Cyber Security threats and mitigations in the Healthcare Sector with emphasis on Internet of Medical Things.

IE3022-Applied Information Assurance

Cyber Security – Year 3, Semester 1

H.M.T.D.Herath

IT20627928

IT20627928@my.sliit.lk

ABSTRACT

The relevance of information security and privacy in the healthcare industry is rising. Better information security is required as a result of the adoption of digital patient data, greater regulation, provider consolidation, and the growing need for information among patients, providers, and payers.

Organizations like hospitals, clinics, and pharmacies handle a lot of patient health-related data and information. Some of this information may involve sensitive topics, thus it has to be safely kept. Information technology is essential to the industry since it allows for the organized storage of data. Additionally, we need the availability of software that will protect all stored data and restrict who may see it.

Growing medical device connection to computer networks and the convergence of technologies have made vulnerable hardware and software applications more susceptible to mishaps. It is now well recognized that patient data must be protected against cyberattack. However, healthcare organizations, regulators, and makers of medical devices are all worried about the possible influence on clinical treatment and patient safety. It is also possible for control of a medical device to be compromised.

This essay examines the cybersecurity issues that the healthcare industry is now dealing with as a result of recent regulatory changes, hyper connectivity, and technological convergence. It highlights the problems and conflicts that arise between safety and security as well as possible solutions.

INDEX TERMS

EPHI:Electronic protected health information , HIT: Health information technology , HIPPA:Health insurance portability and accountability act , HHS:Health and human services , EHR:Electronic health records , IOT:The internet of things , PHI: Personal health information , IT: Information technology , OCR:Optical character recognition , CMS:Centers for Medicare and medical services.

I. INTRODUCTION

Wirelessly enabled healthcare networks are anticipated to provide real-time monitoring, emergency care, early diagnosis, and the treatment of chronic illnesses.

The storage of medical data, the creation of health records, and the provision of on-demand services to authorized stakeholders all depend on medical servers, databases, and cloud-enabled services.

Additionally, it provides a wide range of medical applications, including monitoring of chronic diseases, rehabilitation, fitness programs, wearable monitoring devices, and geriatric care.

Therefore, many medical gadgets, sensing devices, diagnostic and imaging devices may be seen as smart devices or objects that form a crucial component of the IOT in healthcare.

The overall goal of I0T-based healthcare services is to save costs, improve patient care, and improve user experience.

II. Research statement / Objectives

Almost every department in a hospital manages personally identifiable information (PII) and protected health information (PHI) in one or more health information systems. Electronic health records (EHR), e-Prescribing software, remote patient monitoring, laboratory information systems, and so forth are used by all healthcare professionals, including doctors, physician assistants, nurses, pharmacists, technicians, dietitians, and physical therapists.

The billing office also uses medical billing software to access insurance and financial data, and the scheduling and administration departments use scheduling software to access clinical information. In contrast to most other organizations (academic institutions, enterprises, etc.), where PII is often restricted within a small number of departments where cybersecurity measures may be consolidated, practically every department in a hospital handles PII in some capacity. By safeguarding devices, electronic systems, networks, and data against assaults, cybersecurity solutions seek to safeguard PII and PHI.

In this paper we review about the all of the above things and cyber security challenges to the healthcare sector and their mitigations to protect healthcare industry from that threats.

III. Review of the literature

What is a medical device?

Any device intended by the manufacturer to be used, either alone or in combination, for a medical purpose qualifies as a medical device. This includes instruments, apparatuses, implements, machines, appliances, implants, reagents for in vitro use, software, materials, and other similar or related items.

Medical equipment have seen significant technical advancements throughout time.

Before	Now
Devices are connected to patient physically.	Devices are connected wirelessly to patients and other devices.
Data obtained from devices are stored on local paper or locally.	Data obtained from devices are stored in the cloud.
Devices are physical products.	Devices include software and even databases of health information.
Care is hand-administered at a health care location.	Care is available to patients in the palm of their hand through apps.
Physical access is needed to view health data.	Health data can be accessed anywhere on earth.

How IOT is beneficial for Healthcare

There has been a drastic growth in the variety of medical equipment, which are often coupled with smart devices like mobile phones, tablets, and wearable technology that also run medical apps and software. Today's houses already include these gadgets.[4]

The advantages of using I0T enabled technology in the healthcare industry are briefly shown in the below section.

