Healthcare Data Security and Privacy

Ashish Goyal
Computer Science
Case Western Reserve University
Cleveland, Ohio
axg1503@case.edu

Shraddheya Vinod Tarekar
Computer Science
Case Western Reserve University
Cleveland, Ohio
sxt887@case.edu

Prassana Kumar
Computer Science
Case Western Reserve University
Cleveland, Ohio
pxp488@case.edu

ABSTRACT

As the healthcare industry continues to embrace digital transformation, the importance of safeguarding sensitive patient information becomes paramount. This paper addresses the critical issue of healthcare data security and privacy, focusing on the challenges and emerging solutions in an era of increasing cyber threats and evolving regulatory landscapes.

The first section of the paper delves into the current landscape of healthcare data, highlighting the types of sensitive information stored, the stakeholders involved, and the potential risks associated with data breaches. Emphasis is placed on the evolving threat landscape and the need for adaptive security measures.

The second section evaluates existing regulatory frameworks and industry standards related to healthcare data security and privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). The paper critically analyzes the strengths and weaknesses of these frameworks, proposing potential enhancements to address emerging challenges.

The third section focuses on emerging technologies such as blockchain and artificial intelligence, exploring their potential applications in healthcare data security. The paper assesses how these technologies can contribute to data integrity, secure data sharing, and early detection of security threats. Also the surveys that we have shared with the different sets of people

Finally, the paper concludes with a synthesis of key findings and recommendations for healthcare organizations, policymakers, and technology developers. By adopting a multifaceted approach that combines robust technical measures, stringent regulations, and ongoing education and awareness initiatives, the healthcare industry can strengthen data security and privacy, ensuring the trust and well-being of patients in the digital age.

KEYWORDS

Data privacy, Data Security, Healthcare, Encryption, IoT Technology, Blockchain Technologies, Healthcare industry, Data Breach, Transmission.

I. Overview of terminology and Process

A. Data Security

Data security is the process of protecting digital information from unwanted access, including electronic health records. Organizations in the healthcare sector are safeguarded against:

- Digital Assaults
- Data Hack
- Further security risks

The patient data that is at risk from these dangers and hacking efforts may be vulnerable to theft, criminality, terrorism, and natural disasters. Generally speaking, data security includes a number of procedures, like:

- Encrypting Data
- Data hiding; recovery after disasters
- Use of tokens.

Furthermore, technological advancements as well as user security and privacy policies are necessary for effective data security.

B. Data Security in Healthcare

In order to preserve private patient information and adhere to laws such as those imposed by HIPAA, data security is a critical component of

the healthcare sector. Previously, patient data was stored on paper records that were secured in filing cabinets, making it relatively simple to safeguard and make secure.

However, patient records are now electronically stored on computers, servers, and storage devices as a result of technological advancements and the advent of the digital age. There is a higher chance of viruses, malware, data breaches, and other hostile attacks when there are electronic records.

In order to access, update, and record patient data, doctors, nurses, and other healthcare professionals now rely on technologies like computers and tablets. Additionally, data exchanges between various healthcare facilities and providers are possible. Therefore, in order to lower the chances of malicious data attacks or technological failure, better healthcare data security solutions are required.

C. Why Is Data Security Important in Healthcare

Data security in healthcare is vital to uphold ethical standards, comply with legal regulations, protect patient confidentiality, maintain trust, and prevent the potentially devastating consequences of data breaches, identity theft, and other security threats. It is not only a matter of protecting information but also a matter of safeguarding patient well-being and the integrity of the healthcare system.

Currently, one of the healthcare industry's top concerns is data security. In recent years, the industry has seen a sharp increase in data breaches and cyberattacks.

A 2021 study found that between 2019 and 2020, there was a 55.1% increase in healthcare breaches. In 2020 alone, there were nearly 600 data breaches. It can take a long time to recover from and be costly to fix breaches. The typical healthcare organization needed 236 days and $500 on average per compromised patient record to recover from a data breach. Health care violations are frequent and can have severe repercussions. By implementing data protection measures, healthcare organizations must remain vigilant against intrusions and breaches.

II. Why Healthcare Data Services and Privacy

For a number of crucial reasons, including patient safety, maintaining ethical standards, adhering to legal requirements, maintaining data integrity, and preventing identity theft, healthcare data security and privacy are crucial. These steps are essential to providing reliable, efficient, and safe healthcare services.

Healthcare data security is paramount to protect patient privacy and prevent unauthorized access or breaches. Violations of confidentiality and privacy can be harmful in addition to potentially affecting someone's dignity.

