SAMPLE CASE STUDY STUDENT REPORT – UH Maui College

Discussed with students in the Allied Health and Nursing Program

Case Study on Common Security Vulnerabilities in the Local Healthcare Industry

Problem Statement: *The goal of Remote Patient Monitoring (RPM) is to provide a higher quality of care to more patients, decrease the cost of care for both patients and clinicians, and facilitate better access to care. However, this increased dependence on technology has resulted in a number of different cyber-attacks, the most common of which include Personal Health Information (PHI) theft of 5.6 million patients in 2017 (Landi, 2018) and the malicious tampering of approximately 36,000 vulnerable medical devices (Newman, 2017).*

Research Questions: *What vulnerabilities in RPM devices allow hackers to obtain PHI and tamper with medical devices?*

How can care facilities better fulfill the CIA Triad (confidentiality, integrity, and availability) to decrease occurrences of stolen PHI and medical device tampering?

Cybersecurity in Allied Health:

Vulnerabilities in Local Maui Industries

STUDENT NAME

University of Hawaii Maui College

Table of Contents

Overview

Before the 1960's, healthcare patients residing in remote parts of the U.S. would face a plethora of obstacles while attempting to obtain simple care. The lack of proximity to facilities and contact with clinicians proved challenging and problematic. A solution to this problem spawned in the late 60's in response to NASA's healthcare needs. Long duration space missions meant that astronauts needing consistent healthcare would need to find creative ways to monitor their health from afar (Gruessner, 2015). Thus, we see the very first indications of telemedicine and Remote Patient Monitoring (RPM) use. Today, RPM has become a crucial part of life for many patients residing in rural areas.

Healthcare is a monstrous industry that is certainly not immune to the turmoils of cyber-attacks. The more this industry evolves and attempts to adapt to our increasingly technologically dependent society, the more exposed to cyber-attacks companies and patients become. While RPM has been a revolutionary advancement for both patients and providers, it is also an adaptation what has contributed to cyber-attack vulnerabilities. The most significant threats are two-fold: theft of Personal Health Information (PHI) and the malicious tampering of medical devices. This paper will investigate 1) the vulnerabilities in RPM devices that allow hackers to obtain PHI and tamper with medical devices and 2) how care facilities can better fulfill the CIA Triad (confidentiality, integrity, and availability) to decrease occurrences of stolen PHI and medical device tampering. Results and analysis will be obtained through surveys of care facilities around the island of Maui to provide a localized interpretation of RPM cybersecurity problems.

Background

Technology is an integral part of society today. The innovation, convenience, and efficiency that modern technology provides is undeniable. Information technology serves as the backbone of many organizations and advances in this sector have equipped companies with the tools to store, manage, and protect exuberantly large amounts of data and information. But at what cost? The healthcare industry is one that is not immune to the increasing dependence on technology. Companies within this industry rely heavily on various types of technology, including information technology, to find better ways to assist and care for their patients.

Remote Patient Monitoring (RPM)

Currently, healthcare providers are looking to technology to facilitate higher quality and more frequent interactions between clinicians and patients residing in rural areas. One of these innovations is a type of telehealth delivery system called Remote Patient Monitoring (RPM). RPM uses information technology to gather patients' medical data (such as vital signs, weight, blood pressure, blood sugar, oxygen levels, heart rates, etc.) and transmit the data to centrally located providers for assessment and recommendation (Care Innovations, 2018).

This new telehealth technology has been instrumental in the advancement of modern healthcare access. Supporters of RPM claim that it is the key to unlocking what medical professionals call the "triple aim of health care." That is, the three most sought after goals in the industry: improving care experience, improving the health of more people, and lowering the overall costs of healthcare (Basile, 2018). A 2015 study examined 269,471 cardiac rhythm device patients and their RPM use. The study ultimately concluded that there was a positive correlation between the amount of time patients spent using RPM and survival rates (Varma, Piccini, Snell, Fischer, Dalal, Mittal, 2015). Additionally, this improved access to healthcare from the patients' home also significantly reduces costs for both the patient and the providers. A study conducted by a healthcare analytics company, Geneia, found that a savings of over $8,000 per patient per year can be attributed to the use of RPM (Zimmerman, 2016).

