IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy

Haidhar Athir Mohd Puat* and Nor Azlina Abd Rahman*

Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur

*Corresponding author e-mail: nor_azlina@apu.edu.my

Abstract. Internet of Medical Things or IoMT is known as the most wanted technology in the healthcare sector. Almost 420 million connected device have been deployed globally to all healthcare facilities and with around 70 million more devices expected to be deployment by early of 2020 [4]. This types of technology and connection of medical devices to healthcare IT framework is not only beneficial to the patients but facilitates the structure of the traditional healthcare system of delivery information from department to department in healthcare environment. As a result to this budget for healthcare management and handling can be reduce and use for better improvement. However, with the advantages of IoMT, all the security behind every IoMT devices need to be considered. This paper is reviewing on several IoMT devices such as smart pen, implantable cardiac devices (pacemaker), wireless vital monitors and several other devices in terms of its functionality and vulnerabilities that might expose the devices to the attacker. More detail discussion is focusing into Pacemaker which is one of the IoMT devices. Several security strategy and solutions to minimize the vulnerabilities of IoMT devices are also being discussed.

Index Terms. IoMT, pacemaker, vulnerability, security strategy, security solutions

1. Introduction

Most of IoT devices are vulnerable to attack due the runs on legacy operation system and often build on outdated software. Devices such as pacemakers, X-ray machines and CT scanners are running under an outdated software which are not patch routinely .The devices of Internet of Things (IoT) are constantly collecting and storing huge amount personal information of individual, which makes them more appealing target for cyber criminals and it is the mostly easiest entry point for hacker to attack to Information Technology (IT) network where more critical data is stored.

Medical record is less valuable stolen medical records is more cheaper to obtain rather than hacking them which led to ‘threat actor’ factor and to find a more beneficial alternative to exploit may involving hacking medical device to access medical information of patient or healthcare data. Evolution of cyber-attack schemes, where healthcare database is at risk when medical devices is involved. IT network that is connected to the medical device which is able to exploit with a ‘back
door ‘ led hacker to find a newer strategy method such as Distributed Denial of Service (DDOS) attack to compromise the network.

The prioritize of patient health over cybersecurity is the No .1 priority of patient care rather than the prevention of cybersecurity is not the main concern of clinicians. With this in mind, the upgrading and patching up of cybersecurity flaws should also be a priority for medical devices. If not some clinician may go rogue for them to keep up with the workflow by using unauthorized applications. No mandates for Food and Drug Administration (FDA) issued security recommendation. If healthcare organisation and manufacturers struggle to adhere the FDA’s guidelines to reduce device security risks, a right firm to mandate should be set up to review all these crucial issues. Out of 100 percent only 44 percent of medical devices in healthcare organisation adopt the FDA guidelines [1].

For example, ultrasound machine is using a technology that is far beyond than we expected to achieve, thought recent years ultrasound machine have the ability to share data with patient and doctor in an instant. Even though these innovations have not expanded to IT security, but the among of workload can be reduce in which machine sit and are connected to transfer all recorded image to the doctor on call. Over the year 2019 march , approximately one million of patient in the united states medical database was leaked in data breaches. This lead to one of many medical centre in Michigan was force to close down, this show that healthcare is popular among hacker target. Never less, with all the report of the weakness of cloud, mobile and IoT platform in the network healthcare organization still not doing any changes to protect from this threat [2].

2. Internet of Medical Things (IoMT) Security Issues
The IoMT market consists of smart devices, such as personal Tracker and smart wearable to track their day to day perform are among the highest device that have been purchases in 2019 [3]. Not to forget also medical/vital monitors that is made firmly for health care use on the body which provide a precise real time location and other service is tend to digital attack by intruders. This types of technology and connection of medical devices to healthcare IT framework is not only beneficial to the patients but facilitates the structure of the traditional healthcare system of delivery information from department to department in healthcare environment. As a result to this budget for healthcare management and handling can be reduce and use for better improvement. However, with many advantage of IoMT, people need to understand all the security behind every IoMT devices.

