Review Paper on Critical Infrastructure Security in the Healthcare Sector

Sri Lanka Institute of Information Technology (SLIIT) | IE3022-Applied Information Assurance | Assignment 01

17th of May 2021

Jayasundara H. M. D. E. K. | IT 19081762

Email: it19081762@my.sliit.lk

1. ABSTRACT

Healthcare organizations are an easy target for cybercriminals because of their essential and fragile facilities. With the rise of digitization, several security issues have arisen, and it is worthwhile to consider these critical issues not only from a specific point of view but also from a legal and managerial point of view. It is also important to identify potential. It is important to understand the ways in which attackers can damage and destabilize the health care system, as well as the ways in which attackers use them to achieve their goals. For that reason, it is also important to recognize the potential dangers of combating cybercrime. It is not just a physical and cyber threats; it has become a mixture of both. This review magazine provides an overview of the major issues facing the health sector as well as a list of recent safety events.

Index terms: *Healthcare and Public Health (HPH), Artificial Intelligence (AL), Cybercrimes and Cyber Security, Internet of Things (IoT)*

2. INTRODUCTION

Critical infrastructure (CI) is a core component of the traditional operations of human society that can be defined as having significant impact on important social functions, such as health, safety, security, the economy or the social well-being of people, and the failure to care for those functions Possible disruption or destruction. Logically, it is considered the economic "central nervous system" of a nation. Without a properly functioning, or truly vulnerable CII, nations will find it difficult to achieve and maintain national goals of social and economic progress and development. In samples of CI; Special attention is paid to the protection of health and public health systems. With a greater focus on enhanced efficiency, functionality and productivity, this information and technology, and thus the Internet, has teamed up to create this multifunction.

The Healthcare and Public Health (HPH) Division manufactures and distributes essential products and services to ensure local and global health well-being and maintains key areas before or after health effects. The services provided by the HPH Division to protect the world's population are excellent. Appropriate collaborators are needed to optimize the stability and durability of the essential infrastructure and a strategy is needed to coordinate them. Also, health care and public health appear to be partners in achieving this goal. In any emergency, it is very important that the quality of health care systems remain high, and that an emergency management situation can contribute to national security.

Threats to resources have grown in the modern world. The Health Care and Public Health (HPH) Division-Specific Plan was developed to improve the stability and durability of essential infrastructure in industries that are vulnerable to all hazards. It is intended to be customized to be specific to market competitors among Sector-Specific Plan (SSP). The National Infrastructure Protection Plan has played a major role in achieving all these goals. This article outlines the critical infrastructure safety and security team action procedures and future technologies in the healthcare sector.

3. RESEARCH STATEMENT/ OBJECTIVES

The main concept of this research is to gather more than 15 sources and conduct an extensive study of them, providing a comprehensive analysis of the critical areas of the world's healthcare infrastructure, such as artificial intelligence and cyber security. The focus is on the Health and Public Health Specific Plan (SSP), which aims to improve the safety and resilience of critical infrastructure in all hazardous industries. Of particular note is the inability of the healthcare system to provide reliable and secure treatment without digital access. If the health care system is unsafe, it could jeopardize the safety of patients and expose them to unwanted accidents.

All healthcare providers have a great responsibility to protect patient data and medical equipment primarily. With regard to corporate initiatives that enhance the cyber security of healthcare organizations, healthcare organizations have widely stated the importance of cyber risk assessment. This article will give you an idea of what health care is all about. Artificial intelligence now occupies a leading position in the field of health. Artificial intelligence enables healthcare professionals to better understand the day-to-day patterns and needs of their patients. This shows how the advancement of technology can be applied to infrastructure. The final section covers future research and new discoveries in this regard.

4. REVIEW OF THE LITERATURE

A cyber threats on a healthcare sector that disturbs its ability to oversee patients can be destroying to a neighborhood local area's capacity to deal with the standard consideration of its populace. quiet flood during disastrous occasions. The effect of cyber threats on health care sector can be coordinated into three categories:

Losses of secrecy: The openness of individual information and data can trigger gradually expanding influences for casualties of digital wrongdoing, including burglary or loss of patient data. Another thought is the association between persistent information and individual clinical gadgets. Those gadgets convey security and protection hazards as they become progressively arranged and remote.