Maui is a great candidate for RPM programs. Approximately 23,000 Maui residents (14% of the population) reside in what the U.S Census Bureau would define as “rural” areas (Hawaii State Data Center, 2013). The nature of Maui’s landscape makes access to care inconvenient, difficult, or even impossible for residents depending on their degree of isolation.

RPM Cybersecurity Vulnerabilities

In an industry that handles such personal and sensitive information, effective cybersecurity measures are critical for patients’ safety and confidentiality. Unfortunately, despite the obvious benefits of RPM, this increased reliance on technology leaves vast amounts of data more vulnerable to attackers. According to an article from Reuters.com, the FBI warns patients about cyberattacks stating that “your medical information is worth 10 times more than your credit card number on the black market” (Humer, Finkle, 2014). Since RPM remains a relatively new concept, cybersecurity standards surrounding it are mediocre at best. For example, a study by the U.S. Department of Health and Human Services found that almost 33 million medical records were compromised in the year 2015 as a result of cyberattacks and, unfortunately, these figures are increasing. Cyberattacks in the healthcare industry increased by 72% from 2013 to 2014 (Alfson, 2016).

Research in this area has revealed how cybercriminals can use RPM to their advantage. Attacks via RPM have included theft of medical records used to impersonate patients, intentionally malfunctioning patients’ health machines, and tampering with submitted data (Metzger, 2016). A few of the most pressing cybersecurity considerations with RPM include user verification, authentication controls, and the use of outdated technology due to the industry's extensive testing and clinical trial laws (Sumra, 2018).

Problem Statement

The goal of Remote Patient Monitoring (RPM) is to provide a higher quality of care to more patients, decrease the cost of care for both patients and clinicians, and facilitate better access to care. However, this increased dependence on technology has resulted in a number of different cyber-attacks, the most common of which include Personal Health Information (PHI) theft of 5.6 million patients in 2017 (Landi, 2018) and the malicious tampering of approximately 36,000 vulnerable medical devices (Newman, 2017).

Research Questions

- What vulnerabilities in RPM devices allow hackers to obtain PHI and tamper with medical devices?
- How can care facilities better fulfill the CIA Triad (confidentiality, integrity, and availability) to decrease occurrences of stolen PHI and medical device tampering?

Review of Literature

Vulnerabilities in RPM result most commonly in two problems: theft of PHI and malicious tampering of medical devices. With Maui having a plethora of patients residing in rural areas, the local healthcare system is not immune to these issues.

Theft of Personal Health Information (PHI)

With the health industry's Internet of Things (IoT) continuously growing, PHI is becoming increasingly accessible to hackers. Not only are companies moving towards completely electronic patient medical records for reasons such as organization, volume of storage, and ease of use, but are also incentivized and often required by the American Recovery and Reinvestment Act as well as the Affordable Care Act to do so (Metzger, 2016). This combined with the $363 black market value of medical records (about 10 times that of a credit card number) puts PHI at high risk (Alfson, 2016). The U.S. Department of Health and Human Services reports that 2017 saw an estimated 477 healthcare data breaches resulting in approximately 5.579 million compromised patient medical records. A shocking 37% of these breaches can be attributed to hackers utilizing ransomware and malware. These attacks effected approximately 3.4 million patient medical records (Landi, 2018). Hackers see the value of PHI and are able to take advantage of the many vulnerabilities that PHI is subject to.

