Comparative Study of Patient Data Safety Considering Security and Privacy Standards Between Indian and U.S. Hospitals

By

Aditi Mathur

Dissertation submitted for the partial fulfillment of the

MBA Hospital and Health Management

Academic year, 2015-2017

The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Sanganer, Airport
Jaipur 302029, Rajasthan
Ph: 0141 3924700, Fax: 3924738
Website: **www.iihmr.edu.in**

Comparative Study of Patient Data Safety Considering Security and Privacy Standards Between Indian and U.S. Hospitals

By

Aditi Mathur

Dissertation submitted for the partial fulfillment of the

MBA Hospital and Health Management

Academic year, 2015-2017

NTT Data, Bengaluru

The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Sanganer, Airport
Jaipur 302029, Rajasthan
Ph: 0141 3924700, Fax: 3924738
Website: www.iihmr.edu.in

INSTITUTE OF HEALTH
MANAGEMENT RESEARCH
(WHO Collaborating Centre for District Health System Based on Primary Health Care)

IIHMR UNIVERSITY

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Aditi Mathur student of MBA Hospital and Health Management. The IIHMR University, Jaipur has undergone internship training at NTT DATA, Bangalore from 6th February to 5th May, 2017.

The Candidate has successfully carried out the study designated to her during internship training and her approach to the study has been sincere, scientific and analytical.
The Internship is in fulfilment of the course requirements.

I wish her all success in all her future endeavours.

(Col.) Dr.Ashok Kaushik
Dean, Academics and Student Affairs
The IIHMR University, Jaipur

Dr. NutanP. Jain
Professor
The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Near Sanganer Airport, Jaipur- 302029, Rajasthan, India.
Ph.: 0141- 3924700, 2791431- 32, Fax: 0141 3924738, E-mail: iihmr@iihmr.edu.in, Web.: www.iihmr.edu.in

NTT DATA Information Processing Services Private Limited
(Formerly known as Dell Business Process Solutions India Private Limited)
Plot 123, EPIP Phase II, Whitefield Industrial Area
Bengaluru, Karnataka 560 066, India

NTT DATA
Global IT Innovator

To whomsoever it may concern

This is to certify that **Aditi Mathur** of **The IIHMR University, Jaipur** has been working with NTT DATA Services for her summer project.

Project Details:

Project Name : A comparative study of patient data safety considering security and privacy standards between Indian and US Hospitals
Duration : 90 days
Location : Bangalore
Guide Name : Dr. Shelja Khurana & Piyalee Pandit
Sponsor Name : Ajay Aiyar

She has successfully completed her project and her performance during the tenure of the internship has been found to be satisfactory.

Her findings in course of the project has been found to be practical and relevant and some of the recommendations will be incorporated on the floor on approval from the business.

Thanking You,

Regards,

Dilipkumar Santhanam
Business Partner Director, Services HRBP Team
NTT DATA Services

THE IIHMR UNIVERSITY, JAIPUR

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled "A Comparative Study of Patient Data Safety Considering security and Privacy Standards between Indian and US Hospitals" submitted by Aditi Mathur Enrollment No. (IIHMR-U/01/2015-17/0247) under the supervision of Nutan Purohit Jain for award of MBA in Hospital and Health Management of the University carried out during the period from February to May embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other institute or other similar institution of higher learning.

Aditi Mathur

Signature

THE IIHMR UNIVERSITY, JAIPUR

CERTIFICATE BY SCHOLAR

This is to certify that all ethical issues have been considered while collecting data for my dissertation titled ''A Comparative Study of patient data safety considering security and privacy standards between Indian and US hospitals''.

Aditi Mathur

Signature of student

Acknowledgement

I started off my training with a vision in my mind so as to be able to learn about the practical aspects of Healthcare Information Systems in a detailed manner.

I am thankful to **Ajay Ayar**(Senior Manager) for giving me the opportunity to carry out my dissertation and for his constant support and encouragement. I am thankful to him for the time and efforts they spent from his busy schedule.

