Fall 2020

Internet of things medical devices cybersecurity

Mohamed Ali

Internet of Things Medical Devices Cybersecurity

Mohamed Ali
Iowa State University
Ivy College of Business
Ames, Iowa 50011
mali@iastate.edu

Internet of Things Medical Devices Cybersecurity

Abstract

Taking appropriate precautions and security is particularly important when knowing the level of risk at any time. Tightly organize the design and distribution of medical devices and equipment. Healthcare is becoming more connected with hospitals, doctors, and nurses increasingly reliant on internet-connected devices and sensors to monitor patients. However, while this can help provides better and more personal treatment, it also carries risks because many Internet of Things (IoT) medical devices are vulnerable to cyberattacks. IoT's discovery has enormous benefits for users; However, some of the challenges appeared with this invention. This paper examines the environment adopting IoT devices to classify the security challenges and their effect on interoperability in a medical ecosystem. Also, the goal of this study is to find solutions that address the need for IoT device security by today’s healthcare delivery organizations.

i. Introduction

Connected medical devices play a critical role in patient safety today. The rise of these devices represents significant innovations and inpatient care. IoT medical devices help doctors share information with other healthcare providers and provide access to cloud computing. However, we all need to realize that the security of these medical devices is unique, and it is especially critical because patient lives and privacy are at risk. However, while this can help provide better and more personal treatment, it also carries risks because many IoT medical devices are vulnerable to cyberattacks.

Cyber-attacks on medical devices may put patients at risk. Internet of Things technology allows healthcare providers to reduce costs and improve patient care delivery. Specialists expect that the IoT medical device business reach $ 136.8 billion worldwide by 2021.[1]. IoT technology manufacturers are computing to meet the market, although presenting immeasurable cybersecurity risks to healthcare organizations and their patients. By the Internet of Things (IoT) approach, businesses are experiencing a digital transformation more significant than the PC and Mobile revolutions combined – and healthcare is no exception. The latest type of connected medical devices conveys the commitment of improved patient care, more reliable clinical data, improved efficiency, and reduced costs – but they also bring increased security risks. According to a commissioned study conducted by Forrester Consulting, 63% of healthcare delivery organizations have experienced a security incident related to unmanaged and IoT devices over the past two years.

[1] *"Internet of Things (IoT) Healthcare Market Is Expected to Reach $136.8 Billion by 2021 – Cole of Duty." Coleofduty, 4 June 2020,* coleofduty.com/news/2020/06/04/internet-of-things-iot-healthcare-market-is-expected-to-reach-136-8-billion-by-2021/. Accessed 17 May 2020.

"The Cybersecurity Improvement of IoT Act of 2017", which was introduced on August 1, 2017, by four members of the US Senate, was developed in response to a series of cyberattacks related to the Internet Things that occurred in 2016.[2] The law sets this improvement threshold Minimum cybersecurity requirements for connected devices purchased by the United States government, including:[3]

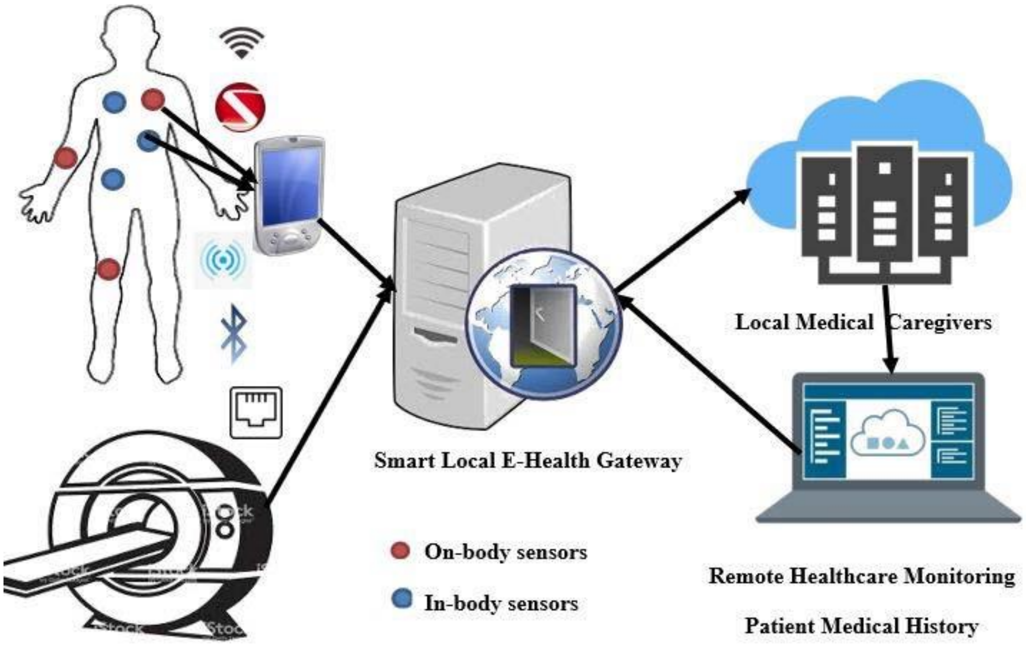
- Requiring vendors to ensure that their equipment is accessible, relies on industry-standard protocols, does not use encrypted passwords, and does not contain any known security vulnerabilities.
- Require vendors selling IoT devices to submit a written certificate stating that the device does not, at the time of submitting the offer, contain any hardware, software, or firmware components with any known security vulnerabilities or defects. If the seller identifies weaknesses, he must uncover the reported correction promptly.
- Require each enforcement agency to account for all internet-connected devices used by the agency.
- In conjunction with NIST, define specific measures, such as network segmentation, for agency recruitment.
- Department of Homeland Security (DHS) Department of Protection and Directive of National Programs (NPPD) to develop harmonized disclosure guidelines, allowing researchers to discover vulnerabilities and share with sellers.