Malicious Medical Device Tampering

While theft of PHI can be devastating, malicious medical device tampering can be life threatening. Wearable medical devices are an integral part of RPM and include devices such as pacemakers, insulin pumps, vital patches, and more. There are currently 4 million medical devices in use (Robinowitz, 2018). Healthcare providers rely heavily on these devices to remotely obtain patient information. However, the cybersecurity of these have come under intense scrutiny as of late. Hackers can take advantage of vulnerabilities in these to infiltrate the devices and alter their performance to put patient's health at risk. In 2017 the FDA recalled 465,000 pacemakers that showed signs of security vulnerabilities (Morris, 2017). One of the biggest hurdles that healthcare providers face with efforts to combat these hacks is the medical device Time to Market (TTM). Wearable medical devices support and/or sustain human life and are, therefore, considered "Class III" devices according to the FDA. These types of devices take a minimum of 180 days to be approved after a lengthy submission and that is only if changes to the device are not required throughout the approval process (which there often are). By the time the device actually makes it to the market, the software is likely outdated which exposes it to cyberattacks (Sumra, 2018).

Local Implications

Hawaii, in particular, appeared on HealthcareITNews.com's list of "The Biggest Healthcare Data Breaches of 2018 (so far)." Hackers infiltrated servers of the Fetal Diagnostic Institute of the Pacific (FDIP) in June compromising approximately 40,800 patient medical records (Davis, 2018). However, despite these figures, the rural nature of the islands means that patients and healthcare providers still need to rely on RPM technology. According to the Health Resources and Services Administration (HRSA), the entirety of Maui County is considered what they would call "medically underserved," with the *most* underserved areas being Hana, Haiku, Molokai, and Lanai. The term "underserved is defined as areas that have 3,500 or more individuals per primary care physician. It is also known that approximately 20% of Maui County residents did not have a usual source of health care in 2013 (Belforte, Carter, Reinisch, Zheng, 2013).

Findings

Maui has a particularly unique health industry due to the rural nature of the area. RPM is used throughout the island and, therefore, cyber vulnerabilities are prevalent. A survey was conducted in order to investigate the implications of RPM vulnerabilities locally. The methodologies and results of this study are discussed below.

Methodology

This survey targeted several major organizations around the island providing various health services as well as a few very knowledgeable professionals in the field of healthcare. Some of the healthcare organizations targeted for the survey included Maui Memorial Medical

Center, Kula Hospital, and the Pacific Cancer Institute. Examples of healthcare professionals targeted in this study include University of Hawaii Maui College allied health department chair Anne Scharnhorst, campus health center director Denise Cohen, and nursing department program coordinator Kathleen Hagen.

The questions throughout this survey were formulated to investigate the two research questions described above, RPM vulnerabilities and facility fulfillment of the CIA triad. Questions 1, 2, 6, and 8 explored the priority that organizations place on vulnerabilities and were created gain insight as to what RPM vulnerabilities throughout Maui may be present that would contribute to risk of PHI theft or medical device tampering. Questions 3, 4, 5, and 7 pertained to the confidentiality, integrity, and availability of PHI in RPM and were intended to gather information about how local companies were currently fulfilling the CIA triad and how they could better fulfill the CIA triad in the future. Question 9 asked for any additional comments or information that would be valuable to the survey. Questions 1 – 7 required responses while questions 8 and 9 were optional due to the sensitive nature of question 8 and the expansive nature of question 9.

Results

The survey reached a total of 33 people/organizations and received 8 confidential responses. When asked about the priority of RPM vulnerabilities in the facility, 62.5% of respondents indicated that their facility considered RPM vulnerabilities a 5 (highest priority) on a scale of 1 to 5. When asked a similar question about the priority of employee cybersecurity training, 50% responded giving this topic the highest priority rating (5 on a scale of 1-5). The next three questions asked about the respondents' satisfaction with confidentiality, integrity, and availability of PHI in RPM (fulfillment of the CIA triad). Confidentiality received 50% response to a 3 satisfactory rating (neutral) on a scale of 1 to 5. Integrity was split evenly between a 3 and a 4 rating on a scale of 1 to 5 with 37.5% choosing each. Availability saw a 62.5% response to a 3 satisfaction rating on a scale of 1 to 5.