Ensuring IoMT network is really critical as it not only profit the healthcare infrastructure and device but eliminating the potential threat that can possibly led to digital attack and data privacy breach. IoMT is known as the most wanted technology in the healthcare sector. Almost 420 million connected device have been deployed globally to all healthcare facilities and with around 70 million more devices expected to be deployment by early of 2020 [4]. There are several numbers of medical devices was brought up concerning the cybersecurity issues which are related to the CIA security triad consisting of Confidentiality-Integrity and Availability requirement emphasizes HIPAA compliance and guided policies for information security within an organization. There are a few medical IoT device that are proven to be more vulnerable and vital in the network as discuss in this section [5].

2.1. Infusion and Insulin Pumps
Among thousands of devices Insulin Pumps is one of the majorities of IoT medical devices made to ease the process of patients in treating their diseases. Insulin Pumps have the ability to remotely manage and administer blood, saline, and other medical fluids. This device is control with IoT infusion from medical professionals to provide a quality assuring of the patient and reducing the cost of treatment. This technology allows several infusions to be operated from a main single hub simultaneously. Which led to malicious attack by exploiting the connectivity of the devices in delivering the right amount of drug based on medical records.
2.2. **Smart Pens**

With rapid development of medical devices like smart pens digital devices and touch screens makes the process of recording patient care documentation as piece of cake. However, storing treasured and sensitive patient information in a smart pen is a major issue in compliance of HIPAA security. This have caught the attention of cyber criminals to exploit the smart pens vulnerability by accessing patient data as stated by cybersecurity researcher in 2017. Based on the research conducted on smart pen, the researcher managed to find an entry point to access into information technology writ large including personal patient information and medical history.

2.3. **Implantable Cardiac Devices**

As Among hundreds of medical devices out there, Implantable Cardiac Devices like pacemaker is amongst the top and famous IoMT devices to treat heart failure patient. Even though it helps patient but yet security concerns are discovered. These disruptive innovation in healthcare devices is not 100% safe but also vulnerable to any potential security threat that pose a risk to patient health. Especially when we talk about pacemaker, as this device act as a device that produce electrical impulses that makes the heart muscle chamber contract to pump blood. Pacemaker have a potential to stop which to killing the patient by just send an attack as simple as DDOS or denial-of-service attack [5].

2.4. **Wireless Vital Monitors**

Wireless Vital Monitors is one of the common and famous devices used by healthcare worldwide .This device help to transmit data like heart rate, sugar level and many more vitals immediately to the physician without having to go through a physical examination hourly even though the patient has been discharged. Moreover, patient also have the ability to check and automatically record their health condition constantly via Bluetooth. All alerted on any abnormal vitals in patient condition will be directly notified through a mobile phone, applications, other devices. as a result to this crucial data is transmitted wirelessly and it is exposed for men in the middle attack to occur.

2.5. **Thermometers and Temperature Sensors**

Have you heard a casino was hacked via their lobby fish tank by changing the temperature. The reality is far more important where fish is not on the line but human life. With IoT being a big part of healthcare environment in terms of monitoring temperature, sensor and etc makes it more vulnerable to unforeseeable attack. Today's sensor technology is cheap, and operations management are more likely to adopt this tech to manage almost everything from Hvac to normal refrigeration.

3. **Implantable Cardiac Devices (Pacemakers)**

The heart is one of the body's most essential organs in the human body and approximately 550,000 new cases are diagnosed in the U.S. each year. However implantable cardiac device is an alternative to treat patient suffering from major heart problem. With IoMT technology in the market, it plays an important role in treating heart problem especially when comes to heart failure [6]. The concept of implantable device was discover over 60 year over with a purpose to manage arrhythmias and heart failure. Ever since then, devices like this has become a solution in improving patient condition suffering from bradyarrhythmia's, atrial fibrillation, ventricular arrhythmias, and heart failure. These medical devices are no more a new thing but a common method of care in managing patient health. These devices include implantable cardioverter-defibrillators (ICDs), cardiac resynchronization therapy (CRT) and also pacemakers [7].