Policies and technology used to safeguard patients' and medical clients' sensitive health information are included in the category of healthcare data privacy. Protected health information (PHI) or sensitive patient medical data may only be viewed by those who are authorized, such as physicians.

All medical institutions, including large hospitals, small clinics, and private practices, are required by law and morality to protect patient health information (PHI) from unauthorized individuals. Medical records of patients may be gathered by numerous organizations or individuals for a number of purposes, such as financial gain or ransoming, among others. Medical organizations can safeguard their patients' and clients' private health information and fortify their systems against unauthorized digital intrusions by implementing smart healthcare data privacy practices.

Data breaches and cyberattacks are much more common these days due to the rapid spread of digitalization, making patient information more vulnerable than ever. For this reason, ensuring the highest level of data privacy is crucial for healthcare services.

III. Impact of Data Breaches

A data breach in healthcare can have significant and far-reaching impacts on individuals, healthcare organizations, and the broader healthcare ecosystem.Both short-term and long-term effects are possible. It can severely damage a healthcare organization's reputation, reducing public trust and patient confidence. These breaches occur when sensitive patient

information is accessed, disclosed, or stolen without authorization. The number of healthcare data breaches, the volume of records exposed, and the monetary losses brought on by compromised records are all rising quickly. Information from the medical field is considered to be extremely valuable.

The following are some of the most significant effects of data breaches in the healthcare industry:

- Legal and regulatory penalties
- Patient Privacy Violation
- Financial Loss
- Reputational Damage

A. Legal and regulatory penalties

Healthcare organizations that experience data breaches may face legal consequences, including fines and lawsuits for failing to protect patient data adequately. Laws like the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose strict regulations and penalties for non-compliance. Government agencies and regulators may intensify their scrutiny of healthcare organizations following a data breach. This can result in audits, fines, and additional regulatory requirements. Data breaches can lead to severe legal and financial penalties for non-compliance.

B. *Patient Privacy Violation*

Patient privacy is a fundamental right in healthcare. When a data breach occurs, patient information, including personal and medical records, can be exposed. This breach of privacy erodes trust between patients and healthcare organizations. Stolen healthcare data can be used for identity theft, leading to financial fraud, insurance fraud, and other criminal activities. Criminals may use the stolen information to obtain medical services or prescription drugs under the victim's name. If a data breach disrupts healthcare operations, it may impact patient safety by impeding access to critical medical records and information, potentially leading to medical errors or delayed treatment.

C. *Financial Loss*

Data breaches can result in significant financial costs for healthcare organizations. These costs may include legal fees, notification and credit monitoring services for affected patients, and potential fines. Victims may incur expenses related to identity theft protection services, legal fees, or financial losses due to fraud. Data breaches require thorough investigation, notification of affected individuals, and implementing security measures to prevent future breaches. These processes are costly.

Long-Term Financial Impact are :

- Ongoing monitoring and support: Healthcare organizations may need to provide ongoing credit monitoring and support to affected individuals, incurring costs that can extend for several years.

- Loss of grants and funding: Research institutions and nonprofit healthcare organizations may lose grant funding or charitable donations as a result of reputational damage from data breaches.

D. *Reputational Damage*

Healthcare providers and institutions can suffer severe reputational damage as a result of a data breach. News of a breach can tarnish their reputation and make it difficult to attract and retain patients and partners. Patients may seek care elsewhere if they believe a healthcare provider cannot protect their data, leading to a loss of business. Media coverage of data breaches in healthcare can lead to negative public perception. It can result in damaging headlines and public scrutiny, making it difficult for the organization to recover its reputation.

Reputation damage can also affect the ability of the healthcare organization to attract and retain top talent, as potential employees may have concerns about the organization's security practices. Patients who lose trust in a healthcare organization may seek care elsewhere. This can result in a loss of patients, reducing the organization's revenue and damaging its long-term viability.

IV. Current Threats to Healthcare Data Security

Healthcare data security is a critical concern due to the sensitive and personal information stored in

electronic health records (EHRs), insurance records, and medical databases. Several threats to healthcare data security persist, and they continue to evolve. It's important to note that the threat landscape evolves rapidly, so it's essential for healthcare organizations to stay vigilant and adapt to new threats.

A. Phishing Attacks

The most common cybersecurity risk in the healthcare industry is phishing. Phishing attacks involve deceptive emails or messages that trick employees into revealing sensitive information, such as login credentials, which can then be used to access healthcare systems.

The most common type of phishing attacks is email phishing. In healthcare, the consequences of falling victim to phishing attacks can be severe, potentially resulting in data breaches, compromised patient records, and financial losses.