1. Constant real-time reporting and monitoring

Real-time monitoring of medical data during a medical emergency helps prevent fatalities from conditions including heart failure, stroke, diabetes, asthma attacks, etc. Utilizing a mobile data connection, various instruments and sensors attached to the human body gather and transmit health information [12]. Your doctor, your insurance company, a collaborating healthcare institution, or an outside party may have access to this acquired data. It may also be kept in the cloud or on distant servers and shared with an authorized party. Additionally, it enables users to view the acquired data from any place, at any time, and via any device.

2. Examining the data

There is less need to keep raw data since I0T networked devices can gather, analyze, and publish the data in real time. It is challenging to store and handle the enormous quantity of real-time data that a device captures and sends in a short period of time if cloud access is not accessible.[8] Additionally, gathering data from several devices or sources and manually analyzing it is a laborious undertaking for healthcare professionals.

3. Monitoring and alerting

Medical I0T devices collect vital information in life-threatening circumstances and transmit it to physicians and hospitals for real-time monitoring while also sending notifications to the people concerned.

4. Emergency assistance on the go

The medical professionals will examine patients right away and identify problems that occur while they are on the road using the most up-to-date mobility gear. Patients may communicate with the medical professionals who are many kilometers away in an emergency using a smart mobile device.

5. Accessibility and low cost

With the use of cutting-edge healthcare facilities, healthcare automation systems, and other cutting-edge technology, I0T will automate patient care processes. Interoperability, machine-to-machine connection, knowledge exchange, and data migration are made easier by healthcare I0T, which improves the efficiency of healthcare service delivery.

6. A lower price

IOT enables real-time patient monitoring, significantly lowering the need for unneeded doctor visits, hospital stays, and readmissions, as well as their associated costs.

7. Better treatment for patients

On the basis of the gathered data, clinicians may use IOT-powered devices and technology to make informed, evidence-based judgments.

8. More rapid diagnosis

Real-time data collection and ongoing patient monitoring make it possible to identify symptoms even before they appear.

9. Taking care of supplies and medications

The purchase of drugs and medical supplies is a serious issue for the healthcare industry.

These are properly managed and optimized by linked devices and sensors, resulting in a decrease in wasteful expenses and man hours.

How Healthcare Can Adapt to Cyber Threats

As the healthcare advances in technology, cybersecurity threats rise.

Medical devices have an inherent security risk since they may be able to reveal both data and device control.

This creates a conflict between safety and security that has to be resolved by more stakeholder participation, especially in design and regulatory methods.

Regulators, device manufacturers, healthcare providers, IT vendors, and patients themselves are increasingly included in this group of stakeholders.

The methods used by cybercriminals to assault the healthcare sector have become pretty sophisticated.

Hackers prefer to steal medical records that include personal data like credit card numbers, financial information, and banking information.[15]

Stolen medical records are more valuable on the black market and have a longer shelf life.

Hospitals and doctor's offices may have data breaches, but insurance firms experience them more often.

They may either use the credit card and social security data for their own gain or sell them on the black market.

The value of selling this information online rises as there are more opportunities to profit from the stolen healthcare data, including names, Medicaid, and tax numbers.

According to KPMG's 2015 cybersecurity study, barely half of healthcare businesses felt properly prepared, and 81% of them had experienced attacks in the previous two years. The main driving force was the black market value of patient health information.

Hospitals in several nations, including the US, UK, and Australia, have been impacted by the recent sharp rise in "crypto ransomware," in which thieves use malware to encrypt information before demanding payment in digital currency to decrypt it (including patient data) and resume operations.

Unfortunately, improper cybersecurity implementation might potentially compromise patient privacy and endanger their health. The risk has been increased by technology convergence, embedded computing, mobile computing, and the wide range of stakeholders.

Healthcare institutions and corporations that manufacture medical devices must contend with a variety of cyber threats, including targeted and increasingly sophisticated untargeted assaults.

Threats consist of,

- Termination of care or services (including potential for patient deaths)
- Using counterfeit emails and bogus websites to trick employees into giving up their login information or installing malware
- Insider threats, whether unintentional or deliberate, may constitute a serious risk because of the position of trust they have inside an organization.
- The theft of patient data, particularly electronically secured health information (ePHl)
- Asset loss, exfiltration of information, and data breaches
- The use of sensitive material that has been exfiltrated for blackmail, extortion, and pressure.
- Theft of intellectual property (IP)

According to research, the safety of patient health data is still the main emphasis of healthcare cybersecurity, which ignores or inadequately protects patients' health from more serious threats.