I wish to express my sincere gratitude to **Avishikta Sarkar,** (IT Service Manager) for her supervision, advice, and guidance. She was a source of inspiration and has enriched my growth as a student, a researcher. I am indebted to him, for his faith in me and providing the right direction whenever I needed it the most.

I thank my managers, **Archika Roy**(Service IT Manager) and **Ramkishore M.P.**(Service IT Manager) for their guidance and interest in my work and their time.

My heartfelt thanks to my mentors **Shelja Khurana (**Business Systems Analyst) and **Piyali Pandit (**Business Systems Analyst) for their tremendous help as a mentor and providing the much needed support, meticulous work habits, immense patience and for answering my endless questions when I started my work.

I am thankful to all the members of NTT Data Service who helped me in one way or the other to carry out my work successfully and to learn about the Electronic Medical Records (EMR) systems and those who were a part of my project without whose unconditional cooperation my study would not have been completed successfully. My special thanks to **Col. Dr. Ashok Kaushik**, Dean Academics and Students Affair, IIHMR University, Jaipur for being a continuous guiding source throughout the degree, I would also like to thank **Dr. Nutan P. Jain** IIHMR University, my guide for providing me support in completing my project successfully as well as giving insight in to my operational issues which came across during the project.

My colleagues from different colleges also hold a special mention here for supporting me throughout the training and making it a great learning experience.

Aditi Mathur

ABSTRACT

Introduction-

The health information system is evolving day by day. Preserving health information is very important so as to maintain privacy and confidentiality of patients' health information from any harm and misuse. Importance of health information access is a complicated process as relevant workforce should be appointed for the purpose. There are many opportunities if the importance of patient data safety is understood at the right time. The methods generally used are basic data entry in paper files and very limited use of local health information systems in the hospitals. Still traditional methods like paper records are being used even if any healthcare organisation can afford it.

Objectives

1) To understand the differences between patient data safety standards between U.S and Indian Hospitals.
2) To study Indian hospital's perspective on application of data security standards.
3) To study the scope for implementing HIPAA guidelines in Indian hospitals.

Methodology

The study was descriptive and cross-sectional and conducted in NTT data services, Bangalore from February to April, 2017.Six Indian hospitals were identified on the basis of convenient sampling, considering single speciality, super specialty and multispecialty hospitals as per their availability and accessibility. Open-ended questionnaire was designed to capture information on perception about various safeguards used by the hospitals staff. A checklist was developed to observe and record certain administrative, physical, and technical data safety processes/ practices in Indian hospitals for protecting patient data. A total of 105 respondents, 15 from each hospital (six nurses, three doctors or physicians, four administrative and two IT staff) were interviewed.

Results

Administrative and physical safeguards were followed in appropriate manner but technical safeguards were not looked upon very well even if proper HIS system is established in the hospitals. Secondary data analyses revealed that there were appropriate rules and regulations for handling patient data safety which helps to govern the US hospitals. There were stringent rules mandating the US hospitals to disclose data breaches whereas such provisions were lacking in India. Lack of monitoring of application of laws and regulations was found poor. The results revealed that there was less awareness of the significance of patient data safety protocols being followed in the hospitals among the staff members. About one-third of the physicians and nurses responded having HIS is necessary to secure patient for medical legal purposes and continuity of care. To manage patient data in the hospitals 73 per cent nurses and 42 per cent physicians consider both paper records and HIS are the means of data handling in which medical records department plays the major role. One of the major barriers was lack of human resources.

Conclusion

US healthcare is well equipped with rules and India too is on the way of improvement towards sensitive patient health data. Technical, administrative and physical safeguards are adopted in Indian hospitals to some extent to secure patient data. There was a lot of scope in Indian health care to develop better patient data safety standards through skilled human resources, correct knowledge of rules and regulations, and adoption of technical safeguards can lead to streamlined and modern way of data handling.

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Aditi Mathur student of MBA Hospital and Health Management. The IIHMR University, Jaipur has undergone internship training at NTT DATA, Bangalore from 6th February to 5th May, 2017.