Here are some specific aspects of phishing attacks and their impact on healthcare data security :

- Data Breaches : Phishing attacks can lead to data breaches if healthcare employees are tricked into disclosing login credentials or providing access to patient records. Attackers can then steal or manipulate patient data.
- Compromised Login Credentials : Phishing attacks often target login credentials, and once attackers gain access to healthcare systems, they can view, steal, or manipulate patient records, leading to data breaches.
- Email-Based Phishing: Phishing emails, disguised as legitimate communication, may contain malicious links or attachments. Clicking on these links or downloading attachments can install malware on the victim's computer, potentially compromising the entire network.

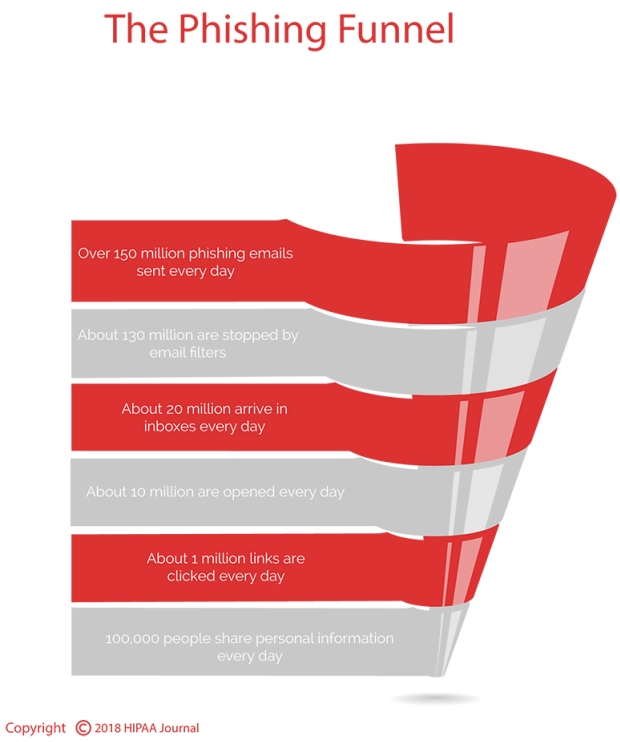

Figure 1: The Phishing Funnel

B. *Ransomware*

Ransomware attacks have been on the rise in the healthcare sector. Cybercriminals use malware to encrypt patient data and demand a ransom for its release. This can disrupt healthcare services and compromise patient safety. In the healthcare sector, the impact of ransomware attacks can be particularly devastating due to the critical nature of patient data and the need for uninterrupted access to medical records.

Here are the key aspects and threats associated with ransomware attacks in healthcare:

- Data Encryption and Inaccessibility: Ransomware encrypts critical patient data, making it inaccessible to healthcare providers. This can disrupt patient care, cause treatment delays, and compromise patient safety.
- Ransom Demands : Attackers typically demand a ransom payment, often in cryptocurrency, in exchange for the decryption key. Paying the ransom is

discouraged by law enforcement agencies and cybersecurity experts, as it doesn't guarantee data recovery and may incentivize further attacks.

- Financial Costs : Dealing with a ransomware attack can result in significant financial costs for healthcare organizations. These costs include the ransom itself, incident response efforts, system restoration, and potential regulatory fines for data breaches.

C. Insider Threat

Insider threats are a significant concern in healthcare data security. These threats involve individuals within an organization, such as employees, contractors, or business associates, who misuse their access privileges to compromise the confidentiality, integrity, or availability of healthcare data. Insider Threats are responsible for 90% of security incidents.

Insider threats can be intentional or unintentional and may include the following aspects and threats to healthcare data security:

- Unauthorized Data Access : Insiders with legitimate access to patient data may misuse their privileges to access information that they should not, potentially for financial gain, personal reasons, or malicious intent.

- Data Theft and Exfiltration : Insider threats can lead to the theft and exfiltration of sensitive patient data, which can be sold on the black market or used for identity theft and fraudulent activities.

- Data Modification : Insiders may tamper with patient records or healthcare data, which could have serious consequences for patient care, including incorrect diagnoses and treatments.

D. IoT Vulnerabilities

IoT (Internet of Things) vulnerabilities present a growing threat to healthcare data security. As the healthcare industry increasingly adopts IoT devices, such as connected medical equipment, wearables, and remote monitoring devices, the attack surface for cybercriminals expands.

A recent study conducted by healthcare cybersecurity company Cynerio found that in the previous two years, 56% of hospitals experienced attacks on their IoT/IoMT devices. 88% of data breaches involved IoT devices. An alarming figure is that 53% of medical IoT devices have at least one critical vulnerability.

