iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** III **Month of publication:** March 2021

DOI: https://doi.org/10.22214/ijraset.2021.33159

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue III Mar 2021- Available at www.ijraset.com

Cyber Security in Healthcare

Shweta Vivekananda Kondewar
Computer Science Department, Pune University, 205 A Navi Peth Solapur, India

Abstract: ***India is a popular destination for medical tourists, given the relatively low costs & high quality of it's private hospitals. Emerging technologies & advanced devices creates huge potential to improve healthcare system. Despite this, there are some loopholes in healthcare system. Increased connectivity to existing computer network has exposed healthcare data to new cybersecurity threats. Cybersecurity breaches include stealing health information/records & ransomware attacks on health organizations. Covid-19 shows the deficiencies of management & security in the healthcare system. To make the healthcare system. More efficient we need to take actions. Government should implement rules & regulations that will help to protect the healthcare system from cyberattacks.***

Keywords: Cybersecurity, Healthcare

I. INTRODUCTION

Covid-19 showed the different era to the world. Health organizations, doctors & patients gave their best to save people's lives where, emerging technologies gave chance to communicate people from home. IT-sector & many organizations adopted work-from-home culture. In Pandemic technology helped in every aspect. Healthcare systems are saviours for people in pandemic. India is a favourite destination for medical tourists because of low costs & high quality of it's private hospitals. New technologies & advanced devices give immunity to the healthcare system in India. The culture of the healthcare system is rapidly changing. Health organizations shifting their focus towards advanced medical devices & emerging technologies. Every system has its own advantages & disadvantages. No doubt, due to technology patient's get rid of diseases easily & efficiently but is patient's data really safe?

Cyberattacks on hospitals or health organizations for ransomware is an increasing concern for health organizations. The lack of attention by health organizations is a major reason for cyberattacks. Health organizations are not aware of cyber attacks & their regulatory laws. To make the healthcare system more efficient we need to create awareness among health organizations for cyberattacks & its compliance in India.

II. MODERN TECHNOLOGIES IN HEALTHCARE

As technology is rapidly changing, healthcare is the most beneficial of them. Due to modern technologies & advanced devices patients can get rid of disease easily & efficiently. Digital technology could help transform unsustainable health care systems into sustainable one, equalize the relationship between medical professionals & patients, provide cheaper, faster & more effective solutions for disease. Computer exposed Networks allows hospitals to record every single detail of each & every patient. Many modern technologies such as Artificial intelligence, Augmented reality, Virtual reality, Nanotechnology have the potential to redesign the healthcare system completely. As the future of medicine & healthcare is closely connected to the empowerment of patients as well as individuals taking care of their own health through technologies.

A. What is Data in Healthcare?

Data collection in healthcare allows health systems to create holistic views of patients, personalize treatments, advance treatment methods, improve communication between doctors & patients, & enhance health outcomes. Patient's records & past history of patients helps medical professionals to treat patients effectively & efficiently. According to the patient record appropriate treatment is given to the patient. A Personal electronic health Record (EHR) is a system that collects information about the patient's health from a number of sources. An EHR includes test results, clinical observation, diagnoses, current health problems, medications taken by the patient, the procedures he/she underwent etc. It also includes data of health insurance & bank details of Patients

B. Cybersecurity in Healthcare

Gone forever are the days when a patient was treated by a single physician. Today, a team of physicians & specialized medical technicians rely on complex medical equipment to diagnose & treat patients. This collaboration is made possible because electronic medical records (EMR) securely store large amounts of medical & clinical information, which is exchanged electronically among healthcare entities by an industry specific medical grade network. This medical information is susceptible to being stolen or held for ransom & malicious hackers can even take direct control of connected active & passive medical devices over the internet & injure patients.

C. What is Ransomware?

Ransomware is a type of criminal malware that restricts access to the infected computer system in some way, & demands that the hospital pay a ransom to the malware operators to remove the restriction. The computer can be a server holding patient files or a computer that is built into an active medical device. Health organizations can not treat a single patient until the ransomware is paid.[2]

Figure 1 – Ransomware Attack

D. Cyberattack on Presbyterian Medical Centre

In 2016, the computer systems of Hollywood Presbyterian Medical Centre were held hostage by hackers. Staff at the 434bed hospital were unable to access the patient's records, & they had to resort to paper records. The hospital administration was under a ransomware attack, hackers were also asking for bitcoins, a hard-to-trace electronic currency favored by cyber criminals. The administrators paid $17,000 in bitcoins as a ransomware to access electronic health records of patients.[1]

E. What is Social Engineering?

Social Engineering is another common way for cybercriminals. Hackers target health organizations that publicly display their employee's contact information. Hackers send individuals an email containing links or attachments. When individuals click an attachment or link it will immediately infect the user's computers & begin to spread throughout the rest of the health system.