The Candidate has successfully carried out the study designated to her during internship training and her approach to the study has been sincere, scientific and analytical.
The Internship is in fulfilment of the course requirements.

I wish her all success in all her future endeavours.

(Col.) Dr.Ashok Kaushik	Dr. NutanP. Jain
Dean, Academics and Student Affairs	Professor
The IIHMR University, Jaipur	The IIHMR University, Jaipur

NTT DATA Information Processing Services Private Limited
(Formerly known as Dell Business Process Solutions India Private Limited)
Plot 123, EPIP Phase II, Whitefield Industrial Area
Bengaluru, Karnataka 560 066, India

NTT DATA
Global IT Innovator

To whomsoever it may concern

This is to certify that **Aditi Mathur** of **The IIHMR University, Jaipur** has been working with NTT DATA Services for her summer project.

Project Details:

Project Name : A comparative study of patient data safety considering security and privacy standards between Indian and US Hospitals
Duration : 90 days
Location : Bangalore
Guide Name : Dr. Shelja Khurana & Piyalee Pandit
Sponsor Name : Ajay Aiyar

She has successfully completed her project and her performance during the tenure of the internship has been found to be satisfactory.

Her findings in course of the project has been found to be practical and relevant and some of the recommendations will be incorporated on the floor on approval from the business.

Thanking You,

Regards,

Dilipkumar Santhanam
Business Partner Director, Services HRBP Team
NTT DATA Services

THE IIHMR UNIVERSITY, JAIPUR

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled "A Comparative Study of Patient Data Safety Considering security and Privacy Standards between Indian Hospitals and US Hospitals" and submitted by Aditi Mathur Enrolment No. (IIHMR-U/01/2015-17/0247) under the supervision of Nutan P. Jain for award of MBA in Hospital and Health Management of the University carried out during the period from February to May embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other institute or other similar institution of higher learning.

Aditi Mathur

Signature

THE IIHMR UNIVERSITY, JAIPUR

CERTIFICATE BY SCHOLAR

This is to certify that all ethical issues have been considered while collecting data for my dissertation titled ''A Comparative Study of patient data safety considering security and privacy standards between Indian and US hospitals''.

Aditi Mathur

Signature of student

10

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

HIS- Health Information System

PHI- Protected Health Information

HIPAA- Health Insurance Portability and Accountability Act

EMR- Electronic Medical Records

1 Introduction

The advancement of health information technology has been a major mission around the globe. Guarding patient's data involved in research or maintaining from harm and preserving their rights is essential to ethical study. But today's healthcare industry is complex in terms of limiting the access to healthcare information to the relevant workforce and understanding the importance of privacy and confidentiality of it. It is essential to stress that privacy also has value at the social level. In different hospitals and data handling organisations, different level of access is required so as to perform multiple functions.

The privacy and security standards are interlinked. According to Ministry of Health and Family Welfare for every health system it is very important to ensure that the patient information is not disclosed, altered, misused, deleted inappropriately during the process of storage, retrieval and transmission.[1]Hence, the privacy and security standards mechanism rely upon protections and appropriate controls.

Organizations must develop security audits and related standards and norms for procedures to hold memberships of the workflow accountable to their actions when accessing e-PHI through the electronic health record (EHR).

EMRs are already used in United States, which is known as the largest health systems of the world. Their agenda is to improve quality, efficiency and convenience. Still, health information system confronts the issues of privacy and security. The Health Insurance Portability and Accountability Act of 1996 for US healthcare is there with the intent of providing information technology with reduced cost, improved quality, ensure continuity and portability of health insurance coverage. The HIPAA has bifurcated its laws into physical, administrative and technical safeguards. The best thing there is that the government provides funds and actively participates in it.