Here are some of the key aspects and threats related to IoT vulnerabilities in healthcare data security:

- Inadequate Security Protocols : Many IoT devices in healthcare lack robust security features. These devices are often designed with a focus on functionality and cost, neglecting essential security measures like encryption and authentication.

- Absence of Patching and Updates: Internet of Things devices might not be regularly updated with security patches. Vulnerabilities discovered in these devices often remain unaddressed, leaving them susceptible to exploitation.

- Unauthorized Access : IoT devices may be accessible via the internet or connected to a network, providing potential entry points for attackers. If not properly secured, unauthorized individuals could gain access to these devices and the patient data they handle.
- Data Interception : IoT devices may transmit patient data wirelessly. If this data is not encrypted or secured, it can be intercepted by attackers, compromising patient privacy and confidentiality.

V. Regulatory Compliance Requirements

Regulatory compliance requirements in data privacy for the healthcare industry are essential to safeguard patient information, maintain patient trust, and protect sensitive healthcare data. It is a critical aspect of the healthcare industry, with various regulations like HIPAA, HITECH ACT,

EU GDPR, INDIA DPDP 2023. These rules are designed to enhance operational efficiency while preventing fraud, waste, and abuse, safeguarding worker safety, and protecting patient privacy.

A. *Health Insurance Portability and Accountability Act (HIPAA)*

The Health Insurance Portability and Accountability Act of 1996 outlines national standards for the protection of electronic personal health information (ePHI).

- Since its implementation in 1996, HIPAA has been one of the most important regulations in the healthcare industry to comply with.
- The regulation has significantly impacted how health information is managed and shared among different stakeholders in the healthcare industry. Its goal is to guarantee that people's protected health information is kept private, secure, and unreadable by outside parties.
- Technological measures include limiting authorized personnel's access to ePHI, requiring them to use unique identity methods (MFA) to verify their identity, keeping an eye on hardware and software access logs for unusual activity, encrypting sensitive data, and defining emergency access protocols.
    -
- Physical safeguards like restrictions on who can physically access facilities, enforce restrictions on access to workstations and electronic media, and procedures for disposing of or moving workstations and electronic media.

B. *B. Health Information Technology for Economic and Clinical Health (HITECH) Act*

The Health Information Technology for Economic and Clinical Health (HITECH) Act is a significant piece of healthcare legislation enacted in the United States as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Enforces stricter security and privacy requirements for electronic health records (EHRs) and introduces financial incentives for the meaningful use of EHRs.

- HITECH Act modifications to HIPAA and other rules.
- Several privacy provisions from the HITECH Act were incorporated into HIPAA through the Final Omnibus Rule.
- Expansion of patients' rights to receive copies of and amend PHI
- Changing the specifications for Notices of Privacy Practices
- Extending the list of disclosures requiring permission
- Limitations on disclosures for treatment payments made privately
- Permission for families and other authorized parties to access PHI

C. *EU General Data Protection Regulation (GDPR)*

The General Data Protection Regulation of the European Union applies to all healthcare organizations that store or process data related to EU residents, regardless of location. It Requires explicit consent for data processing, mandates data protection impact assessments, and imposes strict notification and reporting requirements for data breaches.

- **Privacy by design** : The term "Privacy by Design" means nothing more than "data protection through technology design." This is based on the idea that data protection practices in data processing operations are best followed when they are built into the technology from the beginning.
- **Privacy by default**: A social media platform should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, restricting the user's profile's accessibility right away to prevent an infinite number of people from having default access to it.

D. *INDIA DPDP 2023*

The Bill calls for the processing of digital personal data in a way that respects people's rights to privacy protection as well as the necessity of processing such data for legitimate purposes and for purposes related to or incidental to those purposes.

The following seven guiding concepts form the basis of the Bill:

- Consent-based, lawful, and open use of personal data is a fundamental principle.
- Use of personal data only for the purposes indicated at the time of obtaining consent from the data principal is known as the purpose limitation principle.
- The data minimization principle states that personal information should only be collected to the extent required to fulfill a given purpose.
- The accuracy of data principle (making sure data is updated and accurate).
- The storage limitation principle (keeping data only as long as it's required for the intended use).
- The principle of reasonable security safeguards.
- The accountability principle (adjudicating data breaches and Bill provisions violations and imposing penalties for the breaches).