Respondents were then asked two open ended questions. The first question was: "what steps does your facility take, if any, to guard against RPM cyberattacks?" Common answers consisted of extensive employee training and risk management/assessment. Respondents were also asked: " In your opinion, what can be done to better protect patient PHI while using RPM?" Answers included more awareness to the problem. A few respondents mentioned that they did not even know this was a problem at all. Question 8 and 9 were not required as mentioned above and, therefore, did not receive significant responses to draw any conclusions.

Analysis

At the start of this study, it was understood that the use of RPM exposed patients and healthcare providers to a risk of cyber-attacks, particularly theft of PHI and malicious tampering of medical devices. However, it was unclear how these cases of increased risk affect the local healthcare industry here on Maui. This survey provided some interesting results.

Awareness

One of the most surprising findings of the study was a lack of awareness of the problem at all. Some of the google form responses included "be certain all staff are aware of the protections," "awareness," "education about the problem, I don't think this is talked about enough in Maui." It was interesting to see these responses from professionals within the healthcare industry because it seems to indicate that this problem is more detrimental than previously thought. As mentioned before, many infiltrations are very difficult to trace within systems so they can lay dormant for long periods of time before they perform an attack. If companies are unaware of these attacks, then the outcome can be much more damaging. And even after the attacks happen, it is still difficult to trace or find indications of the attacks. Therefore, PHI can be compromised without anyone knowing.

Employee Training

Another popular finding was attention to employee training. Respondents to the survey either indicated that their facility already focuses on these particular areas, they think these two things can be done to better protect patients, or both. This finding implies that the source of this problem stems from the human intervention part of the chain (password security, sharing computers, logging out, etc.). In a recent study of 400 U.S workers, 40% of healthcare workers indicated that they would share their work computer with a coworker. Additionally, 74% of healthcare employees could not identify a suspicious link. This indicates a severe misunderstanding of cybersecurity best practices (Donovan, 2018).

CIA Triad

When it comes to the confidentiality, integrity, and availability of PHI in RPM, the healthcare industry, specifically in Maui, seems to be lacking. While availability of PHI seems to be decent, confidentiality and integrity are compromised with this lack of awareness and employee training. Therefore, these two aspects of the CIA triad are not fulfilled.

Recommendations

These findings were very interesting and give great insight to the problem of cybersecurity here in Maui in general, what is already being done about it, and what still could be done about it.

Awareness

National Cybersecurity Awareness Month (NCSAM) is observed every October and was created in 2004 by the National Cybersecurity Alliance and the U.S. Department of Homeland Security (StaySafe). This type of attention is exactly what is needed in the healthcare industry. Organizations need to focus on making sure the issue of cybersecurity is well known so it can be taken seriously by all staff and steps can be taken to better protect against attacks. Some examples of ways companies could increase awareness is recognizing NCSAM every October, regularly sending out newsletters about changes and advancements in cybersecurity attacks, regularly educating on best practices, continuously performing risk assessment, and running/displaying reports about cyberattacks within the company and within different companies so staff can see trends. This will significantly contribute to the fulfillment of the CIA Triad.

Employee Training

Employee training is vitally important for companies to fulfill the CIA Triad and help protect the security of their patients. Some examples of effective employee training procedures include onboarding education and policies, computer use policies, password update/sharing policies, internet/email use policies, PHI handling policies, cybersecurity classes, regular refreshment on best practices, etc. Any procedures should be used not only upon initial hire, but should be continuously taught, practiced, monitored, and tested to ensure that employees are knowledgeable about the problem when they are onboarded, they continue to be knowledgeable throughout their employment, and are actively engaging in best practices in order to protect themselves, the company, and the patients.

