ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

CYBER SMART: PROTECT THE PATIENT; PROTECT THE DATA ON ELECTRONIC MEDICAL RECORD

Shreya Thakral, Arti Vaish

E-Mail Id: shreyathakral1998@gmail.com, artivaish@sushantuniversity.edu.in

Sushant university, Gurugram, Haryana, India

Abstract- Cyber security is the practice of defending the computers, servers, electronic devices and data stored in online cloud from mislenious attacks. It is divided in some part like network security and computer security. Network security is to make the network from the attackers from hacking.

In a health care organization where nowadays all work done by using electronic medical record and storing the information in online cloud, there is the higher risk of getting affected by the unwanted attackers and get the information from third party sources. Electronic medical records are at higher risk of getting affected by different method like pissing method or also can be effected by the malware and ransom ware that can be more dangerous to the system.

To make the proper safety, data encryption is very useful where the thirdparty source cannot access the information and the information gets limited the sender and the receiver. And also there is different ways to give the safeguard the patient information in hospital RMR is browsing the internet by using VPN, and not to open any suspicious site.

Keywords: Cyber security, Electronic Medical records, Cyber smart, Malware, Ransom ware, Cyberattack, Cyber threats.

1. INTRODUCTION

"Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks" [1]. It is an interchangeable term from of the information security. It also lead to a breach in the confidentiality, integrity or availability of information [2]. Cyber security is not only a threat to a single person; it can impact the whole organization and also the governing body.

Cyber security can be divided into few common terms first is Network security which means to secure computer networks, second is Application security which indicates to have secured computer applications which helps to provide access to the data as its designed to protect. Another one is Information security which is to maintain the integrity and privacy of the data to be protected in both storage as well as in transit, Last is the Operational security, it includes that how to handle and how to protect the data for example to access the secured data or providing permission to use the data. Some other cyber security methods are disaster recovery when the data get exposed after that how to manage it and recover it and the again protect it another is the End user education as it depends upon the individual like how they are protecting their data or their awareness for examples not to access unknown links, attachments etc, not plug in unknown USB or pen drives etc [3]

The scale of cyber threats globally indicates that it is raising breaches each and every year. According to the report by Risk based security data 79 billion records have been exposed in the year 2019.

Mostly medical sectors experienced the most breaches of cyber threats because they collect financial and medical data and hence experienced the cyber customer's attacks [4]

As the health sector is continuing to give the best possible way to treat the patient in life-critical situations by using the newer technologies like e-medical treatment or medical treatment, etc. Cyber threat hackers try to look into that important patient information. The healthcare industry is more exposed to many cyber attacks nowadays. This issue ranges from malware that can act as a threat to the information of the patient. The healthcare industry also faces many challenges in the form of cyber attacks. The cyber attack done in health care is beyond financial loss

but also the loss of the patient valuable information that can risk the life of the patient. The use of cyber security is basically to protect the patient's data from cybercrime.

2. CYBER RISK

Cyber risk is the risk of damage to an organization through its information system. Many organization and health institutions now a day's moving to use of online storage so it give the hackers chance to get the loopholes of the system to make some changes. Vulnerabilities and weakness, flaws and errors can be exploited by the attackers through internet.

Depending on the attack, the direct and indirect consequences may impact any organization or a system's finances and operation.

By using the electronic medical record system where it becomes easy to record the patient history and also the vision status along with the glasses prescription.

And all this information are now a day's getting saved in electronic medical record so there is a need to give the information a safeguard to the patient ocular status information, so that we can secure from cyber attack. [1]

3. ELECTRONIC MEDICAL RECORD SYSTEM

Electronic Medical record is a collection of medical information of a person stored in the computers such as patient's demographic data, relevant patient's history, examinations, diagnostics tests, possible treatments and referrals.