The UK National Data Guardian has conducted a study and issued suggestions for new information security policies and standards. Patient safety and medical equipment were not included in the evaluation.[13]

In untargeted assaults, staff members may unintentionally install malware on poorly secured systems. In particular, when they may run out-of-date software, be unpatched, be unable to run anti-malware products in line with manufacturer recommendations, or both However, although some opponents may want to damage patient health data, others may accidentally have an influence on it.

Threats to the healthcare industry as a whole and particular risks to medical devices

Cyber threats are dangers that stem from both technology and the internet. Threats relating to technology are present in networks and computer systems. These dangers might seriously harm the network and computer system, as well as compromise patient and hospital information privacy.

Collecting information or employing technologies to ‘sniff' out' or intercept network data, including passwords Active threats occur in a variety of shapes and sizes.

- Hack Threat

The prospect of a hack, whether it comes from hospitals or the outside, puts the health IT at risk. The hacker is the only one with the capacity to infiltrate the system undetected. The system is hacked with the intention of stealing data, spamming other computers, and performing a denial of service (DOS) assault on the target computer. The prospect of hacking is exceedingly hazardous since it may lead to the theft of vital medical data, particularly information linked to individual patients.

- The Fraud

The act of fraud is to deceive someone or an organization by doing something heinous and making a false claim. If a person has the user name and password for a computer or application at a hospital, health IT fraud may result. The owner of the ID and password would be held responsible if the individual gained entry to the hospital and did dishonorable actions.[17] The reputation of the hospitals may also be harmed since fraudsters may exploit the applications of the hospitals to solicit donations from other organizations or engage in dishonorable behavior against the hospitals.

- Malicious Code

Malicious code may pose a hazard to the health IT. A program known as malicious code is designed to damage, steal data, use system resources, and provide unauthorized access to a computer. Some examples of harmful code include Trojan horses, worms, malware, and viruses. Email, infected floppy disks, instant chats, file-sharing services, and pop-up advertisements are just a few of the ways that harmful software may propagate.

- Denial-of-service attack

An further technology-related danger to health IT is a denial of service attack. A denial of service assault, often known as a DOS, aims to break down one or more computers. Typically, a DOS assault involves several computers and is conducted simultaneously. This is because DOS operates by simultaneously delivering a stream of requests to a single server. Incoming requests will be queued if the server cannot handle the volume of simultaneous requests, which will result in a sluggish response or no answer at all. This threat may be quite troublesome, particularly if it renders a huge website offline during the peak period of traffic.[2]

- Harassment

One of the technology-related threats to the health IT is computing harassment. When someone engages in vulgar, unpleasant, and profane behavior online or via a computer network, or when they make suggestions about unlawful or immoral behavior, it is harassment.

- Data Breaches

A hazard that constantly exists in organizations and businesses is a data breach. This danger indicates that private and protected information belonging to a certain organization might be taken and seen by someone who is not allowed to do so. In hospitals, data breaches often occur because thieves are trying to take intellectual property, trade secrets, or personally identifiable information (PHI)[9]. The disclosure of classified information to an unauthorized person by an authorized person is also considered a data breach, even if it did not happen in secret.

According to the Internet Threats Report from 2012, the healthcare sector has the highest percentage of reported data breaches across all businesses (36%). This analysis leads to the conclusion that the largest hazard to the health sector is a data breach. The health website ranked tenth with 1.7% in the same research on website exploitation. The findings of this study highlighted the fact that hackers often target health IT security in their attempts to compromise computer systems and networks.

Medical system cybersecurity priorities vary and are related to deployment Hospital IT systems prioritize maintaining patient privacy to avoid data leaks or ransomware attacks (which can also impact availability of systems if made unusable by encryption). When patients are exposed to medical devices as part of their treatment, including implanted devices, patient protection is a top responsibility. Accessibility of such devices is a goal. Confidentiality is also a concern for "non-medical" or wellness gadgets, such fitness trackers, but with far less effect.

There are very serious potential issues if a medical device is hacked.

- Potential damage to patients.
- Patients may pass away.
- Protected health information may disappear.
- Decreased faith in linked gadgets.

Managing Cyber Risks in the Healthcare industry.

Electronic Health Records (EHRs) may now be separated from desktop computers thanks to mobile devices including laptops, handhelds, cellphones, and portable storage devices.

However, these possibilities also pose risks to the security and privacy of personal information.

1. Protect mobile devices.

• Due to their mobility, these gadgets are susceptible to theft and are simple to misplace.