Transforming healthcare through information technology is undoubtedly gaining momentum in India. The adoption of m-Health, eHealth, cloud infrastructure, healthcare data analytics and Customer Relationship Management are all gaining popularity and are promising enough to improve and enable the overall healthcare delivery. Thus confluence of these technologies clearly benefits the maximization of availability of quality healthcare for everyone. Information Technology Rules of 2011 ("IT Rules")

regulates the primary Indian legislation of data privacy under the Information Technology Act, 2000. The I.T. Rules are implemented by the department of Electronics and Information Technology ("I.T Department"). The I.T Rules look out for standardising collection, storage, archival, and disclosure of protected data which is termed as 'sensitive personal data or information'.[2]Hospitalsin India are progressively using EMRs as the preferred method of storing patient information. The law proposed on mandatory use EMR and EHR laid emphasis on maintenance and provision of EMR for every patient under Clinical Establishments (Registration and Regulation) Act of 2010 for the purpose of registration and continuation of clinical institutions.[3]The law which is recently formulated and tentatively called Healthcare Data Privacy and security Act formulate a comprehensive legal framework for protection of individual health data and its standardisation, and identify the "ownership" of that data through the establishment

Unfortunately, there is absence of a proper framework, almost no principles governing how this information should be stored or used. It creates possibilities of medical health data to be misused and commercialised.

Data security and Privacy

The Privacy and the Security Standards are necessarily linked. Any health record system requires safeguards to ensure that the data is accessible when needed and which is not revealed, transformed, edited, used or deleted incorrectly while being stored or retrieved or transmitted.

Three important and correlated concepts are used frequently and interchangeably in discussing protection of health information system and those are *privacy, confidentiality and security*. The fundamental meaning of these concepts has unique roles to perform.

Preserving and securing of patient health information is a top priority for patients as well as their families, healthcare providers and authorities, and the government.

The term "privacy" is often used, yet there no such universally accepted definition, it differs with the perceptions, meaning, and scope of the concept. Privacy addresses the question of who has access and authorised to personal information of the patient and under what conditions. "Privacy is concerned with handling of patient health details by collection, storage, and use of personal information and analysing the authorised

particular use of his or her personal health information. The top-of-mind example of HIPAA Privacy Rule, which has established national standards for health information privacy protection and is named as protected health information".

Confidentiality in health care refers to the duty of professionals who have access to patient records or communication to hold that information in confidence. This professional responsibility to keep health information confidential is supported in professional association codes of ethics, as can be seen in principle I of the American Health Information Management Association Code of Ethics, "Advocate , uphold and defend, the individual's right to privacy and the doctrine of confidentiality in the use and disclosure of information" (AHIMA,2011)[8]. Confidentiality safeguards information that is gathered in context of a close relationship. It addresses the issue of how to keep information exchanged in that relationship from being revealed to third parties. For example, confidentiality prevents physicians from disclosing the physician- patient interaction and information to be shared. Unauthorized or inadvertent disclosures of data of the patient-physician interaction are considered breaches of confidentiality.[4]

Security refers directly to protection and the means to protect the privacy of health information and support professionals in holding that information in self-assurance. The concept of security has been seen as health records in paper form in locked file cabinets. [5]The increasing concern over security of this information buds from the rise of EHRs. Increased use of mobile devices such as smart phones, medical identity theft, and extensively anticipated exchange of data between and among organisations, clinicians, patients, and federal agencies curtails predominantly to the concept of security. The recent survey found that 73% of physicians breach health information by texting other physicians about work. So to keep this information in these exchanges protected is a major concern. Computer workstations are rarely lost, but some of the mobile devices can easily be damaged, misplaced or even stolen and there is another potential threat of data being hacked, destroyed, and manipulated by internal and external users. Consequently, security measures and ongoing educational programs must involve all users. Encryption of mobile devices should be of utmost importance that is used to transmit confidential evidence. Organizations must formally designate a security officer to work within the team of health information technology experts who can keep a check

on system's users, identify security threats and flaws and should have risk taking capability towards safety apprehensions and report them.

Information security and privacy in the healthcare sector is an issue of growing importance. The adoption of digital patient records, increased regulation, and the increasing need for information for patients, providers, and payers, all point towards the need for better information security.