[2] Krebs, B. (2017, August). *Tag: IoT Cybersecurity Improvement Act of 2017*. Krebson Security. https://krebsonsecurity.com/tag/iot-cybersecurity-improvement-act-of-2017/

[3] Security, H. N. (2017, August 2). *US senators introduce bill to improve IoT security, protect researchers probing it*. Help Net Security. https://www.helpnetsecurity.com/2017/08/02/iot-security-legislation/

- Request the event report, with recommendations for updates, to present to Congress after five years.[4]

The IoT healthcare security solution is not yet robust but continues to improve. Hence, it is arduous to name, and divine all potential risks, threats, and vulnerabilities associated with the IoT medical domain. Nevertheless, there is a requirement for the security establishment effort to promote a risk management model before any security incident occurs.[5]



A	B	C

Figure 1: Devices Communication architecture

[4] Sterling, B. (2020, November 18). *Spime Watch: the fact sheet for the Internet of Things Cybersecurity Improvement Act of 2017*. Wired. https://www.wired.com/beyond-the-beyond/2017/08/spime-watch-fact-sheet-internet-things-cybersecurity-improvement-act-2017/

[5] *Islam, S.M. Riazul & Kwak, Daehan & Kabir, Md. Humaun & Hossain, Mahmud & Kwak, Kyung.* (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access. 3. 678-708. 10.1109/ACCESS.2015.2437951

ii. Communication Architecture

It is essential to understand the communication architecture that devices support to communicate with healthcare providers, cloud-supported data hubs, hospital systems, and systematic data analysis. The network type is displayed in Figure 1 to demonstrate communication progress and potential attack patterns. Figure 1 presents the network connection model for wireless medical devices and medical equipment.

Part (A) describes wireless medical devices that combine smart wireless body sensors, small, and limited resources. Sensors are placed inside the body in various parts of the human body to store, process, and monitor the various psychological factors required for a diagnosis. This level also includes on-site medical devices, including radiology equipment, ICU, ventilator, anesthesia, and hemodialysis machines. Moreover, it is connected to the internet to provide the right health treatment. Wireless medical devices share physiological data through an individual digital assistant/smartphone or device programmer.[6]

Part (B) introduces sensor data transmission from mobile devices or medical equipment to a smart local gateway via wired or wireless communication protocols. The geographical distribution of many e-health portals moved to cloud development to perform health-related tasks on the local layer.[7] Each portal acts as a dynamic hotspot between Internet / Local Switch and WBAN as it supports different protocols. It performs complex services, including protocol

[6] Leu, F. −. Y., Ko, C. −. Y., You, I., Choo, K.-K. R., & Ho, C.-L. (2018). *A smartphone-based wearable sensors for monitoring real-time physiological data.* Computers & Electrical Engineering, 65, 376–392. https://doi.org/10.1016/j.compeleceng.2017.06.031

[7] Chen, M., Li, W., Hao, Y., Qian, Y., & Humar, I. (2018). Edge cognitive computing based smart healthcare system. *Future Generation Computer Systems*, *86*, 403–411. https://doi.org/10.1016/j.future.2018.03.054

switching, filtering, data aggregation, and security. Health service providers can access the patient's physical information through the portal.

Part (C) displays applied cloud computing to saving and analyzing relevant data collected in part (A) and processing it in part (B). This level performs data analytics, biomedical and epidemiological research, broadcasting, machine learning, and data warehouse tasks. Finally, it provides a graphical interface for feedback and final visualization. Service providers and caregivers can use this cloud infrastructure to access disease trends, medical history, and epidemics and monitor healthcare remotely

iii. Literature Review

Cybersecurity and privacy risks are the main concerns of security researchers and professionals. The discovery of the Internet of Things has enormous benefits for users; However, some of the challenges appeared with this invention.

Because many devices have a low level of computing capacity, memory, and storage, security risks are increased, limiting the chances of providing security on these devices. Cyberattacks on IoT devices are now rising at an unprecedented rate, according to F-Secure security researchers.[8] There is no real threat from a single infected Internet of Things (IoT) device with malware. However, attackers must infect a group of these devices to bring down the entire system. Botnet attacks are the most common attacks that happen to IoT devices with poor security.[9]

[8] Doffman, Z. (2019, September 14). *Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims*. Forbes. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/?sh=2f0bf3915892

[9] *What is a DDoS Botnet | Common Botnets and Botnet Tools | Imperva*. (2020, September 30). Learning Center. https://www.imperva.com/learn/ddos/botnet-ddos/

Cybercriminals are more advanced in internet technology, and the number of medical devices connecting to the internet is rising exponentially. As a result, cybersecurity threats are a significant concern for device companies. A breach can compromise patient data or software and the performance of life-critical devices like infusion pumps, ventilators, and pacemakers. Nevertheless, the pressure to speed up market entry means cybersecurity testing often happens post-market - or not at all. As regulators recognize the risks of cyber-attacks, cybersecurity is becoming a regulatory imperative for device manufacturers who want to ensure timely clearance.