Losses of Integrity: Patients and experts may lose trust in a medical services supplier's capacity to keep up persistent protection, because of view of lacking security.

Losses of Availability: Cyber threats to information and activities frameworks can take an office disconnected, prompting interruption of care because of programming blackouts. Moreover, the deficiency of admittance to wellbeing records may restrict the supplier's capacity to give proper consideration, safe house, and medication in the midst of hardship. In conclusion, harm to framework. like protection and installment or utility frameworks. Keep individuals from getting to essential healthcare consideration.

Medical services foundation is now defenseless, as our medical care conveyance framework regularly works at or close to 100% of limit on a day-by-day basis. Compounding the weight on the framework is the increment in the maturing U.S. populace and ascend in clinic affirmations because of the effects of clinic terminations, the utilization of crisis offices as an essential mark of care for the uninsured, and expanded length of stay because of increasing ongoing ailment rates as of late. Likewise, close joint effort among public, private, and non-legislative partners to guarantee safe medical services framework is a test.

Private and non-benefit medical services conveyance frameworks don't worry about the concern of basic foundation security alone. The general wellbeing area state and nearby wellbeing offices are pioneers inside the medical services area to get ready for,

react to, and recuperate from man-made and catastrophic events. For neighborhood general wellbeing, medical care is an equivalent accomplice in keeping the country's wellbeing administrations secure for all networks. Public trust relies on the supportability and strength of our public medical services and general wellbeing basic infrastructure.

Current arrangement misses the mark regarding shielding the wellbeing area from digital dangers. To cultivate the enhancements of the medical services conveyance framework, Federal precept, like the National Health Security Strategy (NHSS), the Center for Disease Control and Prevention's Public Health Preparedness Capabilities: National Standards for State and Local Planning (PHEP), and U.S. Division of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response's Healthcare Capabilities: National Guidance for Healthcare System Preparedness (HPP) has advanced the appropriation of innovation in medical care offices. Be that as it may, as medical services suppliers use e-Health, data innovation, and other electronic devices with lacking security frameworks or requirement, the area opens itself to openness to digital dangers. As indicated by the Third Annual Benchmark Study on Patient Privacy and Data Security (2012), 94 percent of medical care associations have had in any event one information penetrate in the previous two years. 45% report that they have had more than five incidents.

From the leader level, President Obama gave Presidential Policy Directive (PPD)– 21 and Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, accentuating the requirement for all encompassing contemplating basic framework security and hazard the board. Those orders and chief orders will drive activity towards basic framework frameworks including medical care to improve their organization security. Furthermore, those approaches will help advance and boost the selection of network protection rehearses, increment digital danger data sharing, assess, and develop public-private organizations, and comprehend the falling results of foundation disappointments. With the arrival of PPD-21 and EO 13636 and the resulting operationalization of these approaches, Federal organizations liable for NHSS, PHEP, and HPP ought to focus on improving security of medical services data frameworks, fortifying of public-private associations fundamental to medical care network protection and flexibility, and receiving principles and systems for data sharing and security inside the corrections of direction regulation.

Pushing ahead, general wellbeing and medical care accomplices need not hang tight for amendments of government regulation or full execution of PPD-21 and EO 13636 to start improving the security of medical services offices. Networks can improve digital protection by opening a discourse with the key nearby open private partners to improve associations and data sharing. Medical care offices can arrange across areas to connect with innovation specialists to additionally improve framework security and guarantee the insurance of their information and frameworks. In conclusion, the medical

services area can raise representative consciousness of digital danger by carrying out computerized cleanliness preparing – intended to make a typical comprehension of how to protect PC frameworks. By making those first contemplations to improve wellbeing data sharing and digital protection, medical care area administrators can start to decrease the danger and openness that accompanies the reception of new innovations to improve their administration conveyance, patient consideration and flexibility of their networks.

5. FUTURE RESEARCH

Innovations through future technologies are rapidly being incorporated into healthcare systems as well. Technological advances from anesthetics and antibiotics to radiation therapy and magnetic resonance imaging scanners have also made a huge difference to health care. But due to technological innovations, human factors will continue to be one of the permanent limitations of using new drugs and therapeutic methods, the introduction of new devices, the availability of new social media support for health services, and so on.