References

Alfson, J. (2016). Patient Data Breaches: Threat to Health IT & Telemedicine in 2016 and Beyond. Retrieved from https://southwesttrc.org/blog/2016/patient-data-breaches-threat-health-it-telemedicine-2016-and-beyond

Basile, L. (2018). Telemedicine Deep Dive: The Power of Remote Patient Monitoring. Retrieved from https://www.telequality.com/blog/2018/4/11/telemedicine-deep-dive-the-power-of-remote-patient-monitoring

Belforte, J., Carter, J., Reinisch, F., & Zheng, D. (2013). Maui County Community Health Needs Assessment. *Healthcare Association of Hawaii*. Retrieved from http://hah.org/wp-content/uploads/2013/12/2013_maui_county_chna.pdf

Care Innovations (2018). What Is Telehealth? What Is Remote Patient Monitoring? How Are They Different? Retrieved from http://news.careinnovations.com/blog/what-is-telehealth-what-is-remote-patient-monitoring-how-are-they-different

Davis, J. (2018). Ransomware attack on fetal diagnostic lab breaches 40,800 patient records. Retrieved from https://www.healthcareitnews.com/news/ransomware-attack-fetal-diagnostic-lab-breaches-40800-patient-records

Donovan, F. (2018). Healthcare Workers Uninformed About Cybersecurity Best Practices. *Health IT Security.* Retrieved from, https://healthitsecurity.com/news/healthcare-workers-uninformed-about-cybersecurity-best-practices

Gruessner, V. (2015). The History of Remote Monitoring, Telemedicine Technology. Retrieved from https://mhealthintelligence.com/news/the-history-of-remote-monitoring-telemedicine-technology

Hawaii State Data Center. (2013). *Urban and Rural Areas in the State of Hawaii*. https://doi.org/10.1038/bjc.2011.483.

Humer, C., & Finkle, J. (2014, September 24). Your medical record is worth more to hackers than your credit card. *Reuters*. Reuters. Retrieved from http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Landi, H. (2018). 2017 Breach Report_ 477 Breaches, 5. Retrieved from https://www.healthcare-informatics.com/news-item/cybersecurity/2017-breach-report-477-breaches-56m-patient-records-affected

Metzger, K. (2016). Cybersecurity and Data Protection: Helping Healthcare Clients Protect Patient Information. Retrieved from https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/06/03/cybersecurity-and-data-protection-helping-healthcare-clients-protect-patient-information.aspx

Morris, C. (n.d.). 465,000 Pacemakers Recalled on Hacking Fears. Retrieved from http://fortune.com/2017/08/31/pacemaker-recall-fda/

National Cybersecurity Awareness Month (n.d.). StaySafe. Retrieved from, https://staysafeonline.org/ncsam/

Newman, L. (2017). MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE. Retrieved from https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

Robinowitz, J. (2018). The Problem with the Medical Device Industry that The Bleeding Edge Ignores. Retrieved from https://www.cybermdx.com/blog/the-problem-with-the-medical-device-industry-that-the-bleeding-edge-doesnt-address

Varma, N., Piccini, J. P., Snell, J., Fischer, A., Dalal, N., & Mittal, S. (2015). The Relationship Between Level of Adherence to Automatic Wireless Remote Monitoring and Survival in Pacemaker and Defibrillator Patients. *Journal of the American College of Cardiology*, *65*(24), 2601–2610. https://doi.org/10.1016/j.jacc.2015.04.033

Wareable. (2018). How FDA approval affects your wearables, and how it's going to change. Retrieved from https://www.wareable.com/wearable-tech/fda-wearables-state-of-play-239

Zimmerman, B. (2016). Remote monitoring could save more than $8,000 annually per patient, study finds. Retrieved from https://www.beckershospitalreview.com/quality/remote-monitoring-could-save-more-than-8-000-annually-per-patient-study-finds.html