VI. PRIVACY CONSENT

Privacy consent is a crucial aspect of data privacy in healthcare. It refers to the formal and voluntary agreement given by a patient or data subject to allow a healthcare provider or organization to collect, process, and share their personal health information. Privacy consent is essential to protect patient rights and privacy while ensuring that healthcare providers can provide necessary care and services. Most of the data protection acts have privacy consent as one of main regulations.

Facts regarding privacy consent :

- In GDPR they used the term consent 108 times, imagine how hard and complex it is.
- PayPal privacy notice is 36275 words. That's by the way longer than Hamlet company.
- iTunes privacy policy comes to 19972, just longer than Macbeth. Imagine how long it takes us to read that.
- iTunes privacy policy comes to 19972, just longer than Macbeth. Imagine how long it takes us to read that.

A. Privacy Preservation Strategies

Data privacy in healthcare is critical to protect patients' sensitive information and maintain trust in healthcare systems.

Preventing security breaches in healthcare can be challenging and will often require extra funding, but in the long run it may save the organization from bigger problems, including loss of reputation. The following are the principal actions that can be taken to improve healthcare data security.

- Data encryption
- Avoid using Old infrastructure
- Firewalls
- Multi Factor Authentication

VII. Data Authorization and Authentication

It ensures the information is only accessible to authorized users and also helps to safeguard medical data from unauthorized access to reduce the risk of data breaches and cyber attacks. Sensitive patient data is protected from unauthorized access and interaction thanks to these procedures. Robust authorization and authentication procedures are essential in the healthcare industry because patient privacy and security are of utmost importance.

A. Biometric Authentication

Authentication is the process of confirming the identity of a user or system attempting to access healthcare data. Biometric authentication is a robust and increasingly popular method for enhancing data privacy and security in healthcare. It involves using unique physical or behavioral

traits of individuals to verify their identities. Biometric authentication can provide several benefits in the context of healthcare data privacy.

- Strong Security
- Patient Identification
- Prescription Verification
- Two-Factor Authentication
- Reducing Fraud

It's critical to take into account any potential issues with biometric authentication in the healthcare industry, such as the requirement for biometric templates to be stored securely, ethical issues, and potential privacy implications. In order to safeguard patient data, healthcare organizations must also adhere to all applicable data protection laws and regulations when implementing biometric authentication.

B. Facial Recognition

The potential of facial recognition technology to improve security and expedite access to sensitive information and facilities has made it popular in a number of industries, including the healthcare sector. Facial recognition has potential advantages and disadvantages with regard to data privacy in the healthcare setting.

- Enhanced Security
- Patient Identification
- Access Control
- Patient Consent and Authorization
- Streamlining Processes

In addition to providing a number of benefits for improving security and patient identification in healthcare, facial recognition technology raises privacy and ethical issues. When using facial recognition technology, healthcare organizations must obtain patient consent and implement the necessary safeguards to ensure data privacy and regulatory compliance. Furthermore, it is crucial to continuously monitor and assess the accuracy and fairness of the technology.

VIII. Healthcare Industry in India

- India's healthcare system is a hybrid of the public and private domains.
- The healthcare industry in India is rapidly evolving and the diverse sector plays a crucial role in providing medical services to a population of over 1.3 billion people.
- India's hybrid healthcare system includes both public and private healthcare providers.
- Over the years it has shown tremendous growth, and development. But with this the cyber attacks has also being increased rapidly.
- According to an article written by "The Wire", nearly 60% of the healthcare organisations in India have suffered cyber attack over the last year.
- According to an article by "Mint", in 2022 till november 28, Indian healthcare organisations faced 1.9 million attacks.

IX. Cyber Attacks Happened in India

Nearly 60% of healthcare organizations in India have suffered a cyberattack in the past 12 months

India is ranked 10th out of the countries that saw the most cyberattacks in 2022, which should raise red flags throughout the nation. According to a report published by the Indian Future Foundation, these cyberattacks affected businesses of all sizes in every industry, so no sector was immune.

AIIMS : It fell victim to one of the biggest ransomware attacks. This attack encrypted critical data, forcing the company's IT systems to shut down.

Sun Pharmaceutical : The IT systems were impacted due to the attack which resulted in a major data breach. ALPHV ransomware group has claimed responsibility for the attack.

The Indian government and private organizations have taken measures to enhance cybersecurity, including the establishment of cybersecurity agencies, promoting awareness, and implementing security protocols. However, the evolving nature of cyber threats requires ongoing efforts to stay ahead of potential risks.