Medical devices like pacemaker and devices used to program them is another disruptive innovation in healthcare. A cardiac pacemaker is a device that produce electrical impulses which is delivered by electrodes to make the heart muscle chamber to pump blood by contracting. In doing so it replaces and synchronizes the function of electrical conduction system in the heart. Pacemaker is a small device which is position in the chest and abdomen of the patient shown in figure 1 to assist abnormal rhythms.
on the heart. as explained above, pacemaker transmit electrical pulses to stimulate the beat of the heart on a regular rate help patient suffering from arrhythmias (ah-RITH-me-ahs) that have unstable heart rhythm [8].

Figure 1. Pacemaker [8]

3.1. Who needs a Pacemaker

Pacemaker has always been a way treating patient who commonly suffering from bradycardia and heart block. Bradycardia is a disease that the heartbeat of the individual is slower than normal. Bradycardia are more prone to the age and physical condition for example, elderly people. For instance, normal adult has a resting heart rate below 60 beat per minute (BPM) is consider a bradycardia sickness. But it’s an exception if the individual heart rate falls below 60 BPM during a deep sleep. And active adult like athletes where their resting heart rate is slower than 60 BPM [8]. In addition, patient with heart block as a disorder where the electrical signal is disrupted or slowed when transmitting to the heart. This can occur as a result of aging or major damage to the heart due to heart attack. Not to forget, also suffering from muscle and nerve disorders can be another reason of heart block such as muscular dystrophy.

The recommendation of implanting a pacemaker can be varies especially when age increase or any heart disease that damages the sinus node which help in correcting the pace of your heartbeat. As patient suffering from this, they tend to have a slower heart rate or long pauses between each beats. as a result. It can cause irregular heart rhythm between every beats, maybe slow or fast. This disease is known as sick sinus syndrome. Furthermore, if you always faint or having symptoms that cause slow heartbeat. For example, when your main artery in the neck which provide blood to brain is sensitive to pressure. By just twisting your neck could led in slowing the heart rate. Which resulting insufficient of blood flow to brain can cause collapse and faint is a possible reason for the doctor to recommend a pacemaker to managed the sickness.

Moreover, if a person suffered from muscle problem especially relating to the heart muscle which cause signal impulse moves slowly through the heart muscle. With pacemaker ability to provide CRT or cardiac resynchronization therapy to help coordinating the electrical signaling among hearts lower chambers is a good alternative in treating this sickness. Finally, arrhythmia or famously known as atrial fibrillation is the only medical procedure to treat this type of disease. to generate a normal heartbeat procedure of implanting a pacemakers is required. Not to forget also, patient that have long QT syndrome where they are always at risk to dangerous arrhythmias are considered to go through the procedure.
3.2. How Does Pacemaker Works

Every pacemaker comprises of a battery to generate power, computerized generator to run the system on the devices and sensors with wires on the tips that are called as electrodes. The battery generates power which are surrounded by a thin metal box consisting wires connected to the heart. The electrodes identify the heart’s electrical activity and transmits every data gathered to computer generator through the thin wires to help controlling and monitoring heart rate rhythm [8]. However, heart beats that is found abnormal, the computer immediately transmit electrical pulses to the heart via generator instruction. With an instant the wires that contain pulses is travel rapidly to the heart. In addition, modern pacemaker that are more efficient to monitor breathing pattern, blood temperature and others can adjust the rate of the heart to change based on your activity.

Furthermore, every pacemaker comes with storage to store record of every heart electrical activity and rhythm. This reading will be review by the doctor to determine on the optimization of the pacemaker to the host body. The programming of the pacemaker is conducted with an external device using a needle inserted directly to pacemakers. But current pacemaker in the market, this adjustment can be handled wirelessly. There are three wires that are each located in different chambers of the heart. Firstly, pacemaker wires in single-chamber normally transmit pulses to the right ventricle (heart lower right chamber). Secondly, dual-chamber wires transmit pulses to the right atrium (heart upper right chamber) and the ventricle on right. The timing of contraction of the two chambers is coordinate by the pulses.