Usually, low security in IoT medical devices creates risks for both the infrastructure of the hospital operating systems and the healthcare of individuals.

Medical devices give the potential to enhance healthcare and working performance, although they additionally present further safety risks. There are three distinct security challenges:

- No Security: the devices cannot suit a security factor. Consequently, Devices cannot be legitimately observed or constrained by popular IT security products or methods.
- New Connection Protocols: the devices frequently interact across wireless protocols through the range of old system security controls.
- Vulnerable Operating Systems: various of the more complicated machines are dependent on traditional, exposed operating systems, such as old window versions.

Nevertheless, there are no significant security devices that healthcare security teams use to detect attacks like malware.[10]

[10] *Connected Medical Devices (IoMT) The New Target for Cybercrime. (2019, December 17). Retrieved May 20, 2020, from* https://www.armis.com/resources/iot-security-blog/connected-medical-devices-cybercrime/

Healthcare organizations are cybercriminals' new preferred targets. Cybercriminals are hacking hospitals' devices by installing malware on X-Rays, MRIs, and CT scanners. As the medical data has sensitive patients' information, and that is what cybercriminals look after. As a result, the demand for healthcare data in the dark web market is higher than other data. If a connected CT scanner goes down in a ransomware attack ER, doctors immediately lose capabilities that they may need to select a course of treatment for a stroke patient. There are many types of ransomware attacks where cybercriminals have successfully locked down entire hospital networks.[11]

On the other hand, Vectra Networks reported that healthcare is the top-targeted vertical for cybercrime in 2107.[12] Moreover, the HIPAA Journal reported that 2018 was another record year for hackers, with 365 breaches of 500 or more records[13].

Data breaches are more costly for healthcare providers than for any other type of business. The reason for that is due to the severe fines and charges that are mandated by the HIPAA rules. According to "Ponemon," healthcare is a significant valuable business that has the most breach of damages, with an average mitigation loss of $6.45 million in 2018. Healthcare data breaches usually cost 65% more than other industry sector data breaches, Ponemon researchers found.[14] Cyberattacks on IoT devices are now rising at an unprecedented rate, according to F-Secure security researchers.[15]

[11] Ng, A. (2017, May 14). *Worldwide ransomware hack hits hospitals, phone companies*. CNET. https://www.cnet.com/news/england-hospitals-hit-by-ransomware-attack-in-widespread-hack/

[12] *Seals, Tara. "Healthcare the Top-Targeted Vertical for Cybercrime." Infosecurity Magazine, 7 June 2017,* www.infosecurity-magazine.com/news/healthcare-the-toptargeted-vertical. Accessed 19 May 2020.

[13] *HIPAA Journal. "Largest Healthcare Data Breaches of 2018." HIPAA Journal, 27 Dec. 2018,* www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/. Accessed 19 May 2020.

[14] Snell, E. (2019, July 15). *Ponemon Finds 125% Increase in Healthcare Cyber Attacks*. HealthITSecurity. https://healthitsecurity.com/news/ponemon-finds-125-increase-in-healthcare-cyber-attacks

[15] Doffman, Z. (2019, September 14). *Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims*. Forbes. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/?sh=2f0bf3915892

Nowadays, Covid-19 has had a massive impact on healthcare security. Hackers know that the healthcare industry is a mess right now in terms of cybersecurity, and this gives them more of a motivation to create more attacks. Hence, it is an actual attack of opportunity for cybercriminals. Healthcare organizations intensify their focus on strategic planning for a digital future, and they are preparing themselves to pass expected testing, so cybersecurity has been one of those critical components that the healthcare industry is focusing on. Therefore, healthcare provides continue to make cybersecurity a top strategic initiative for the organization.

Securing medical IoT during Covid-19 needs a new view strategy within the organizations. It is critical for validating the actual medical devices on virtual networks.

There are individual medical devices that exist with Windows XP still embedded, which is a significant problem, becoming a huge issue. These medical devices contain many risks associated with it. For example, the pacemaker software, an implantable medical device, has 8,600 security flaws, which indeed put patients' lives at risk.[16]

iv. Challenges And Security In IoT Medical Devices

Understand the medical devices' security challenges. Medical device security differs and has more challenges compared to normal IT security for many causes. However, many medical devices affect a patient's physiology and thus pose a constant risk. Lack of memory, physical length boundaries, processing power, and battery life restrict alternatives for security countermeasures. An additional challenge happens in emergency conditions that are not established in other areas. Medical devices should prevent unauthorized access, but they may

[16] WBB Inc. (2019, September 25). *Flaws in Pacemaker Software Put Patients' Lives at Risk*. https://www.wbbinc.com/flaws-in-pacemaker-software-put-patients-lives-at-risk/

need to allow quick and simple access in an emergency. Another problem is reproduction. Security researchers regularly require access to established devices, and therefore, their ability to analyze attacks and protection is restricted.