2 Objectives-

1) To understand the differences between patient data safety standards between U.S and Indian Hospitals.
2) To study Indian hospital's perspective on application of data security standards.
3) To study the scope for implementing HIPAA guidelines in Indian hospitals.

3 Methodology-

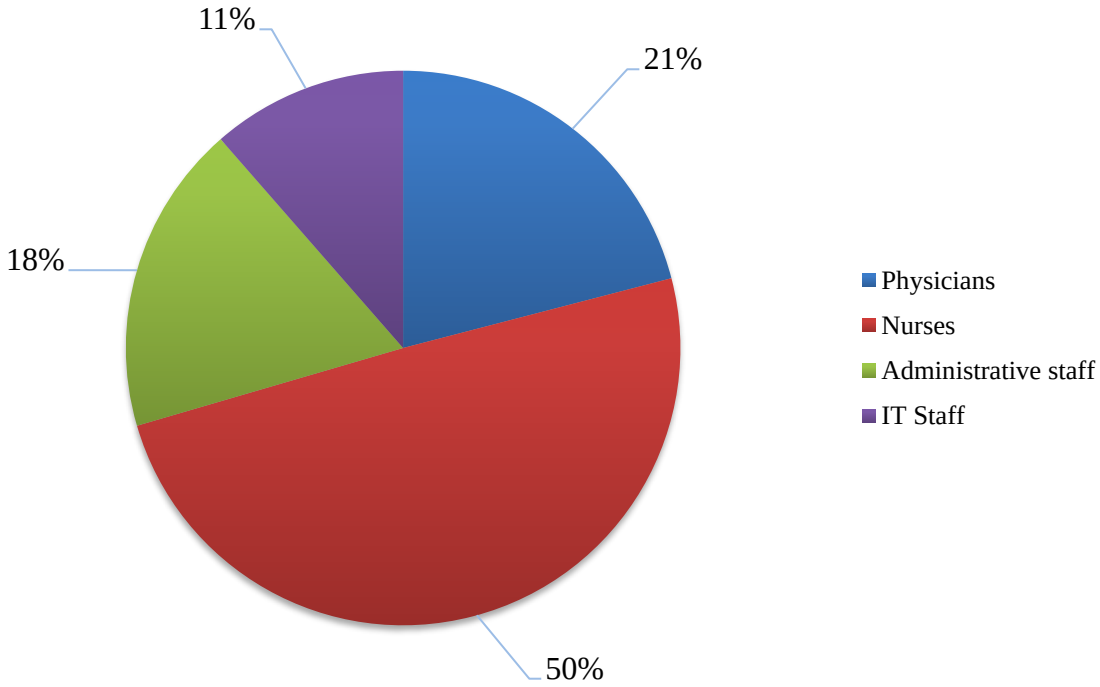
3.1 Study Design- The present study was descriptive and cross-sectional so as to understand the current scenario of patient data security standards being implemented and to what extent the rules and regulations being followed by the hospital staff, their awareness and perspective towards it. The study is conducted in particular period of time and responses were drawn on the present settings of the hospitals.

3.2 Study Duration- Three months from February 2017 to April 2017.

3.3 Study Population-The study was conducted on physicians, nurses, administrative and IT staff of the hospitals in Bangalore.

3.4 Sample Size-From each hospital, following were the respondents from each hospital. In total 22 physicians, 52 nurses, 19 administrative staff and 12 IT staff members were obtained for the whole procedure.

Fig 1: Percent distribution of respondents by their categories



3.5 Sampling Technique-Indian hospitals were identified on the basis of convenient sampling, for the research purpose.

TABLE 1NUMBER OF RESPONDENTS FROM EACH HOSPITAL

Respondents	Hospital A	Hospital B	Hospital C	Hospital D	Hospital E	Hospital F	Total
Physicians	4	3	3	5	3	4	22
Nurses	9	12	7	10	8	6	52
Administrative staff	3	3	4	3	3	3	19
IT Staff	4	2	1	2	1	2	12
TOTAL	20	20	15	20	15	15	105