5.1 DEEPER AI INFUSION

Artificial Intelligence (AL) has been a part of the healthcare sector. AI has the potential to reduce the complexity of the healthcare data is analyzed. A survey of 200 healthcare professionals released by Intel Corporation in July 2018 revealed that 37% of respondents use AI technology in a limited way, and 54% of professionals believe that in the next five or 10 years That AI technology will have to be widely used.

ROBOT HEALTH WORKERS and BLEEDING ROBOTS are among the technologies that may be at the forefront of future AI technology.

5.1.1 BLEEDING ROBOTS

Pediatric HAL is a medical robot that has the ability to mimic bleeding, urination, limb movements and other human behaviors. Medical students use these HAL robots to identify real-life patients' conditions and to better diagnose and treat them before working with them. Children's HAL is part of a robot company called Gomard, which will rapidly spread among medical students around the world in the future.

5.1.2 ROBOT HEALTHCARE WORKERS

Attitudes towards robots are determined by how they are framed when used. Replacing health care staff has become a bigger problem because there are not enough people in the essential places for care. As a result, technology has emerged as a tool that helps people do their jobs. Undoubtedly, this technology will grow further in the future. Health literacy officers trained to work with UNDP robots in Rwanda must develop computer literacy programming and software development skills. Countries around the

world can cope with this digital revolution and bring about such technological advances that will make the healthcare sector more advanced and efficient in the future.

5.2 BETTER CLOUD INTEGRATION WITH EXISTING TECHNOLOGIES

According to the 2017 Healthcare Information and Management Systems Association (HIMSS) Cloud Usage Survey, more than 90% of healthcare companies use cloud applications. Although healthcare organizations have a high level of cloud usage, they often use the cloud only for separate purposes, such as clinical applications, data hosting, and backup, and do not make perfect use of it. That is, activity is still limited. Digitizes electronic data or X-ray data and modifies data in a variety of ways. The use of cloud integration allows data to be exchanged in various healthcare silos, and the use of clouds by healthcare organizations as the number one translator in the future to bring the cloud transformations and that data together.

5.3 SMARTER HEALTHCARE SYSTEMS

Smart healthcare services comprise of various members, like specialists and patients, clinics, and examination organizations. It is a natural entire that includes various measurements, including sickness avoidance and observing, analysis and therapy, emergency clinic the board, wellbeing dynamic, and clinical examination, IoT, cloud computing, large information, 5G, big data, and mobile Internet, along with present day biotechnology establish the foundation of shrewd medical care. These technologies are widely used in every aspect of smart healthcare. Equipment may be used in the future to monitor patients' health, access medical assistance through virtual assistants, and operate remote services. Also, physicians can use a variety of intelligent clinical decision support systems to assist and improve diagnostics.

Specialists can oversee clinical data through a coordinated data stage that incorporates Laboratory Information Management System, Picture Archiving and Communication Systems (PACS), Electronic Medical Record, etc. More exact a medical procedure can be accomplished through careful robots and blended reality innovation. From the viewpoint of medical clinics, radio-recurrence distinguishing proof (RFID) innovation can be utilized to oversee faculty materials and the store network, utilizing incorporated administration stages to gather data and help dynamic. The utilization of portable clinical stages can upgrade patients' encounters, From the viewpoint of logical examination foundations, it is feasible to utilize strategies, for example, AI rather than manual medication screening and to discover reasonable subjects utilizing big data. Through the utilization of these advancements, smart health care can adequately lessen the expense and hazard of operations, improve the usage productivity of medical assets, advance trades, and participation in various locales, push the advancement of telemedicine and self-administration clinical consideration, and at last make customized health benefits. The application of smart healthcare can be divided as follows:

a. Assisting diagnosis and treatment
b. Disease prevention and risk monitoring
c. Virtual assistants
d. Smart health care centers
e. Assisting drug research

5.4 INFRASTRUCTURE UPGRADES THAT MAKE HEALTHCARE MORE ACCESSIBLE

The ability of physicians to diagnose and prescribe medication through web and mobile portals is essential for the management of chronic care. As tele-health proliferation continues to grow, patients and physicians have not yet fully grasped its potential and uses. The lack of full-fledged Wi-Fi and stable cellular service in many health care facilities is still a barrier to integrating telehealth and other mobile healthcare services. And for some as a baby gets older, he or she will outgrow this. But in the future this telehealth concept will come to the fore.