Many countermeasures were specified for medical device vulnerabilities, and they can be preventive, corrective, or investigative. Examples consist of audit, notification, relied on outside or inside medical devices, and cryptographic security.

Some of the security challenges are:

a. Hardware Safety And Security Challenges

Hardware safety issues are more common than security concerns; hence the electromagnetic resistance of other devices with their manufacturers is a good example. Nowadays, the Trojans on medical devices appear to be unreliable, but safety measures are necessary to mitigate the risk of attack. After reporting backdoors in military chips, cybercriminals can now damage military devices by taking configuration data out of the device and re-encrypting system software[17]. A method is designed for the automatic embedding of customizable hardware Trojans into arbitrary devices with limited status. Hardware Trojans are challenging to discover and can be developed rapidly, bypassing evolving security

measures.[18]

It should be considered that hardware Trojans can be routes of attack on medical devices as well. It is imperative to ensure that such malware is not placed in the design process. Due to the

[17] Skorobogatov S., Woods C. (2012*) Breakthrough Silicon Scanning Discovers Backdoor in Military Chip. In: Prouff E., Schaumont P. (eds) Cryptographic Hardware and Embedded Systems – CHES 2012. CHES 2012. Lecture Notes in Computer Science, vol 7428. Springer, Berlin, Heidelberg.* https://doi.org/10.1007/978-3-642-33027-8_2

[18] CiteSeerX — *The undetectable and unprovable hardware trojan horse*. (2013). citeseerx.ist.psu.edu. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.387.7849

reliance on computer-aided design tools, it is also imperative to ensure that no Trojans are installed in making these tools. The verification methods used in designing the devices should ensure that the resulting output designs match the input and do not contain additional circuits. Far from using reliable manufacturers at every design stage, ensuring hardware devices are Trojan-free is not practical. Hence, the importance of detection and mitigation capabilities will remain critical. Once malicious devices are detected and their behavior is understood, research on how to mitigate the harmful device's outcome to achieve medical device safety will be a significant concern. Moreover, another hardware security problem is using- radio waves into computers, leading to the possibility of controlling computers remotely and providing malicious programs, even while computers are offline.[19]

The manufacturer is responsible for patching, and they have an unfortunate history of passing those patches in an inappropriate form. Other tools usually use enclosed real-time operating systems (RTOS), such as ThreadX**.** The software update installation must be manually performed when a vulnerability needs correction.

Manufacturers can remotely maintain these devices and provide individuals with the ability to understand their health status through connected apps. For example, now there are brain implants that can be monitored and controlled with a smartphone, and with deep brain stimulation where an electrode is surgically implanted into the brain and connected to a computer, it can provide results that can be read by an external device. Also, children can get faster MRIs through real-time processing into the clouds, and parents can now monitor their child's blood sugar and insulin release on their phones. Medical devices, such as the ones described above, as well as

[19] Sanger, D. E., & Shanker, T. (2014, January 15). *N.S.A. Devises Radio Pathway Into Computers*. The New York Times. https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html

other devices to run operations, are common in healthcare delivery organizations. According to the 2019 Forrester Consulting study, 64% of healthcare delivery organizations estimate that at least half of all devices on their network are unmanaged or IoT devices, including medical devices.[20]

b. Device Software

Medical devices software developers must work on developing and making sure of the integrity and protection of the system. Every protected development and safe update device is required.[21]

- **Safety Development**: Safety is a risky asset. The device is not 100% secure. If the vulnerabilities are unspecified is a responsibility, this is not always an issue. If cybercriminals identify a particular vulnerability, the target network is a comprise threat. The safety of medical software is not practical from developing different forms of software programs. Except for the writing program's fundamental complexity, it takes specific expertise, additional education, and different development skills to create protected programs.[22] Hence, financial and social factors regularly play a position in opposition to superior protection.

In the medical device software program, we should ensure that protection and safety are of the highest precedence, and there is a system described for reporting and fixing vulnerabilities. Medical devices' challenge is that the additional safety code should not interfere with actual time and other resource obstacles, including confined battery strength.

[20] *Palmer |, D. (2018, March 15). IoT security warning: Cyber-attacks on medical devices could put patients at risk. Retrieved May 19, 2020, from* https://www.zdnet.com/article/iot-security-warning-cyber-attacks-on-medical-devices-could-put-patients-at-risk/

[21] *Fu, Kevin & Blum, James. (2013). Controlling for Cybersecurity Risks of Medical Device Software*. *Communications of the ACM*. 56. 35-37. 10.1145/2508701.

[22] *Howard, Michael & Lipner, Steve. (2006). The Security Development Lifecycle*. 10.1007/s11623-010-0021-7.