3.6 Number of hospitals surveyed- Total six hospitals were surveyed considering single speciality, super specialty and multispecialty hospitals as according to their availability and accessibility

3.7 Data source and data collection tool- Primary data was collected through semi-structured questionnaire and checklist. Open ended questionnaire was designed to capture information on the perception, knowledge and awareness about various safeguards used by the hospitals staff. Checklist was designed to analyse certain administrative, physical, and technical data safety processes/ practices in Indian hospitals for protecting patient data. Observations were drawn from the checklist parameters. Secondary data is based on the studies being done so far, various standards rules for Indian as well as U.S healthcare will be performed by reviewing journals, reports, and online articles.

3.8Data analysis and presentation- Survey analysis was done using Microsoft excel and results have been presented in the form of Pie-diagrams, bar and column graphs.

4 Review of Literature

Patient's medical records whether in paper or electronic form are usually moving within different departments and treatment sites which many a times leads to problems in clinical care, and research. This process often comprises the patient's medical records privacy and confidentiality thereby leading to data breaches. There are separate rules and regulations which is being formulated in different countries. Not many studies have been done which clearly states the differences between US and Indian healthcare in terms of security and privacy rules of patient health information safety, rather many fragmented studies were found.

HIPAA i.e., Health Insurance Portability and Accountability Act was enacted on 21 August, 1996. The main agenda of this act was to help reconstruct the health insurance industry and to reorganize administrative processes of healthcare industry. The responsibility of Human and Health services is to make sure about the awareness among public about standards for security, privacy and health information exchange.

According to Standards for Privacy of Individually Identifiable Health Information (known as the Privacy Rule) there are two Goals:

(1) To allow for the electronic flow of health information between covered entities (health plans, healthcare providers, healthcare facilities, healthcare clearing houses) with the purpose of promoting high quality health care.

(2) To protect public's health and wellbeing and the privacy of patient health information".

According to Legal Information Institute, the protected health information(PHI) is the part of privacy rule which protects information namely: "the telephone number, fax number, email address, Social Security Numbers, Medical Record Number, postal address, biometric identifiers such as finger prints, full-face photos and other relevant confidential identifiable information including demographic information collected from an individual and is related to the past, present, future physical mental health of an individual, provision of healthcare and the type of payment.

Another act of security was formulated in 2005, namely The Standards for the Protected of Electronic Protected Health Information which became effective to operationalize the

whole procedure of the security of electronic health information. The rule requires taking stringent steps for the covered entities to protect the integrity, confidentiality and availability of all electronic protected health information (PHI) that they create, receive, maintain, or transmit protect against reasonable breaches or disclosure of PHI; and train their workforce in data security compliance.

Recent studies in the article "Information security and privacy in healthcare: current state of research", broadly categorised privacy threats into two areas:

1) Organisational Threats, which occurs due to wrong means of access of patient data either by internal or external agents, thereby mistreating the privileges given and exploiting the susceptibility of information systems.[10]
2) Systematic Threats, that arise due to an agent in the process flow chain.

It has enlisted organisational threats into five levels:

- Accidental disclosure: When the healthcare information is unintentionally disclosed
- Insider Curiosity: When the data-access privilege is misused for their own benefit.
- Data breach by insider: When one of the insiders access and transmit the information to the outsiders for profit or revenge.
- Data breach by outsider with physical intrusion: When an outsider makes forceful entry and gains access to the system.
- Unauthorised intrusion of network system: When an outsider, including former employees, hackers intervenes somehow in the organisation's network from outside so as to gain access to the system with the intension to make system inoperable, steal data etc.[10]

Systematic Threats: It is commonly observed that the major harm to patient data is not from outside, but is from the inside who is within the flow chain as he/she is the person who has legal access.

The HIPAA Security rule not only provides the guidelines to protect what information but also governs how to store and transfer of the electronic PHI from one location to another.

For Healthcare Maintenance Organisations (HMOs) to work smoothly HIPAA compliance has become a basic business necessity.