F. Cyberattack on University of Washington Medicine

In 2013, A hospital employee was sent an email that includes a link. The link was accessed in so as to look at an attachment. When the attachment was opened the hacker accessed the employee's computer containing files needed for billing of nearly 90,000 patients at University of Washington Medicine. It also contained the personal information of patients. University of Washington Medicine paid $7,50,000 to hackers. In order to avoid these kinds of cyberattacks health organizations should educate users on how to manage communication in a secure manner. The staff & administration should be trained.

G. HIPAA (Health Insurance Portability &Accountability Act)

Health Insurance Portability & Accountability Act, a federal law is designed to improve portability & continuity of health insurance coverage in group & individuals markets. HIPAA was developed with 2 goals of making healthcare delivery more efficient & with increasing the number of health insurance coverage also with 3 main provisions.

1) The portability provisions.
2) The tax provisions.
3) The administrative simplification provisions.

The act also includes standardization of data interchange security & confidentiality of healthcare related data. HIPAA rule helps to protect the patient information in order to protect the patient privacy, security & confidentiality of patient information.[5]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue III Mar 2021- Available at www.ijraset.com

III. NEED FOR HEALTHCARE COMPLIANCE IN INDIA:

HIPAA was fully implemented in the year 2003 in USA with privacy & security rule obligations. No similar act in India as HIPAA is available & some provision is available in IT act. In the year 2007, handful of companies in India started requiting professional services for HIPAA training & investing in HIPAA preparation which accelerated in 2008 & more companies of midsize become " HIPAA Compliant ".

In a survey, 50 selected laboratories in India, 14(28%) of the laboratories were aware of HIPAA & 36(72%) of the laboratories were not aware of HIPAA. In India HIPAA is not popular & recognized & hence the laboratory is not aware with the HIPAA. 86% of the laboratories believe that HIPAA will be effective & will regularize the health insurance coverage in India. 14& of the laboratories believe that HIPAA will not be effective in regulating the health insurance.[5]

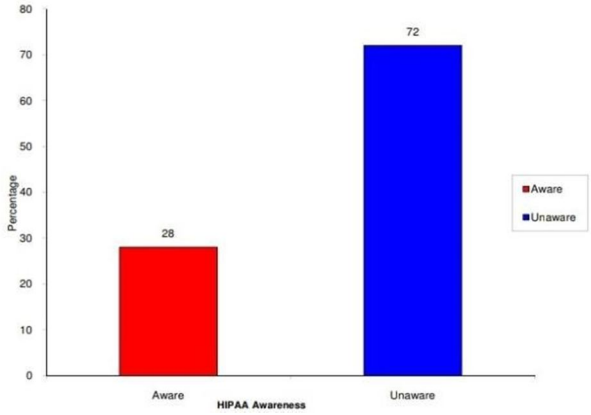


Figure 2 – Statistics for HIPAA Awareness in India

In my opinion, India as an emerging country, first choice of medical tourist due to low cost & high quality of it's private hospitals it is necessary to compulsory laws like HIPAA to boost the healthcare system in India. Act like HIPAA will help us to protect patient's data.

A. Who Should be Compliant?

Health organizations such as small clinics, private hospitals & pathology laboratories are the sources for collection of patient's healthcare data.

B. Privacy & Security Guidelines

1) *The Security Rule:* Security Rule focuses on securing the creation, use, receipt & maintenance of electronic personal health information by health organizations. The security rule sets rules & regulations regarding physical & technical handling of personal health information. It is more focused on the technical aspects of protecting personal health information.
2) *The Privacy Rule:* Privacy Rule sets safeguards to protect the privacy of personal health information of patients such as post medical reports, details etc. The privacy rule limits what information may be used (and in what manner) & disclosed to third parties without prior patient authorization.

C. Roadmap To Healthcare Compliance In India

1) *Educate Healthcare Staff:* In India many people are unaware about cyber attacks. Simple human error or negligence may end in disastrous & expensive consequences for healthcare organizations. Security awareness training equips healthcare employees with the requisite knowledge necessary for creating smart decisions & using appropriate caution while handling patient data.
2) *Restrict Access to Data & Application:* Access restrictions require user authentication, ensuring that only authorized users have access to protected data. We can restrict the access by applying the user's biometric (eye scanning, fingerprints or facial recognition).
3) *Backup Data to a Secure, Offsite Location:* Even a natural disaster impacting a healthcare organizations data center can have disastrous consequences if data is not properly backed up. Therefore frequent offsite data backups are recommended with strict controls for data encryption, access & other best practices to ensure that data backups are secured. Offsite data backups help us from disaster recovery.
4) *Implement Data usage Controls:* Healthcare organizations can use data controls to block specific actions involving sensitive data, such as unauthorized email etc. Data usage control helps us to block unwanted activities in real time.