- **Updating:** While the producers of a device realize its weaknesses, they will cope with the troubles and fix them. The fix ought to then be rolled out to vulnerable systems. The replacement mechanism itself can even be misused to attack. (nevertheless) updates and corrections are much less frequent for clinical gadgets in comparison to computer systems and smartphones.

  Updates should be easy to use for medical devices and take precautions so that malware does not take part in the update procedure itself.
- **Old Software**: Software patches or updates on medical devices are frequently delayed or misplaced altogether. Lacking patches can also be organizational trouble. Delay may also result from the reality that device manufacturers must conform to software program upgrades in addition to any protection installations.[23] The concern with the old software program is that they often comprise recognized security vulnerabilities.

The extended interconnection makes medical devices vulnerable regardless of previous malware[24]. It is crucial for medical devices that the software's manufacturing life cycles of fixed software equivalent to the manufacturing life cycles. Producers should ensure that the software is not applied to medical devices following its expected lifetime.

c. Regulations And Guidance

The FDA's medical devices and software cybersecurity guidance

[23] *Wirth, A. (2011, January 1). Cybercrimes Pose Growing Threat to Medical Devices | Biomedical Instrumentation & Technology | Allen Press. Meridian.Allenpress.Com.* https://meridian.allenpress.com/bit/article/45/1/26/142173/Cybercrimes-Pose-Growing-Threat-to-Medical-Devices

[24] *Fu, Kevin & Blum, James. (2013). Controlling for Cybersecurity Risks of Medical Device Software. Communications of the ACM*. 56. 35-37. 10.1145/2508701.

The Food and Drug Administration has the authority to regulate medical devices in the United States. Regulators have taken notice, none more so than the US Food and Drug Administration (FDA). The FDA has issued several safety communications to overcome the risks of cybersecurity vulnerabilities associated with medical devices. The FDA's advances in cybersecurity and the FDA's commitment to patient safety reduce the risks that cybersecurity vulnerabilities may pose to the devices that patients depend on today for their health and well-being. The FDA worked closely with the Department of Homeland Security and other key stakeholders in public and private sectors to control and respond to medical device cybersecurity issues. As technology evolves and changes, the Food and Drug Administration is adapting and developing methods to keep pace with these challenges, including dealing with a coordinated response to cybersecurity threats.[25]

The manufacturer of the device is responsible for the approved configuration of the device. Device users, such as hospitals and patients, cannot access the device software environment and cannot install additional security measures. Usually, any upgrade or update for added functionality or security measures needs approval from the manufacturer. Consequently, manufacturers usually delay the publication of security-related upgrades.[26]. Manufacturers, importers, and device user facilities are required to report adverse events and device-related issues. The FDA is acting with manufacturers and others to ensure that medical devices'

[25] Center for Devices and Radiological Health. (2020, October 22). *Cybersecurity*. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[26] Wirth, A. (2011, January 1). *Cybercrimes Pose Growing Threat to Medical Devices | Biomedical Instrumentation & Technology | Allen Press*. Meridian.Allenpress.Com. https://meridian.allenpress.com/bit/article/45/1/26/142173/Cybercrimes-Pose-Growing-Threat-to-Medical-Devices

cybersecurity is a patient safety issue. As such, they need to design, deploy, and maintain most cybersecurity and, thus, safety devices possible.[27]

Reviewing Practical control strategies is essential to efficiently collect data on safety and privacy issues in medical devices. Some aspects of regulation and the role of standards have been explained in the FDA medical devices' guidance. We see a demand for action to modify the growing need for software updates for medical devices to re-establish clinical trials after significant modifications. Keep pace with these challenges, including dealing with a coordinated response to cybersecurity threats.[28]

In 2020, the FDA issued safety communications regarding cybersecurity vulnerabilities affecting medical devices to ensure patient safety is continuously at the vanguard of the FDA's efforts. COVID-19 has posed challenges for our community, and the FDA has already learned a lot through response efforts to include issues related to product supply chains, cybersecurity, telemedicine, and the transition to a remote workforce.

Some efforts on the part of the FDA include the efforts regarding program components: The FDA has been one of the primary stakeholders in an ongoing process of exploring the program and supply chain transparency strategies. It is a list or list of program components. The Food and Drug Administration considers these critical program checklists for understanding device cybersecurity risks. The listings will allow the FDA and the manufacturer to respond more quickly to post-market vulnerabilities and allow the FDA to evaluate the devices better before

[27] Center for Devices and Radiological Health. (2020, October 22). *Cybersecurity*. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[28] Center for Devices and Radiological Health. (2020, October 22). *Cybersecurity*. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

being legally marketed. Legacy technology is a complex challenge: Old technology or archaic forms of technology are at the heart of most cybersecurity issues. The issues that created the "old technology problem" were decades in the making. So, the solutions are not simple. The FDA is collaborating with manufacturers, hospitals, and others to discover ways to deal with legacy technology issues in an affordable and informed way.[29]