X. SCOPE OF SURVEY

The purpose of this survey is to investigate in depth the perspectives, experiences, and concerns of healthcare professionals, particularly doctors, regarding healthcare data security and privacy. The survey aims to assess doctors' general awareness of data security and privacy issues in the healthcare sector by addressing a variety of topics. It delves into current practices used by healthcare facilities to ensure the security and privacy of patient data, such as the use of technologies and the frequency with which access credentials are updated. The survey seeks information about perceived risks, experiences with security breaches or privacy violations, and patient consent management in relation to health data sharing.

It also investigates the strategies and challenges of maintaining regulatory compliance, as well as the perceived need for additional data security and privacy training. The scope includes determining how healthcare facilities are prepared to respond to incidents and the challenges they face in adopting new technologies to improve data security. Finally, the survey delves into doctors' perspectives on future trends and technologies that have the potential to improve healthcare data security and privacy, providing a comprehensive overview of the current landscape and future considerations in this critical area..

XI. SURVEY QUESTION AND FINDING

A. Questions

- How Familiar are you with the current healthcare data security and privacy regulations?
- What steps are taken in your practice to ensure compliance with data protection laws?
- Have you received training on healthcare data security and privacy?
- How confident do you feel in your ability to safeguard patient information?
- How is access to patient data controlled within your practice?
- Is Data stored or transmitted in encrypted form?
- What Encryption methods are employed to secure electronic healthcare records.
- What procedures are in place to respond to a data security breach ?
- Have you encountered data security in your organization and how was it handled ?
- Are there specific techniques or tools that you find effectively enhancing healthcare data security ?
- How is patient consent obtained for the collection used for their health data?
- How closely do you work with IT professionals to address security issues?
- In your experience what role does collaboration between healthcare providers and IT Specialist plays in enhancing data security
- What emerging technologies or trends do you see impacting healthcare data security in future?
- How do you anticipate the landscape of healthcare data security evolving over the next few years ?
- How often do you update passwords and credentials for electronic health record systems ?

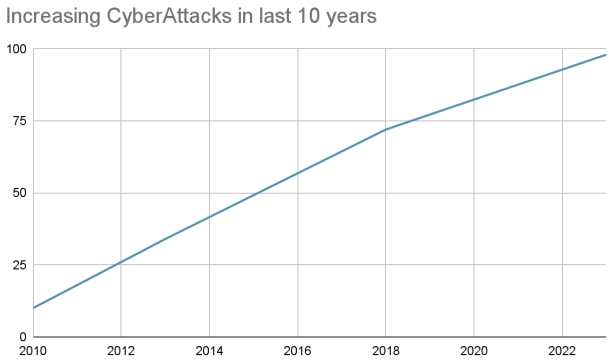

Figure 2: Line Chart - Increasing Attacks

B. Findings

- The majority of healthcare workers are unaware of the rules and regulations governing the data protection.
- No hospital has conducted any training on healthcare data security and privacy to ensure compliance with data protection laws.
- Some hospitals healthcare professionals give their credentials to their juniors to access the data, whereas others grant access to every healthcare worker, allowing him or her to access data related to the case on which they are working.
- Some hospitals store patients data digitally, while others store it both digitally as well as in registers/notebooks.
- Doctors take screenshots of scans or the documents and send it via messaging apps such as whatsapp.
- When there is a security breach, healthcare workers are not aware of any procedures to follow.
- In some of the hospitals, consent is not regarded as such. The patient is not informed of what is happening with their data.
- If there are any problems with the computers or their systems, a third party IT professional is called in. Credentials has been shared to the colleagues, and the password has not been changed for a while.
- Softwares gets updated every two to three months in some hospitals. Hospital infrastructure does not include cyber security.