• Mobile devices are more susceptible to electromagnetic interference than fixed ones, particularly from other medical equipment. The data kept on a mobile device may get tainted due to this influence.

• The user must exercise particular caution to avoid unauthorized access of the electronic health information displayed on a laptop or portable device as mobile devices may be used in locations where they may be viewed by others.

• Not all mobile devices come with reliable access restrictions and authentication. To protect mobile devices from unlawful usage, further measures can be required. Password security is necessary for laptops.

• Wireless data transmission and reception are often done using laptop computers and portable devices. These wireless communications need to be secured from listening in and intercepting.

Not transferring unencrypted electronic health data via public networks.

Mobile device data transport is inherently dangerous. This approach must have an overwhelming rationale that goes beyond simple convenience.

The U.S. Department of Health and Human Services (HHS) has created guidelines on the dangers of remote access to and use of electronic health records as well as potential mitigating techniques [3].

2. Soft wares and operating system maintenance.

Remove any software (such as games, instant messaging applications, and photo-sharing facilities) that is not necessary for operating the practice.

If the software is essential to the operation of the EHR, inquire further with the creator of the EHR.

• When installing software, avoid accepting default settings or "normal" setups.

Go over each decision in detail, comprehend your options, and, if needed, seek technical support.

• Determine whether the EHR provider maintains a direct line of communication with the installed software (a "back door") in order to provide updates and support. If so, make sure the firewall has a secure connection and ask to have this access turned off when not in use.

Disable remote printing and file sharing in the operating system settings. If they are permitted, files can unintentionally be shared or printed to places where unauthorized people might view them.

3. Use a firewall

A small practice should have a firewall to guard against intrusions and threats from outside sources, unless it employs an EHR system that is completely unconnected from the Internet.

4. Install and maintain anti-virus software.

It's critical to maintain anti-virus software updated after EHR adoption. To safeguard against the most recent malware and computer infections, antivirus software needs frequent updates from the manufacturer.[4]

5. Creating a backup.

Making a backup is commonplace.

Where backups are seldom taken into account until after a crash, when it is already too late.

A new EHR must be frequently and consistently backed up from the first day it is operational in a practice.[11]

In order to have a solid backup that you can rely on in an emergency, it's crucial that all the data be completely preserved and that it can be swiftly and accurately restored. The capacity of backup media to perform a successful restoration must be routinely evaluated.

6. Control access to protected health information.

Configure your EHR implementation to limit access to electronic health information to those who have a "need to know" in order to reduce the risk to this data while setting up EHR systems.

Setting file access rights manually using an access control list is often possible in small firms. Only someone with appropriate access permissions to the system is capable of doing this.

It is crucial to decide which files should be accessible to which staff members before establishing these rights.

Additional access restrictions that may be set up include role-based access control, which bases a staff member's access rights on their position within the practice (e.g., doctor, nurse, billing specialist).

7. Use secure passwords and update them often.

8. Limit network access.

Instant messaging and peer-to-peer file sharing are two popular and frequently utilized technologies.

A house or workplace may quickly and easily set up internet capabilities via wireless routing.

Tools that could enable outsiders to access a health care practice's network must be utilized with great caution due to the sensitivity of health care information and the fact that it is protected by law.

9. Manage the data on personal phones & tablets.

10. Don’t let insecure devices on your corporate network.

11. Deploy SSO with badge readers simple & quicker for clinical users.

12. Strong HW, SW, medical device asset.

13. System scanning & patching.

14. Event monitoring & incident response.

15. Data loss prevention.

16. Restrictions on removable media.

IV. Future research

The literature on cyber risk in the healthcare industry is reviewed in-depth in this article. It is an overview of the most important cyber-risk studies. It illustrates the lack of enthusiasm for the topic among scientists. The amount of research on healthcare facilities is inadequate to fulfill demand. There aren't many studies that deal with the problem of cyber risk management in the healthcare industry in the literature. This issue has to be researched throughout the fields of social science, mathematics, business, management, and healthcare.

Manufacturers of healthcare products have been compelled to embrace digitalization at a quick rate due to the need to scale up production and delivery of products to hospitals and clinics as well as the requirement to generate innovative and cutting-edge healthcare gadgets.[15]

To fulfill demand and provide goods as soon as possible, it's likely that organizations have neglected cybersecurity in favor of adopting new technology or working practices. Cybercrime in the healthcare industry not only results in financial losses but also puts patient safety in danger. This is because hackers routinely target medical equipment that may connect to the internet, revealing private patient data online.