Lastly, wires in a biventricular pacemaker transmit to both ventricles and atrium. Coordination of electrical signaling among two ventricles is handle by the pulses. This pacemaker is known as CRT devices. Based on figure 2 shows a pacemaker with a cross-section of the chest. Figure 2A shows the size and position of dual-chamber pacemaker in the upper chest. Electrodes seen above in the right atrium of the heart and upper chest with ventricle inserted through the vein. Figure 2B shows heart muscle stimulated by electrical electrode. Figure 2C shows size and position of single chamber on the upper chest.

Figure 2. Pacemaker with a cross-section of the chest [8]
3.3. Vulnerability of pacemaker

3.4. Heart disease is a primary cause of death in the United States. With a treatment to treat chronic cardiac disease in maintaining a healthy heart rhythm to provide patient with good prognosis. Especially, patients that may have suffered heart damage probably from heart attack or shortness of breath and genetic predisposition such as ventricular tachycardia or ventricular fibrillation. However, pacemaker safe the day by providing a way to treat major heart disease as stated above [9]. With high tech pacemaker made today have made an impact for comprehensive care especially for patients who require constant check and intensive control of their health. Now with the combination of cloud connected devices allow exchange of information between health care professional and machine’s vendor such as patient location data. Although the pacemaker is not always active, these connections are used to configure and set the parameters of the devices to remotely monitor its activity and to transmit data to its carrier. This could make patient vulnerable to hackers. It’s important to understand how we use this tool and how patient are protected. in simple word devices that are related to in sending and receive data through a network is potential for hackers to interrupt the wireless communications between host device and server.

All connected device needs to consider if and how may be hacked. A team of expert and ethical hackers had worked together to determine the potential vulnerabilities that may found in a pacemaker device. Despite some research have begun working in this field it hasn’t been easy as manufacturers do not want to give details on the design or specifications of the running software. Back on 2008 in University of Michigan of United States, a teams of scientists from Archimedes center for medical Device Safety confirmed that pacemakers is possible to hacked, which allow the extraction of personal information and modification of system configuration putting patients life on risk. This news on the discovery was shared among researcher claiming that a well-known hacker known as Barnaby Jack developed software to hack pacemakers and is able to kill anyone wearing one globally regardless the distance. Before the methodology was proved at the Black Hat conference in Las Vegas he passed away. If this was true, that there is method to have full control of a running pacemaker via an internet connection, could led to a major breakthrough in world of cybersecurity. However, no published research could disprove or confirms the concept [10].

Recently “the department of homeland security warned that hacker could wirelessly access implanted pacemakers made by Medtronic”. Medtronic recently voluntarily recalled some of its insulin pumps for similar reasons. Even though the attack must be within close proximity to the victim or only when the device is connected to the internet for transmitting and receive data. According to “Medtronic designed the device’s communication protocol; so that it doesn’t require any authentication, nor is the data encrypted.” Vulnerability of the device making real risk of being hacked and potentially modifying its behavior could outcome in fatal way [11]. Moreover, with a simple of denial-of-service attack against a pacemaker can kill a person. Transmitting an unauthorized radio commands that could reconfigure the implant medical device to drain the battery so boom or transmit multiple electrical impulse to the heart leading to rapid heart rate to their deaths.

Finally, in the case of offline pacemaker where the device has zero connection to the outside world or known as close circuit pacemaker are still at risk. Pacemaker that are preprogrammed and does not provide remote monitoring and instant access of heart
rhythm records an also vulnerable to security breach. During routine checkup, medical professional access pacemaker information via inserting electric probe toward patient pacemaker. Corrupted or unpatched machines might contain malicious malware that expose patient device risk of transmission malware toward the close circuit pacemaker during information gather. The malware transmitted onto the device could corrupt the device and led to malfunction.