The organizations are not obligated to comply with FDA cybersecurity guidance to receive FDA approval for their medical device. Guidance documents issued by the Food and Drug Administration are advisory documents and have no force of law. Nevertheless, the directive reveals the Food and Drug Administration's current consideration, and failure to adhere to their recommendations could thwart the clearance of 510 (k). The Food, Drug, and Cosmetic Act, section 510 (k), requires manufacturers to register their new device to notify the FDA of their intention to market a medical device at least 90 days (about 3 months) in advance. 510 (k) is also known as Premarket notification (PMN).[30] Hence, to ensure continuous patient safety, docility[31]

d. Data Integrity

The amalgamation of data from the device into Electronic Medical Records (EMR) systems has seen considerable progress toward ensuring data integrity and individual security. Patient identification is a critical component as information is gathered from several different devices and incorporated into electronic medical records. Moreover, the data source - where the origin of

[29] Center for Devices and Radiological Health. (2020, October 22). *Cybersecurity*. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[30] Center for Devices and Radiological Health. (2018, September 4). 510(k) Clearances. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/device-approvals-denials-and-clearances/510k-clearances

[31]

the data received from external systems needs to be determined - is required to ensure data quality and information reliability. The method of Unique Device Identification (UDI) is a solution for non-implantable medical devices.[32]and other consumable hardware and Software as a Medical Device (SaMD).[33] The transfer of data across countries has a particular interest concerning local regulations and legislation. Incorrect or missing data recorded in clinical information systems and medical records will affect the data's integrity. It is challenging to identify these records, even with the use of electronic medical records.

Data integrity and data security are two terms close together, each presenting an essential role in successfully achieving the other. Data security means protecting the data from unauthorized access or exposure and is crucial to support the data's integrity.

Compromising Data integrity can be in many ways:

- Individual error, Malicious or accidental
- Transit errors, data breaches
- Cyber-attacks, malware, threats
- Hacked devices, such as devices or disk malfunctions
- Physical hacking of hardware[34]

Data breaches are more costly for healthcare providers than for any other type of business. The reason for that is due to the severe fines and charges that are mandated by the HIPAA rules.

[32] *Center for Devices and Radiological Health. (2020, June 30). Unique Device Identification System (UDI System). U.S. Food and Drug Administration.* https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/unique-device-identification-system-udi-system

[33] *Center for Devices and Radiological Health. (2018, December 4). Software as a Medical Device (SaMD). U.S. Food and Drug Administration.* https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd

[34] What is Data Integrity? Definition, Best Practices & More. (2020, September 11). Digital Guardian. https://digitalguardian.com/blog/what-data-integrity-data-protection-101

According to "Ponemon," healthcare is a significant valuable business with the most breach of damages and is estimated to cost the healthcare business $6.2 billion. Healthcare data breaches usually cost 65% more than other industry sector data breaches, Ponemon researchers found[35].

Figure 2 shows that data security plays an essential role in areas usually connected with genuine experience: security, reliability, and IoT systems' elasticity. Failure to perform proper data security rules can have dire outcomes.