6. CONCLUSION

As the population grows and the demand for new services increases, so does the need for critical infrastructure.

Artificial intelligence will inevitably be useful in advancing the healthcare industry, and AI technology will certainly be of great help in the future for everything from predictive medical care and more accurate diagnoses to motivating patients to care about their health. It will also enhance a patient's experience of the disease and the specialization of health care.

Smart Healthcare was introduced because the system helps to monitor a patient's heart rate, body temperature and humidity in health centers, such as gases such as oxygen and carbon dioxide, and a patient's vital important conductors. Although the advanced health care system allows patients to perform out-of-hospital examinations, the medical staff is able to view and monitor their data in a timely manner, minimizing the risk of death by referring the patient to prompt treatment. Also, medical data can be analyzed through this system in a short period of time so that the healthcare staff can be treated quickly in the event of an epidemic or crisis. This system is very useful for infectious diseases such as the new coronavirus (COVID-19) treatment. The developed system will definitely improve the current health care system.

As a result, an overall increase in cyber security research has been identified and large gaps and opportunities in future healthcare can be identified.

7. ACKNOWLEDGEMENT

First of all, I would like to pay tribute to Mr. Kanishka Yapa, Lecturer in Applied Information Certification (AIA) at the Institute of Information Technology, Sri Lanka, for his efforts to expand our knowledge through the focus of study on a new topic. We consider it a great privilege to be able to enhance our knowledge through a wide range of valuable information in new dimensions while reviewing the critical infrastructure of health care and its safety. I would also like to express my appreciation to all my colleagues who have contributed to my research. I was able to do this research better and look at the research in new dimensions. I will never forget the support of my family members and I would like to express my gratitude for that. Also, I would like to thank my university for improving my education. I would like to pay my respects for leading the way to conquer the world by producing thousands like me. I look forward to doing this with my 100% commitment and full effort for any assignment given. Finally, the research leading to the results presented in this article was found in the Analytical Lens for Internet of Things (ALIoTT) project and similar projects under the Petros Cyber Security at the Internet of Things Research Hub. I would like to express my appreciation for all the projects and

research that have helped make this project a success.

References

[1] I. P. V. M. I. G. P. E. B. E. K. a. N. L. Eva Maia, "Security Challenges for the Critical Infrastructures of the Healthcare Sector," now the , 2020. [Online]. Available: https://www.safecare-project.eu/wp-content/uploads/2020/09/8.-Security-Challenges-for-the-Critical-Infrastructures-of-the-Healthcare-Sector.pdf.

[2] A. R. &. M. R. I. Md. Milon Islam, "Development of Smart Healthcare Monitoring System in IoT Environment," Springer link, 26 May 2020. [Online]. Available: https://link.springer.com/article/10.1007/s42979-020-00195-y#:~:text=Full%20size%20image-,Conclusion,CO%20and%20CO2%20gases..

[3] P. Y. Wang, "Artificial intelligence in healthcare: past, present and future," BMJ Journals, 2017. [Online]. Available: https://svn.bmj.com/content/2/4/230.

[4] "Health Care Industry Cybersecurity Task Force," Public Health Emergency, [Online]. Available: https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx. [Accessed 27 November 2018].

[5] D. G. Jawdekar-Abraham, "The Internet of Things-Missing Link to Smart Healthcare," Science Innovation Union , 31 March 2019. [Online]. Available: http://science-union.org/articlelist/2019/2/25/the-internet-of-things-missing-link-to-smart-healthcare.

[6] W. H. H. M. M. F. Fergus, "A Survey of Critical Infrastructure Security," March 2014. [Online]. Available: https://www.researchgate.net/publication/267391571_A_Survey_of_Critical_Infrastructure_Security.