4. Security Strategy for IoMT devices

With all thousands of endpoint implemented in Healthcare organizations these days that are vulnerable to a security breach and security disruption can cause chaos in the organisation. Prevention to any of threats at the bay of endpoints requires substantial investment in cyber defences. Even though more and more numbers of medical devices are developed, the evolution of security automation process are needed. There are many measures to be considered when implementing medical device in their organization. Listed down below are some practices for organization to create a holistic, effective device security strategy around software automation [12]:

Make process easier – On the off chance that clinicians need to physically update the medical device in order to use it, or are given a procedure out security method to follow for them to utilize the device capability, they are going to search for options, and most are likely not secure enough for the organization’s network. With a good security process that is compatible with clinician typical workflow will make clinician life easier and they will be willing to use the system.

Have a device security breach plan – if any issue or flaws is discovered in any devices a right process and protocols is required to go through. As all the protocol and process predefined for both the IT professional and clinician to address and move forward on any security breach detected. With outstanding device assessment automation tools use can assist the IT professional to verify any breach location and alert the clinician on duty to take the right action. As a result, it will manage security risk issues on real time basis.

Investment on cyber defenses technology – without a good digital technology platform, it will be very difficult for us to tackle any security threat that are there to strike within IoMT devices. A framework which involves right automation technology in handling security patches, cloud-based security solution and tools to monitor traffic across the network are required. On another hand, third party security experts in helping to handle certain tasks and most importantly organisation should also consider micro segmentation to protected devices from any harm in a larger scale.

Approximately 30 hospital has 31 percent vulnerable devices laying around running. Which provide access for intruder to attack and compromise the organisation in an instant. Fortunately, a big number of threats are related to IoMT devices, which can be tackled with a combination of good governance and system solution [4]. Such as

- Each devices password is set unique and strong credential is used
- Patching up software as a routine schedule and check for any vital patching needed
- Maintain software by auditing every device to check whether there is a rogue software and perform right method to eliminate the issue
- Avoid unauthorized access to the network by configuration of the network access control system with extra vigilant security policies
- Conduct a continuous surveillance of every IoMT traffic in and out of the network to accurately detect and resolve and potential vulnerabilities. This malicious activity reviewing is really important to determine and protect any risk in the network

5. Security Solutions for IoMT
Security vulnerabilities highlighted above plays a significance roles in healthcare organization and must be number one priority in IT security. Even though security issues in security protocol standardization is a major concern for IoT devices especially Internet of Medical Things (IoMT) devices, we cannot denied that there are still healthcare organization out there that manage to protect their patient's record securely. With right and good exposure toward security concern planted in every staff in healthcare organization is important to achieve a goal that is mutual for the organization and customer(patient). Among multiple measurement listed, one of the most curial practices is to training every healthcare staffs to be alert in any entry points that exist across their network. The above-mentioned security vulnerabilities highlight the importance healthcare organizations must place on their IT security posture. While there are still issues and vagueness when it comes to, there is still much that healthcare organizations can do to protect their patients’ data. There may be hundreds, thousands medical or IT devices connected to the IT network, and if one the hardware or software is vulnerable to any security breach the right measurement taken is important. Determine every single attack and vulnerabilities in a network is out of question. However, it is vital for healthcare organization to acquire a precise and trusted advanced prevention security solution in their IT evirmonet.as this can help to capture any inevitable attack that are willing to exploit these vulnerabilities.

Besides that, Dividing can never be overestimated, separation of patient data from the entire IT network, provides IT experts to a better view of traffic in and out of the network, this will smooth the work of detecting unusual changes that could implies to a compromised devices or breach in data. To prevent data stealing or malware encryption effecting the network further across the network segmentation is a good practices rather than isolating each the threat found to avoid spreading of damage any further. In addition, there are no real evidence to-date of a hacker harming a patient through a medical device, which led researcher from cybersecurity filed to indicate that every IoMT devices is vulnerable to any sort of cyber-attack and these vulnerabilities must be addressed appropriately. That's where a Managed Detection and Response (MDR) service comes into play. When attack is targeted to a vulnerable IoT device, a constant monitoring by security analysts are required to determine any abnormality in the network and explore further on the issues found. If indeed any security issues or incident occurred, security analyst on duty can help and resolve the threat instantly without going through a process of escalation. Eventually, outsourcing or in house emergency respond team is crucial to help coordinated a good strategy for detection and response. This is the only and best way to avoid and reduce any security breach and to operate Medical IoT devices safely for patients in healthcare organization [5].