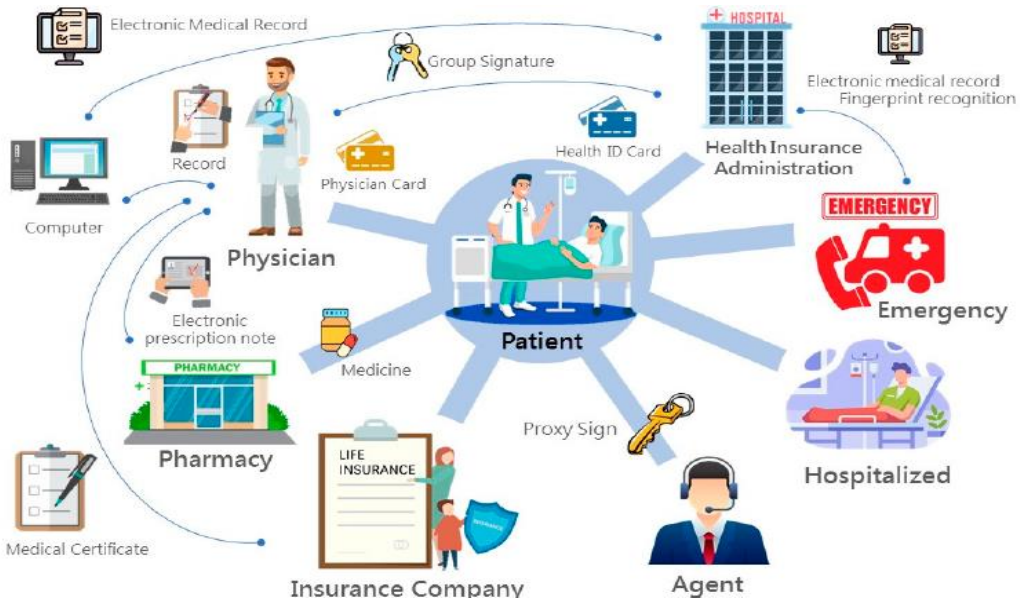

Fig. 3.1 Integrated medical Information system

4. EMR IS AT RISK OF CYBER THREAT

4.1 Phishing Attack

It often come through email in an attempt to lure the user to click the link and after that some viruses get installed to that device that can make certain changes to the device, they also can steal the information of the device along with the IP address.

To avoid these things the physicians should closely examine any file sharing request before sending it to anywhere and also need to make sure that the file is sent to an trusted and authorized address

4.2 Malware and Ransom ware

Malware can enter to the hospital EMR system in a variety of ways - via download, phishing attack and software vulnerabilities through the encrypted traffic sources and they can be used to steal the data of the hospital record and also giving long term herm to the hospital computers.

Table-4.1 The ten Largest HPAA Data Breaches reported to HHS Database as of February 2020

Organization	Type of breach	Date	Number of records	Location of breached information	Nature of lost data
Anthem Inc.	Hacking/IT incident	13 February 2015	78 800 000	Network server	Name, birthday, medical identification, social security number, address, email, and employment information
Premera Blue Cross	Hacking/IT incident	17 March 2015	11 000 000	Network server	Name, birthday, medical identification, social security number, address, email, and employment information
Excellus Health Plan, Inc.	Hacking/IT incident	9 September 2015	10 000 000	Network server	Name, birthday, medical identification, social security number, address, email, and employment information
Science Applications International Corporation	Loss	4 November 2011	4 900 000	Other	Name, birthday, medical identification, social security number, address, email, and employment information
Community Health Systems Professional Services Corporation	Theft	20 August 2014	4 500 000	Network server	Patient name, birthday, social security number, telephone number, and name(s) of employers or guarantors
Community Health Systems Professional Services Corporations	Hacking/IT incident	21 August 2014	4 500 000	Network server	Patient name, birthday, social security number, telephone number, and name(s) of employers or guarantors
University of California, Los Angeles Health	Hacking/IT incident	17 July 2015	4 500 000	Network server	Patient name, birthday, social security number, Medicaid or health plan identification numbers, and medical data
Advocate Health and Hospitals Corporation (Advocate Medical Group)	Theft	23 August 2013	4 029 530	Desktop computer	Name, birthday, address, credit card number, expiration date, demographic and clinical information, and health insurance information
Medical Informatics Engineering	Hacking/IT incident	23 July 2015	3 900 000	Electronic medical record, network server	Name, address, username, password, and health information
Banner Health	Hacking/IT incident	3 August 2016	3 620 000	Network server, other	Name, credit card number, card expiration date, and verification code

Adopted from HHS- office for Civil rights, Breaches portal

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=365037181A402E68E1611931BC7B016, Updated 21 February 2020

On the other hand ransom ware work in a different way, it when steel the patient data or the system information it seek some money to giving back the data to the actual user and the hospital cannot use the EMR until the required payment is not done. This is actually more dangerous to the hospital because using EMR need to be more up to date to the recent advancement to the technique and if it get corrupted then getting it back is very difficult.

Threat from cloud storage: As many of the hospital store the patient data and all the information at cloud to improve the patient care and this can accessible to specific network and other network can’s access it.

But if there is any suspicious person also using cloud storage then they can allow the unnecessary sites to access the cloud storage and get the information from outside that can be a potential risk of having the cloud storage.

5. EMERGING THE NEW CYBER THREATS IN THE HEALTH CARE SYSTEM

Ransom ware, for example, is a particularly dangerous form of malware for hospitals, as the loss of patient data can put lives at risk. It is a type of malware that actually targets the system and files and also the system becomes inaccessible until the required money was given to the party responsible for the cyberattack.