[7] B. Marr, "How Is AI Used In Healthcare - 5 Powerful Real-World Examples That Show The Latest Advances," Forbes, 27 July 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/07/27/how-is-ai-used-in-healthcare-5-powerful-real-world-examples-that-show-the-latest-advances/?sh=7af0297c5dfb.

[8] "HEALTHCARE AND PUBLIC HEALTH SECTOR," Cyber security and infarstuture security agency, [Online]. Available: https://www.cisa.gov/healthcare-and-public-health-sector.

[9] u. Snair, "Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable," 2013, 24 October. [Online]. Available: https://www.naccho.org/blog/articles/risks-of-cyber-attacks-on-the-healthcare-sector-leave-public-health-of-communities-vulnerable.

[10] "Critical Infrastructure Protection for the Healthcare and Public Health Sectors," Public Health Emergency, [Online]. Available: https://www.phe.gov/Preparedness/planning/cip/Pages/default.aspx. [Accessed 24 March 2021].

[11] M. Bamiah, S. Brohi, S. Chuprat and J.-l. A. Manan, "IEEE Xplore," 28 March 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6488073.

[12] M. Athinaiou, "Cyber security risk management for health-based critical

[12] infrastructures," 28 March 2013. [Online]. Available: https://ieeexplore.ieee.org/document/7956566/authors#authors.

[13] "Changing Healthcare Institutions with Large Information Technology Projects," [Online]. Available: http://what-when-how.com/medical-informatics/changing-healthcare-institutions-with-large-information-technology-projects/.

[14] P. Sieńko, "Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies in leading," December 2015. [Online]. Available: https://www.researchgate.net/publication/307708049_Methods_of_securing_and_controlling_critical_infrastructure_assets_allocated_in_information_and_communications_technology_sector_companies_in_leading.

[15] J. P. P. A VasquezMónica HuertaMónica HuertaRoger ClotetRoger Clotet, "Intelligent System for Identification of patients in Healthcare," June 2015. [Online]. Available: https://www.researchgate.net/publication/280445426_Intelligent_System_for_Identification_of_patients_in_Healthcare.

[16] "Advantages & Disadvantages Of Electronic Health Record," E-SPIN Group of Companies, 2005 -2021. [Online]. Available: https://www.e-spincorp.com/advantages-disadvantages-of-electronic-health-record/.

[17] "10 Ways Technology Is Changing Healthcare," The Medical Futurist, 3 March 2020. [Online]. Available: https://medicalfuturist.com/ten-ways-technology-changing-healthcare/.

[18] H. Thimbleby, "Technology and the Future of Healthcare," 10.4081/jphr.2013.e28, 1 December 2013. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4147743/.

[19] C. Young, "10 Technologies that Will Drive the Future of Healthcare," Interesting Engineering, Inc. , 24 February 2020. [Online]. Available: https://interestingengineering.com/10-technologies-that-will-drive-the-future-of-healthcare.

[20] D. Marbury, "Six Healthcare Technologies Coming in the Next 10 Years," vol. 29, no. 2, 2 February 2019.

AUTHOR PROFILE

Jayasundara H. M. D. E. K.

Born in Negombo, Sri Lanka on 05th of October 1999. Studying at University of Sri Lanka Institute of Information Technology, Malabe, Sri Lanka. Received the certificate in INTRODUCTION TO CYBERSECURITY COURSE at Cisco Networking Academy, Sri Lanka, in 2020, INTRODUCTION TO IOT COURSE at Cisco Networking Academy in 2020 and NDG LINUX UNHATCHED COURSE at Cisco Networking Academy in year 2020. Following BSc (Hons) in Information Technology Specializing in Cyber Security degree, Sri Lanka Institute of Information Technology (SLIIT) University, Malabe, Sri Lanka, From February 2019 to February 2023. Mr. Jayasundara currently work as COMPUTER OPERATOR at R & R Foreign Employment Agency, Negombo. His primary research interests include Critical

infrastructure security in healthcare sector, security vulnerabilities, and Cyber Crimes, Artificial intelligence, Internet of Things (IOT), and so on. He is a member of IEEE community at SLIIT, a Member of ISACA community in SLIIT and a member of Cyber Security Community in SLIIT. And he is currently studying in 3rd year 1st semester in his university life.