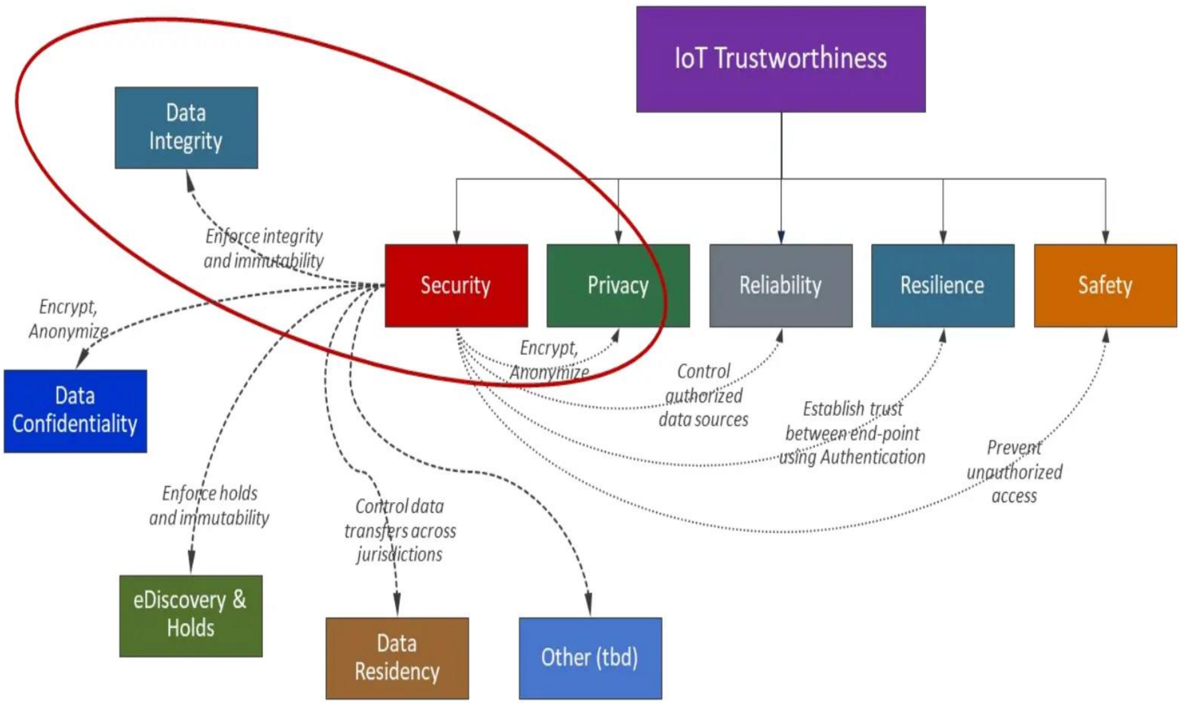

IoT Trustworthiness
Data Integrity
Enforce integrity and immutability
Security
Privacy
Reliability
Resilience
Safety
Encrypt, Anonymize
Data Confidentiality
Encrypt, Anonymize
Control authorized data sources
Establish trust between end-point using Authentication
Prevent unauthorized access
Enforce holds and immutability
Control data transfers across jurisdictions
eDiscovery & Holds
Data Residency
Other (tbd)

Figure 2: The critical role and data protection of IoT data security[36]

[35] Ponemon Institute. (2016, May). *SixthAnnual Benchmark Study on Privacy & Security of Healthcare Data*. https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

[36] Highlighting Data Protection Best Practices for IIoT Systems. (2019, July 25). Digital Guardian. https://digitalguardian.com/blog/highlighting-data-protection-best-practices-iiot-systems

e. Malware

Cybersecurity researchers from the JSOF research lab disclosed a group of 19 vulnerabilities known as Ripple20 developed by Treck Inc. Ripple20 contains 19 vulnerabilities impacting the Treck TCP/IP stack affecting devices in the enterprise, healthcare, energy. Hundreds of millions of connected devices, including IoT medical devices, are affected by Ripple20.[37]

There is no real threat from a single infected Internet of Things (IoT) device with malware. However, attackers must infect a group of these devices to bring down the entire system. Botnet attacks are the most common attacks that happen to IoT devices with poor security.

The botnet attack can also bring down a target after infecting an army of bots with malware and leads them to transfer thousands of requests per second.[38] The Mirai attack in 2016 brought much uproar about IoT security[39]. IoT devices do not have proper security updates like the ones on computers. The IoT devices are very vulnerable to Malware attacks and become infected with zombies that can send vast traffic. According to the Nozomi network, there is an increase in IoT botnets' attacks against the Internet of Things devices this year, 2020. The sharp rise in IoT devices and connections led to an increase in these attacks.[40]

f. Privacy

[37] *Ripple20*. (2020, October 25). JSOF. https://www.jsof-tech.com/ripple20/

[38] *What is a DDoS Botnet | Common Botnets and Botnet Tools | Imperva*. (2020, September 30). Learning Center. https://www.imperva.com/learn/ddos/botnet-ddos/

[39] *Tag: Mirai botnet*. (2018, September 18). Krebsonsecurity. https://krebsonsecurity.com/tag/mirai-botnet/

[40] Team, I. (2019, September 13). *Top 10 Biggest IoT Security Issues*. Intellectsoft Blog. https://www.intellectsoft.net/blog/biggest-iot-security-issues/

When consumers use free Internet services, online service consumers are exposed, analyzed, and become data sources for businesses, thus improving their customer satisfaction. The consumers' data might also be sold to third parties for further analysis, which exposes their privacy. However, it is possible that in the future of the Internet of Things era, companies' policies may lead some consumers to pay to use services to secure their privacy. On the other hand, under restrictions and conditions, others may attempt to hand over data to have free services.

g. Organizational Assessment

Safety in medical devices is most effective when designed in the system from the initial development cycle. Security risk assessment is crucial to developing and maintaining threat models and evaluating device development time risks. A precise plan is needed to provide software updates and patches. Additionally, the Security Response Team must identify, monitor, and lastingly fix security events and vulnerabilities.

For this reason, it is best to motivate user facilities such as healthcare branches and hospitals to report security incidents. Hence, the reports can provide considerable information on the safety issues of medical devices. Moreover, this helps define the safety and threat levels of medical devices with specific business rules and audit guidelines for all relevant stakeholders. Rules-based procedures can then lead to actions needed to respond to IoT medical device security events.

v. Conclusions

Recent technological innovations with the introduction of retinal medical devices have transformed healthcare operations. Therefore, interest in medical retinal device security is proliferating. Over the past few years, many medical devices have been launched on the market. Consequently, the security concerns present in these medical devices have gained researchers' attention from all over the world, and research articles on the vulnerabilities of medical devices and cyberattacks are increasing dramatically.

Cybersecurity must be implemented in the design process, the quality system, and post-market activities of medical device companies to ensure medical device functionality and safety. The use of wireless, networked, and other connected devices exchanging healthcare information increases and will continue with the application of technology to traditional medical devices. From the approach of the PC to the Internet to mobile devices to the cloud to IoT – history is a clear guide. With every technological advance and device, there are new security risks. Those new security risks are real and proliferating.

Today, medical devices are frequently not built with security in mind. Statistics show that hackers are targeting healthcare organizations more than any other industry. As these devices bring more considerable promises in the delivery of healthcare and the well-being of a patient, we must now pay special attention to ensure those devices do not inadvertently harm patient care from ransomware to devise tampering. From a security standpoint, it is the time for healthcare For IoT security specialists, facing these challenges will be extremely tough. Although developing the security of IoT medical devices is significant if the business is ever to develop. To find solutions, they need a more realistic strategy for medical device protection. Their strategy should begin with a continuous basis on complete security in hospitals and clinic systems. organizations to include IoT security as a segment of their complete cybersecurity plan.