So the ransom ware attack in the following way:

- By pushing emails
- By clicking a suspicious link
- By viewing an advertisement containing the malware in it

Table-5.1 Emerging technologies for cyber security

Technology	Description	Application	Examples	Sources
AI	Utilization of complex algorithms and software to simulate human cognition and decision-making	Learning (acquisition of information and rules), reasoning (using rules to reach conclusions), and self-correction	IBM QRadar applies AI to help security analysts investigate and predict cyber treats	www.ibm.com/security/artificial-intelligence www.cybersecurity-insiders.com/ibm-watson-supercomputer-to-be-used-for-cyber-security/
ML	Application of algorithms and statistical models to perform specific tasks without requiring explicit instructions or supervision	Detect threats, including organization profiling and infrastructure vulnerabilities, based on data (server logs, transactions, real time communication)	Amazon ML surveys Amazon Web Services (AWS) data streams to monitor and detect malicious activities or unauthorized behavior	https://aws.amazon.com/machine-learning/ https://builtin.com/artificial-intelligence/machine-learning-cybersecurity
BC	Decentralized database that keeps digital record of transactions accessible to authorized users	Smart contracts connect nodes to connected parties. Blockchain ledgers provide audit trail to ensure transparency	Estonia utilizes BC to capture and record health records for all 1.3 million residents	https://e-estonia.com/tag/blockchain/ www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf
QC	New generation of computers that use quantum mechanics to analyze, solve, and process complex data quickly and efficiently	Cryptography, high-throughput *in silico* trials, and drug discovery	Google's Bristlecone, a 72-qubit QC processor that solves practical and theoretical applications in encryption, optimization, and ML	https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

6. DEFERENCE AGAINST CYBERATTACK

Data encryption help to protect data as if there is encryption has done then the data is transferred to the target user directly and there is no rule for the outsiders for entry and peep about the information for the purpose to steel in any case.

But now a days the hackers are also getting more smarter and they are using blind spots in encryption where they can hide without being notice and avoid detection and then effect the target to attack to get the information of that organization.

7. WAYS TO SAFEGUARD THE PATIENT DATA

To give safeguard to the sensitive information of the patients there are some steps that can be taken

- By using VPN to mask the identity of the user and also the IP aadess. With a VPN, you can certainly avoid all such tracking. It is because the VPN encrypts all the data generated from the device.
- using anti-malware applications because if any how it get entered in the device or the system then it can give damage to the device malware replicates quickly whilst damaging the data files and spread over the entire system or the network
- Don't click at the emails or messages came from un-trusted sites, there is a cyber attack type called fishing technique where the un-trusted sources operators give the attractive mails or messages and when the used clicked the email then there is automatic download of the files that can actually control the entire device of that authority [6] .

8. OPTOMETRY AND CYBER SECURITY

Nowadays many eye care hospitals are also moving themselves to the developed way to record the patient information by using the electronic medical record system where it becomes easy to record the patient history and also the vision status along with the glasses prescription.

8.1 Recommended Approach to Cyber Security in Health Care

As discussed above there are lots of cyber threats ways to be done with the patients data uploaded in the EMR so it is very important to aware and educate the medical professionals to learn the cyber security ways to protect the data from the leaking and misuse of it [5] .

- Quality IT at the foundation- For protecting the data it is important to have proper IT department in the hospitals not only human resources but the IT infrastructure also to safe the patients data
- Preventive and proactive stance- For the preventive aspects the data should be under the surveillance and protection by the certain networks and applications in the hospitals.
- Training and Approach- It is important to safe the data that each and every person should know the basic idea about the protection of the patient's data. Only limited and trust worthy persons are allowed to access the Electronic medical records. [5] .

CONCLUSION

Based on the synthesis and literature selected, it is found that using of the advance technology in the medical field is very appreciable but along with the use of cyber security we can safe guard the patients demographic as well as medical data for safety storage as well as for maintain patient's privacy. We can enhance the advancement of the data protection by the IT professionals and its infrastructure and hence we can provide safe and secured medical service to the society.

REFERENCES

[1] FDA Fact Sheet: THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY Dispelling Myths and Understanding Download the Fact Sheet (/media/123052/download.

[2] Rossouw von Solms, Johan van Niekerk, "From information security to cyber security", sciverse science direct, computers and security, South Africa, 2013

[3] To know about Cyber security https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security.

[4] Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F, "The Importance of Cybersecurity Education in School", International Journal of Information and Education Technology, Vol. 10, No. 5, May 2020.

[5] Frank Luh, and Yun Yen, "Cybersecurity in Science and Medicine: Threats and Challenges", Tends in biotechnology science and societ, 2020.

[6] Salem T. Argaw, Juan R. Troncoso-Pastoriza, Darren Lacey, "Cyber security of Hospitals: discussing the Challenges and working towards mitigating the risks", BMC,medical informative and design making, 2020.

[7] Salem T. Argaw1, Juan R. Troncoso-Pastoriza2, "Cybersecurity in Science and Medicine: Threats and Challenges", trends in biochemistry, science and society, 2020.

[8] Hsuan-Yu Chen 1, Zhen-Yu Wu 2, Tzer-Long Chen, "Security Privacy and Policy for Cryptographic Based Electronic Medical Information System", MPDI, swizerland, 2021.

[9] Anthony Vipin Das, Priyanka Kammari, Ranganath Vadapalli, Sayan Bas, "Big data and the eye Smart electronic medical record system, An 8year experience from a three-tier eye care network in India", Department of eye Smart EMR and Eye, L.V. Prasad Eye Institute, Hyderabad, Telangana, India, 2020.

[10] School of Nursing, "Cybersmart: Protect the Patient, Protect the Data", Journal of nursing and radiology, Hammond, Louisiana, Elsevier Southeastern Louisiana University, Hammond, Louisiana, 2019.