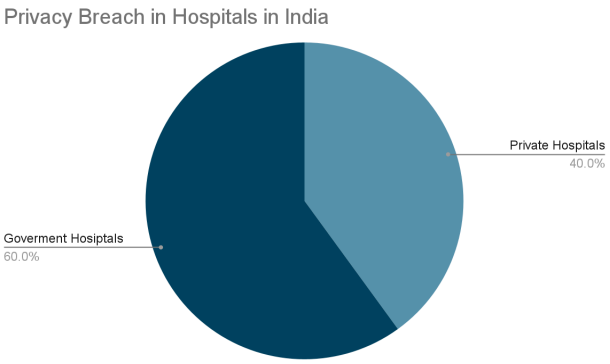

Figure 3: Pie Chart explaining Breach

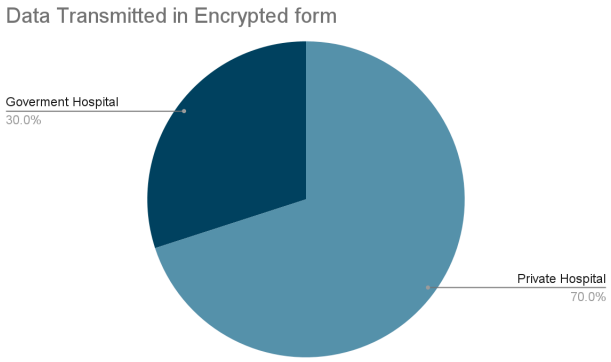

Figure 4: Pie Chart explaining Data transmission in encrypted form

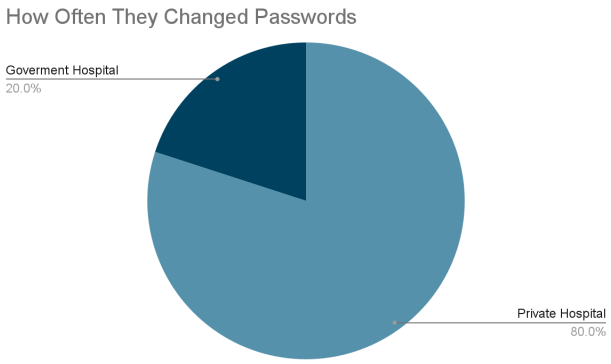

Figure 5: Pie Chart - changing password

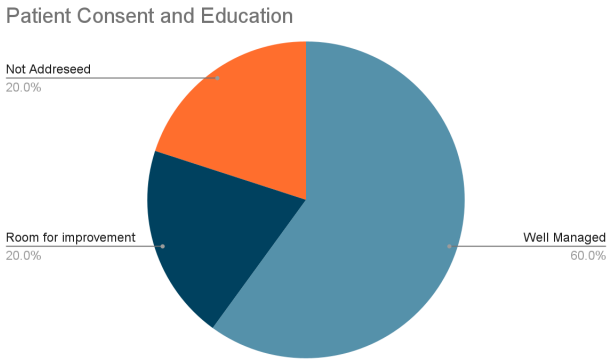

Figure 6: Pie Chart - Patient consent in India

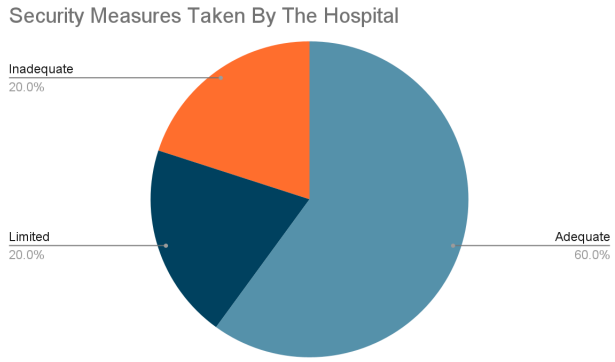

Figure 7: Pie Chart - Security Measures

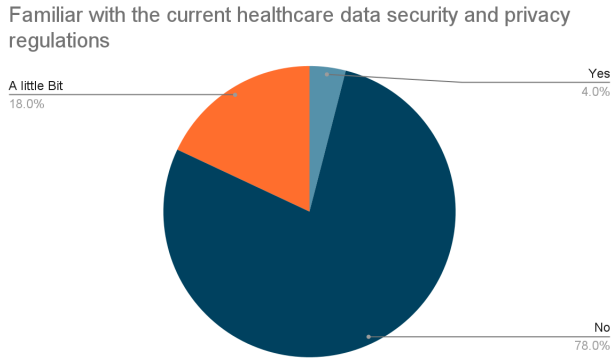

Figure 8: Pie Chart - Laws

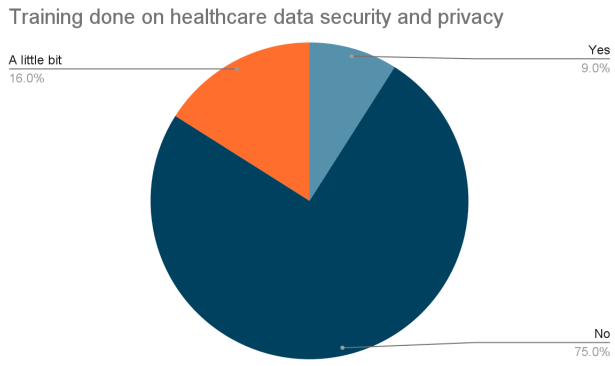

Figure 9: Pie Chart - Training

XII. Problems seen after Survey

- Healthcare workers are unaware of the laws and their significance.
- They do not receive adequate training on data privacy and security.
- The infrastructure is not properly secured. Hospitals infrastructure does not focus more on cyber security.
- There is no awareness among the healthcare workers. Because of the lack of awareness, the systems in some hospitals does not get updated enough.
- The patient does not know what is happening with their data.
- Registers and notebooks are used to write the personal data of the patients.
- The data transferring from one device to another may or may not be encrypted.
- Passwords are not changed on a regular basis.
- There is a little or no interaction between healthcare workers and IT professionals because some hospitals lack IT professionals.
- There are no regular security audits that has been done.