This paper studied how IoT medical devices manufacturers are adapting to the need to classify security challenges and their influence on a medical ecosystem's interoperability. Finding a solution for medical IoT device security needs improvement, and experts believe that the vulnerabilities of IoT medical devices are open to attackers.

Reference:

Center for Devices and Radiological Health. (2020, October 22). *Cybersecurity. U.S. Food and Drug Administration*. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

Center for Devices and Radiological Health. (2020, June 30). *Unique Device Identification System (UDI System)*. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/unique-device-identification-system-udi-system

Center for Devices and Radiological Health. (2018, December 4). *Software as a Medical Device (SaMD). U.S. Food and Drug Administration.* https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd
What is Data Integrity? Definition, Best Practices & More. (2020, September 11). Digital Guardian. https://digitalguardian.com/blog/what-data-integrity-data-protection-101

Connected Medical Devices (IoMT) *The New Target for Cybercrime. (2019, December 17). Retrieved May 20, 2020, from https*://www.armis.com/resources/iot-security-blog/connected-medical-devices-cybercrime
Highlighting Data Protection Best Practices for IIoT Systems. (2019, July 25). Digital Guardian. https://digitalguardian.com/blog/highlighting-data-protection-best-practices-iiot-systems

*"*Internet of Things (IoT) Healthcare Market Is Expected to Reach $136.8 Billion by 2021 – *Cole of Duty." Coleofduty, 4 June 2020,* coleofduty.com/news/2020/06/04/internet-of-things-iot-healthcare-market-is-expected-to-reach-136-8-billion-by-2021/. Accessed 17 May 2020.

Islam, S.M. Riazul & Kwak, Daehan & Kabir, Md. Humaun & Hossain, Mahmud & Kwak, Kyung. (2015). *The Internet of Things for Health Care: A Comprehensive Survey*. IEEE Access. 3. 678-708. 10.1109/ACCESS.2015.2437951.

Musonda, Chalwe. (2019). *Security, Privacy and Integrity in Internet Of Things* - A Review.

Ng, A. (2017, May 14). *Worldwide ransomware hack hits hospitals, phone companies.* CNET. https://www.cnet.com/news/england-hospitals-hit-by-ransomware-attack-in-widespread-hack/

Palmer |, D. (2018, March 15). *IoT security warning: Cyber-attacks on medical devices could put patients at risk. Retrieved May 19, 2020, from* https://www.zdnet.com/article/iot-security-warning-cyber-attacks-on-medical-devices-could-put-patients-at-risk/

Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff. 28 Dec. 2016.

"Ripple20 - JSOF." JSOF, 16 June 2020, www.jsof-tech.com/ripple20/. Accessed 30 June 2020.

Seals, Tara. *"Healthcare the Top-Targeted Vertical for Cybercrime." Infosecurity Magazine, 7 June 2017,* www.infosecurity-magazine.com/news/healthcare-the-toptargeted-vertical. Accessed 19 May 2020.

Skierka, I. M. (2018)*. The governance of safety and security risks in connected healthcare. Presented at the Digital Society Institute, ESMT Berlin, Germany.* https://doi.org/10.1049/cp.2018.0002

The Internet of medical things. (2014, June 3). MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2014/internet-medical-things?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq

Turab, N., & Kharma, Q. *(2019). Secure Medical Internet of Things Framework based on Parkerian Hexad Model. International Journal of Advanced Computer Science and Applications*, 54–60. https://doi.org/10.14569/IJACSA.2019.0100608

WBB Inc. (2019, September 25). *Flaws in Pacemaker Software Put Patients' Lives at Risk*. https://www.wbbinc.com/flaws-in-pacemaker-software-put-patients-lives-at-risk/

What is Data Integrity? Definition, Best Practices & More. (2020, September 11). Digital Guardian. https://digitalguardian.com/blog/what-data-integrity-data-protection-101

What Is Network Segmentation? (2020, October 1). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

What is a DDoS Botnet | Common Botnets and Botnet Tools | Imperva. (2020, September 30). Learning Center. https://www.imperva.com/learn/ddos/botnet-ddos/

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review - IEEE Journals &Magazine. Ieeexplore.Ieee.Org. https://ieeexplore.ieee.org/document/8703068/;jsessionid=nyWm-lL8-L_9pBg5yTveyQt__Gu3erYdWvK5Xsg0LaqpPGr-b080!1360512191?arnumber=8703068&casa_token=b4C0LvpQ-8oAAAAA:wXo_979yd5cX1-aO6Q9Aap6WQUDcpWO_PqODsc_CU35Jh9YabL30XZ1S8vJ8wIzPgeTsSfjRGg&tag=1

Zaleski, J. R. (2012). Medical device interoperability and data integration to clinical information systems: medical device data alignment. PubMed. https://pubmed.ncbi.nlm.nih.gov/23039779/