Finally, apply segmentation should not only focus of patients but also healthcare personnel within the organization who are authorized to access to the system provided that a required perform their roles. Not to forget also, laying out good IoT landscape in healthcare environment is good method to manage and handle IoT risks that may or not occur. With the evolution of technology and the exponential rate we now, medical IoT is the future of healthcare organization as its promises to support expanding patient engagement and enhance delivery of care. Even though the innovation of Medical IoT is advance and electrifying to us, we should not forget the significant of security behind every medical device used. Upon the rate of IoT progress moving forward to healthcare industry, businesses also should be aware and cope with handling data privacy of their client as per-stated are patient record. CISOs and IT managers should always be up to date and caution at all time to detect any vulnerabilities IoT found on their organization, by taking a right measure to prevent any security issues escalating. In addition, taking action like inventory, manage & monitoring the deployment of IoT technology in and out of the organization is vital in reducing cyber risk occurrence.

6. Conclusions
In conclusion, deployment of IoMT devices to all healthcare organization is a good step in moving forward to the era of cloud computing and AI artificial intelligent where innovation or discovered of
diseases can be shared to multiple healthcare organization for research purpose. Even though, there are many advantage of connected medical devices offers but we can denial that intruder will always find vulnerability to attack the organization. This does means we should stop innovating for more advance technology to improve daily life issue. IoMT provide patients & healthcare with potentially life-saving information which support effective method of managing their information. However, good awareness practices should be implemented in every organization including healthcare field to avoid any chances of data breach. They must be aware of vulnerabilities that is related to the devices and also network that may or may not occurred as a result to devices been attack.

In addition, segmentation of network is also a best practice allowing IT professional or manager in sector of healthcare to confidently adopt new digital medical solutions as delivering an additional layer of security in the network to guarantee data protection and price, without compromising consistency or performance. Almost 32 million patient records have been in invaded [13]. Violation of hacker has becoming a crucial issue and prone industry to ransomware and phishing. With evolution of medical devices the security measures taken address these issues may not be as effective as we excepted especially from the leaders. Even though the security threat and matters are constantly going up the scale leaving healthcare industry behind [14].

Devices that are related to medical are more vital as sensitive personal information is at risk and have become a major security concern. Device with wireless communication technology is more prone to be compromised. This could occur when data is intercept by a man in the middle during a transmission over an unsecure channel wirelessly. The information intercept could be a sensitive data of the patient of the network as resulting to full access of the device in the network. With a good awareness program in the healthcare sector to educate, motive and stimulate first line of security resource including doctors and other employees. A good security practices with suitable security action taken will provide staffs a clear direction and education and sufficient training on security breaches recovery and measures.

Patient must be made aware of their device configurations and securities. That frequent update or diagnostic check must be done to keep devices functioning properly and well secured. Routine check-up at the medical centre should include patient general well-being and as well the device diagnostic-check and securities by machine vendors. Each medical professional practicing with pacemaker should have underwent an intensive workshop regarding the device’s vulnerabilities of the devices and early sign of temperament for early intervention. Did you know if medical devices doesn’t get a right update when it is needed, could led to security vulnerability exploitation and puts data of the patient at risk. With update process it helps to patch any security issues found on the device. This approach provides a security alternative by the manufacturer to revamp their unsecure security design used. Patching up medical devices enable it to receive the proper measure in improving functionality, compatibility and safety of patient data. Awareness towards the community regarding the vulnerabilities of medical devices could open to new researches in the field.