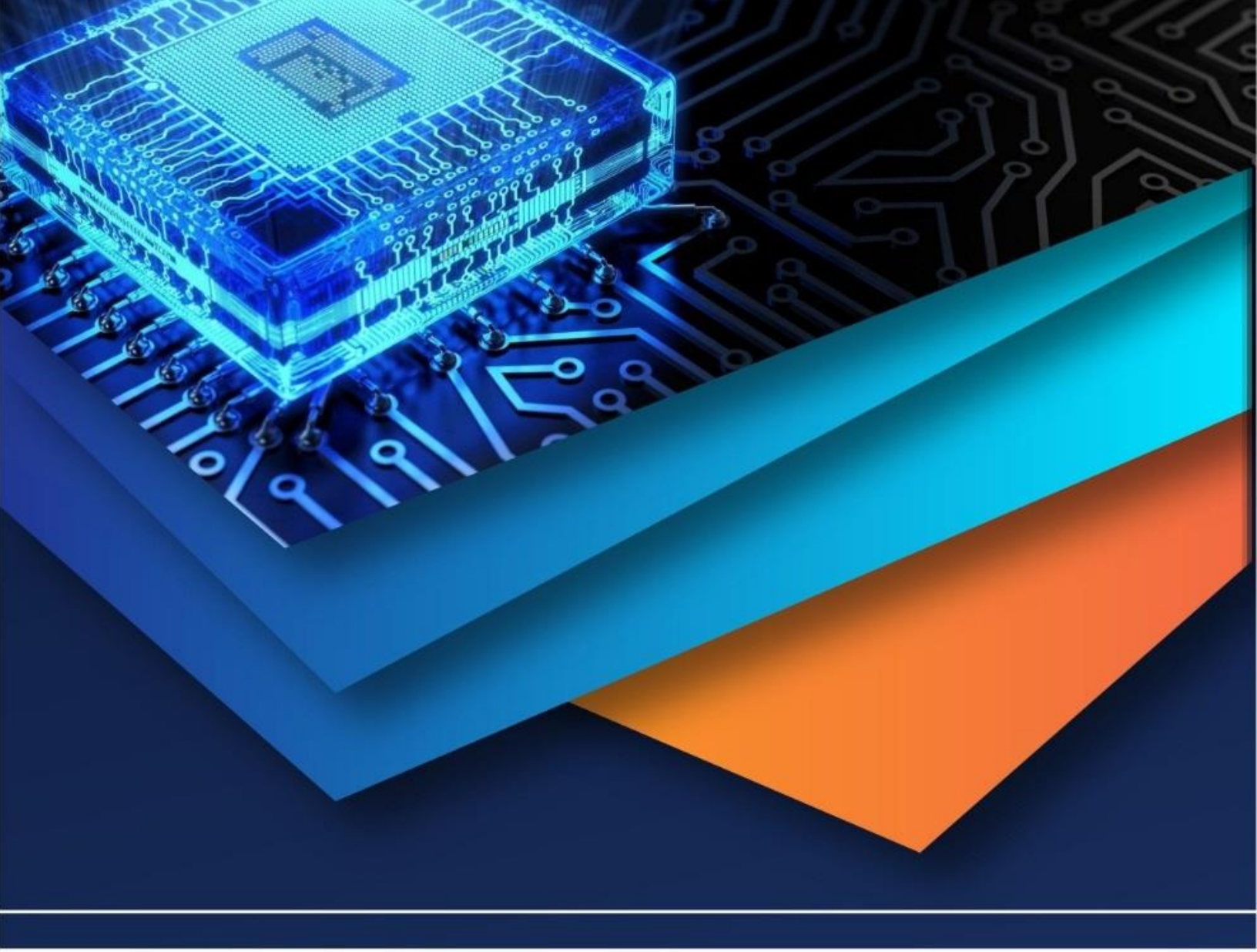
5) *Encrypt Data at Rest & in Transit:* Encryption is one of the most useful data protection methods for healthcare organizations. By encrypting data in transit & at rest, healthcare organizations make it impossible for hackers to decipher patient's data if they gain access to the data.

IV. CONCLUSION

Healthcare systems play a vital role in developing countries. While healthcare technologies play a key role in our population's health they are vulnerable to security threats due to interconnected, easily accessible access points, outdated systems & a lack of emphasis upon cybersecurity. Healthcare is an attractive target for cybercrime for 2 fundamental reasons: It is a rich source of valuable data & it's defence are weak. Most of the attacks are for financial gain. Other attacks may be motivated by political gain.
Every problem has a solution. In cyberattack rules like HIPAA will help us to protect health organizations from cybercrime. It is necessary to take strict actions against cyberattacks, to protect health organizations.

REFERENCE

[1] Cybersecurity : A Real Threat to Patient Safety https://www.jopan.org/article/S1089-9472(17)30143-0/ fulltext.
[2] Cybersecurity for Hospitals and Healthcare Facilitieshttps://link.springer.com/content/pdf/10.1007/97 8-1-4842-2155-6.pdf
[3] Cybersecurity in Healthcare : A narrative review oftrends, threats and ways forward https://www.sciencedirect.com/science/article/abs/pii/ S0378512218301658
[4] Cybersecurity in Healthcare : A systematic review of modern threats and trends https://content.iospress.com/articles/technology-and- healthcare/thc1263
[5] HIPAA Research Chapter V



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY