network. From the information read and taken from the articles, breaches in healthcare facilities are on the rise. Until devices being connected to the network can be controlled efficiently and employees educated correctly, patient information is at risk during a security breach.

References

Arsene, L. (2015, April 10). Hacking Vulnerable Medical Equipment Puts Millions at Risk. Retrieved from http://www.informationweek.com/partner-perspectives/bitdefender/hacking-vulnerable-medical-equipment-puts-millions-at-risk/a/d-id/1319873

Battelle. (2015, April 22). Four Ways Hackers Are Exploiting Medical Devices. Retrieved from http://www.battelle.org/media/the-battelle-insider/the-battelle-blog/2015/04/22/four-ways-hackers-are-exploiting-medical-devices

Berger, D., & Manos, D. (2014, February 19). 5 ways to avoid health data breaches. Retrieved from http://www.healthcareitnews.com/news/5-ways-avoid-health-data-breaches?page=0

*Harman, L., Flite, C., & Bond, K. (2012). Electronic Health Records: Privacy, Confidentiality, and Security. *AMA Journal of Ethics*, *14*(9), 712-719. Retrieved from http://journalofethics.ama-assn.org/2012/09/stas1-1209.html

*HIPPA Journal. (2015, October 30). HOW PRIVATE ARE MEDICAL RECORDS? Retrieved from http://www.hipaajournal.com/how-private-are-medical-records-8166/

Horowitz, B. (2012, April 12). Patient Data Security Demands Strong Compliance, Proactive Policies: Report. Retrieved from http://www.eweek.com/c/a/Health-Care-IT/Patient-Data-Security-Demands-Strong-Compliance-Proactive-Policies-Report-384627

HRSA. (n.d.). How Do I Ensure Security in Our System? Retrieved from http://www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoiensuresec.html

*Johnson, M. (2011, September 26). Health-Care Industry: Heal Thyself. Retrieved from http://www.wsj.com/articles/SB10001424053111904716604576542380296355702)

Munro, D. (2015, August 3). Just How Secure Are IT Networks In Healthcare? Retrieved from http://www.forbes.com/sites/danmunro/2014/08/03/just-how-secure-are-it-networks-in-healthcare/

Niccolai, J. (2015, September 30). Thousands of medical devices are vulnerable to hacking, security researchers say. Retrieved from http://www.computerworld.com/article/2987737/security/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

Ragan, S. (2015, June 4). Attackers targeting medical devices to bypass hospital security. Retrieved from http://www.csoonline.com/article/2931474/data-breach/attackers-targeting-medical-devices-to-bypass-hospital-security.html

Schultz, D. (2012, June 3). As Patients' Records Go Digital, Theft And Hacking Problems Grow. Retrieved from http://khn.org/news/electronic-health-records-theft-hacking/

TrapX Labs. (2015). *ANATOMY OF AN ATTACK MEDJACK (Medical Device Hijack)*. Retrieved from http://deceive.trapx.com/AOAMEDJACK_210_Landing_Page.html

Zetter, K. (2014, April 25). It's Insanely Easy to Hack Hospital Equipment. Retrieved from http://www.wired.com/2014/04/hospital-equipment-vulnerable/