For close circuit devices or offline pacemaker each companion devices should be regularly updated and maintained. This could help in ensuring from risk of transmitting malicious malware. Implementing security alert patches within pacemakers is a measure to provide protection against device tempered. Pacemakers should be equipped with notification if device being hacked. This alert must be informed towards the first emergency response team and the machine vendors which should give patients an idea that their device being tampered. This will bring an immediate response to patient care. As per overall, can conclude that implant cardiac defibrillators, pacemakers or any wireless hospital equipment is constantly at risk to security breaches. Teamwork of researcher, manufacturers and industry are required in producing devices that are safer while complying with the FDA guidelines. Or else, the risk of attacks will continue to increase with advances in technology. Finally, implementation and enforcement of cyber hygiene practice, guarantees their patient records and finances & reputation in the organization are safe in the hand of IT security teams.
References

[1] Synopsys, Inc. . (May 25, 2017). Retrieved from https://www.prnewswire.com/news-releases/synopsys-and-ponemon-study-highlights-critical-security-deficiencies-in-medical-devices-300463669.html

[2] HIPAA Journal. (2019). Healthcare Data Breach Report. Retrieved from https://www.hipaajournal.com/march-2019-healthcare-data-breach-report/

[3] The Expresswire. (6 sept, 2019). Smart Tracker Market Analysis 2019 to 2025. Retrieved from https://www.marketwatch.com/press-release/smart-tracker-market-analysis-2019-to-2025-report-includes-threat-of-new-entrants-demand-supply-investment-opportunities-and-forecast-2019-09-06

[4] Vashkover, A. (13 sept, 2019). Understand how to secure IoMT devices against cyberthreats. Retrieved from https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Understand-how-to-secure-IoMT-devices-against-cyberthreats

[5] Langston, F. (n.d.). Top 6 Hackable Medical IoT Devices. Retrieved from https://ci.security/resources/news/article/top-6-hackable-medical-iot-devices

[6] Emory Healthcare 2019. (n.d.). Heart Failure Statistics. Retrieved from https://www.emoryhealthcare.org/heart-vascular/wellness/heart-failure-statistics.html

[7] Banchs, S. M. (4 february, 2012). Implantable Cardiac Devices In The Treatment Of Arrhythmias And Congestive Heart Failure. Retrieved from https://www.uscjournal.com/articles/implantable-cardiac-devices-treatment

[8] U.S. Department of Health & Human Services. (n.d.). Pacemakers. Retrieved from https://www.nhlbi.nih.gov/health-topics/pacemakers

[9] Alton, L. (13 july, 2018). Health Vs. Hackers: Cloud-Connected Cardiac Care. Retrieved from https://www.digitalistmag.com/iot/2018/07/13/health-vs-hackers-cloud-connected-cardiac-care-06178927

[10] Panda Security. (n.d.). The Internet of Things: Pacemakers. Retrieved from https://www.pandasecurity.com/mediacenter/security/internets-new-heartbreak/

[11] JOHNSON, D. (18 july, 2019). Can Pacemakers (and Other Medical Devices) Really Be Hacked? Retrieved from https://www.howtogeek.com/427904/can-pacemakers-and-other-medical-devices-really-be-hacked/

[12] Young, A. (18 APR, 2018). What Internet of Medical Things (IoMT) Devices Mean for Healthcare Cybersecurity. Retrieved from https://healthtechmagazine.net/article/2018/04/The-Internet-of-Medical-Things-Opens-Health-Organizations-Up-to-More-Threats

[13] Esch, J. (26 august, 2019). Implanted Medical Devices and Vulnerabilities to Hackers. Retrieved from https://www.medtechtelligence.com/column/implanted-medical-devices-and-vulnerabilities-to-hackers/

[14] Protenus. (july, 2019). 32 Million Breached Patient Records in First Half of 2019 Double Total for All of 2018. Retrieved from https://www.prnewswire.com/news-releases/32-million-breached-patient-records-in-first-half-of-2019-double-total-for-all-of-2018-300894237.html