XIII. Mitigations

- To educate healthcare professionals, a public awareness campaign about data privacy and security should be implemented.
- The infrastructure should be updated and patched continuously involving aspects of cybersecurity. Securing the data at rest and in transit by implementing strong encryption.
- Setting up an IT security department in hospitals. HIPAA, Information Technology Act of 2000 compliance must

be made compulsory. Passwords should expire every 60 - 90 days automatically.

- Implementation of single sign ons should be carried out extensively.
- Multiple step verification should be implemented.
- Downloaded files should have a password support meaning they should only open after entering password.
- Every time someone tries to access a patient's file, a token should be generated and should expire when the user logs out.
- The healthcare worker should only be able to access the files of the patient in certain devices.

XIV. Conclusion

- The Indian healthcare system is vulnerable to cyber security attacks, which could be mitigated in the future by doing simple things like training healthcare professionals.
- Adaptation of cybersecurity tools like SaaS products, or partnering with service providers like MSSPs can offer expert guidance and monitoring.
- The investment in backups and endpoint protection can be useful in protecting the data.
- More public education and awareness campaigns are required to emphasize the value of protecting health information. It is imperative that individuals and healthcare providers alike receive education regarding optimal data security practices.
- Encryption and blockchain are examples of cutting-edge technologies that can be adopted to improve the security of medical data. The confidentiality and integrity of patient data can be improved with the use of these technologies.

REFERENCES

[1] Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. Big healthcare data: preserving security and privacy. J Big Data 5, 1 (2018). https://doi.org/10.1186/s40537-017-0110-7

[2] Murdoch, B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med Ethics 22, 122 (2021). https://doi.org/10.1186/s12910-021-00687-3

[3] "What does data protection 'by design' and 'by default' mean? " [Online]. Available : https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

[4] "Privacy by Design" [Online]. Available : https://gdpr-info.eu/issues/privacy-by-design/

[5] "Salient Features of the Digital Personal Data Protection Bill, 2023" [Online]. Available : https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264

[6] "What is Regulatory Compliance in Healthcare" [Online]. Available : https://compliancy-group.com/what-is-regulatory-compliance-in-healthcare

[7] "Protect Healthcare Data from Phishing" [Online]. Available : https://www.hipaajournal.com/protect-healthcare-data-from-phishing/

[8] "The Importance of Data Privacy in Healthcare"[Online]. Available : https://www.tigahealth.com/the-importance-of-data-privacy-in-healthcare/

[9] "What is Data Privacy in Healthcare" [Online]. Available : https://www.tonic.ai/blog/what-is-data-privacy-in-healthcare-everything-you-need-to-know

[10] "THE IMPORTANCE OF HEALTHCARE DATA SECURITY" [Online]. Available : https://primetsr.com/insights/the-importance-of-healthcare-data-security/

[11] "TED talk regarding consent. [Online]. Available: https://www.youtube.com/watch?v=2iPDpV8ojHA&t=426s

[12] "India is the 10th most affected country by cyberattacks in 2022 with healthcare sector most impacted: Report [Online]. Available: https://www.businesstoday.in/technology/news/story/india-is-the-10th-most-affected-country-by-cyberattacks-in-2022-with-healthcare-sector-most-impacted-report-399963-2023-09-27

[13] "Sun Pharmaceutical Cyber Attack Confirmed, ALPHV Ransomware Claims Responsibility [Online]. Available: https://thecyberexpress.com/sun-pharma-cyber-attack/

[14] “Indian healthcare system needs robust cybersecurity infra. Here's what experts say [Online]. Available: https://www.livemint.com/news/india/india-healthcare-system-robust-cybersecurity-infrastructure-aiims-cyberattack-safdarjung-hospital-sun-pharma-cyberattack-11682223039473.html

[15] “Nearly 60% Of Healthcare Organisations in India Hit by Cyberattacks in Past Year: Report [Online]. Available: https://thewire.in/tech/nearly-60-of-healthcare-organisations-in-india-hit-by-cyberattacks-in-past-year-report