V. CONCLUSION

The use of HIT security in healthcare and hospitals may benefit these organizations in a number of ways. Data and information sharing between the two healthcare institutions is now much simpler and more suitable than before. However, integrating IT into healthcare and hospitals may also result in security problems, such as viruses and attacks that might interfere with system operations. The occurrence of any potential risks will be caused by the weaknesses that often happened inside the security mechanism when sharing the material with other study fields. Furthermore, healthcare physical security systems must strike a balance between service and quality, regulatory compliance and safety. In order for the healthcare security system to continue operating securely and effectively, it is crucial to maintain excellent physical security.

The majority of the medical device guidelines is new and under development. There is convergence among healthcare stakeholders and an awareness that cybersecurity is a collaborative effort, not only from a technological standpoint. A number of strategies are now actively addressing the lifecycle risks and possible damage from cybersecurity events, while functional safety and safety-related risk (to the exclusion of cybersecurity or data protection) have historically been the emphasis of medical device risk management. It is advised that medical device makers do a cybersecurity maturity assessment to identify and prioritize areas for improvement. This should take into account product lifecycle security, which is specified in developing assessment methods and expressed in healthcare procurement. All healthcare organizations must have established incident response strategies and procedures in place in order to prepare for the eventual cybersecurity occurrence.

VI. Acknowledgement

Cyberattacks may happen at any endpoint and at any network link. A digitalized health system must have interoperability across software, operating systems, medical device interfaces, and information exchange networks. This is critical for cybersecurity risk management. Attack surfaces and vectors have multiplied due to the growth of medical cyber physical streams, wireless connection, and the introduction of medical applications in healthcare. It is now difficult to protect each point of access to the health system.

VII. References

1. https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7

Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks

2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8059789/

Health Care Cybersecurity Challenges and Solutions

3. https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector

Cyber Attacks: In the Healthcare Sector

4. https://www.aha.org/system/files/2017-12/ahaprimer-cyberandhosp.pdf

Cybersecurity and Hospitals

5. https://www.phe.gov/Preparedness/planning/405d/Documents/resources-templates-508.pdf

Health Industry Cybersecurity Practices - ASPR

6. https://asprtracie.hhs.gov/technical-resources/86/cybersecurity/0

Health Industry Cybersecurity Practices: Managing *Threats* and protecting ... makers and *healthcare* organizations to *mitigate* these *threats*.

7. https://www.ehidc.org/sites/default/files/resources/files/transfoming%20healthcare%20cybersecurity%20from%20ractive%20to%20proactive.pdf

The problem of *cybersecurity* goes beyond patients' priva- cy and the financial burden on the *industry*; it also poses a *threat* to patient safety

8. https://www.changehealthcare.com/insights/enhancing-healthcare-it-cybersecurity

How to Improve Healthcare IT Cybersecurity

9. https://www.infosecurity-magazine.com/blogs/healthcare-cybersecurity-threats/

Healthcare Cybersecurity: Threats and Mitigation

10.

https://www.himss.org/resources/cybersecurity-healthcare?utm_campaign=general&utm_source=google&utm_medium=cpc&utm_term=_&adgroupid=134509372449&gclid=Cj0KCQjw1bqZBhDXARIsANTjCPL4xTLOvBp3qQEjHqkiOG4SGErlGTubeaRvMi7yJ4mtJEQfnXr_sQwaAgusEALw_wcB

Cyber security in healthcare

11. https://cloud.google.com/blog/products/identity-security/how-healthcare-can-strengthen-its-own-cybersecurity-resilience

How healthcare can strengthen its own cybersecurity resilience

12. https://www.difenda.com/blog/three-things-healthcare-organizations-need-to-do-to-prevent-the-next-cyberattack/

Top 3 tips for cybersecurity in healthcare

13. https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise

Healthcare breaches on the rise in 2022

14. https://www.criticalinsight.com/cybersecurity/cybersecurity-for-healthcare

Cyber security for healthcare

15. https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise

Healthcare breaches on the rise in 2022

16. https://www.criticalinsight.com/cybersecurity/cybersecurity-for-healthcare

Cybersecurity for Healthcare

17. https://www.pondurance.com/healthcare-resource-page/

Healthcare pondurance provide a suite of cyber security services to enable healthcare organizations with tools to reduce risk, mature their security posture & maximize their investments.

VIII. Author profile

Hearth H.M.T.D

BSc (Hons) in Information Technology -Specialization in Cyber Security