4.1 Data Security under HIPAA

According to the Official Publication of the American College of Chest Physicians in the article, "Reframing the influence of the Health Insurance Portability and Accountability Act on Research", there is requirement of paper work so as to seek written permission to access PHI. This process is known as "HIPAA Authorization."In this process the written consent is taken from every patient before releasing the information from that organisation to the outsider or use the patient's health data internally. In case the retrieval of data is impossible then a "waver of authorization" is requested from an IRB (Institutional Review Boards).

American Society lays more emphasis and values personal choice, individual rights in one's life. They understand that medical records contain the most intimate and sensitive details about the person's physical & mental health, personal and social relationships and financial status. So, many researches and surveys has been conducted which shows that medical privacy is major concern.

4.2 Data Security under Indian Scenario

According to the rules of Clinical Establishments (Registration and Regulation) Act 2010, notified on May23, 2012 is the "maintenance and provision of EMR or EHR for every patient for the registration and continuation of every clinical establishment". [14]

According to "Section 43(a) and section 72 of the Information Technology Act provide the broad framework for the protection of personal information in India". According to "Section 43(a) along with the sensitive personal information rules-lays down the compliances that need to be observed by an entity that collects or stores or otherwise deals with sensitive information such as financial information, passwords, health conditions, sexual orientations, medical records, and biometric records-mandates corporate to take reasonable procedures to protect sensitive personal data or information". According to Section 72 "protects personal information from unlawful disclosure in a branch of contrast". According to "Section 43 (a) a body corporate,

defined as a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".[14] As there are number of rules and regulations made by Indian Government but very few can afford these private healthcare system in which there is proper infrastructure for abiding these rules. If there are systems installed they are not strictly followed or controlled.

Recently The Ministry of Health and Family Welfare (MoHFW) has envisioned the framework which is in the form of a draft for governing EMRs in India *Electronic Health Records Standards*. This Draft points towards international physical, administrative and technical safeguards and standards for data protection of patient health records. According to the draft the purpose of the security standards is to:

- "ensure the confidentiality, integrity, and availability of all the e-PHI they create, transmit, receive, or maintain
- protect against reasonably anticipated threats or hazards to the security or integrity of their e-PHI
- protect against uses or disclosures of the e-PHI that are not required or permitted under the Privacy Standards
- Ensure their workforce will comply with their security policies and procedures". [1]

5 Results -

Understanding the differences between patient data safety standards between US and Indian Hospitals.

HIPAA, which is The Health Insurance Portability and Accountability Act has concrete framework and has set various guidelines and safeguards to protect patient data. In case of USA it is mandatory for any health organisation to hold HIPAA Compliance and they must have certain administrative, technical and physical safeguards in that hospitals or any other health related entity which is involved with handling patient data. If they don't do so number of laws and punishments are clearly mentioned that govern them. Without implementation of HIPAA rules, licenses would not be allotted by the government to build such organisation. There are factors that specify and consider the money penalty amount for violations in HIPAA. In order to fulfil the HIPAA requirements organisations need to ensure the four main necessities of the HIPAA law. According to HIPAA Compliance for Health Applications Checklist following are the four main requirements:

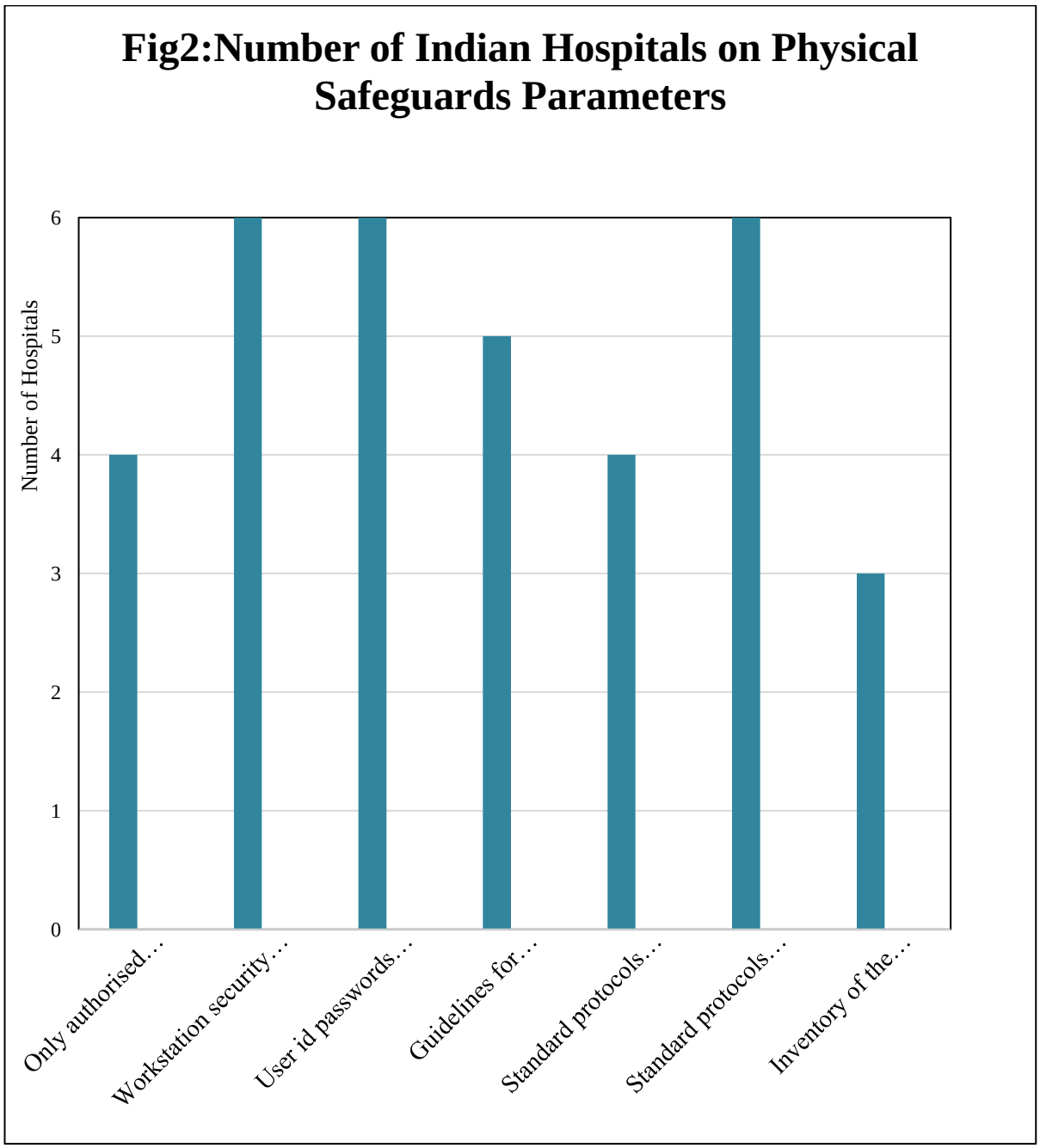
1) They must put safeguard in place to protect patient health information.
2) Limited use and sharing of protected of health information should be the minimum necessity to accomplish the requirements.
3) Organisations should have agreements in place with service providers that perform covered functions. These agreements are called Business Associate Agreements (BAAs) which ensures that service providers (Business Associates) should use, safeguard and disclose patient information properly.
4) Procedures must be there that specifies limits stating who can access patient health information and money penalties."

5.1 Analysis for Indian Hospitals-

Likewise a checklist was developed for analysing the Indian scenario of protecting patient's health data. There was only one checklist for every organisation's evaluation. The checklist has three main safeguards namely:

a) Physical Safeguards
b) Administrative Safeguards
c) Technical Safeguards

Under these safeguards there are assessment parameters based on which the type of safeguards adopted by the hospitals is evaluated and observations were noted.



5.1.1. Physical Safeguards-

There were in total seven assessment parameters under physical safeguards category. The following were the observations:

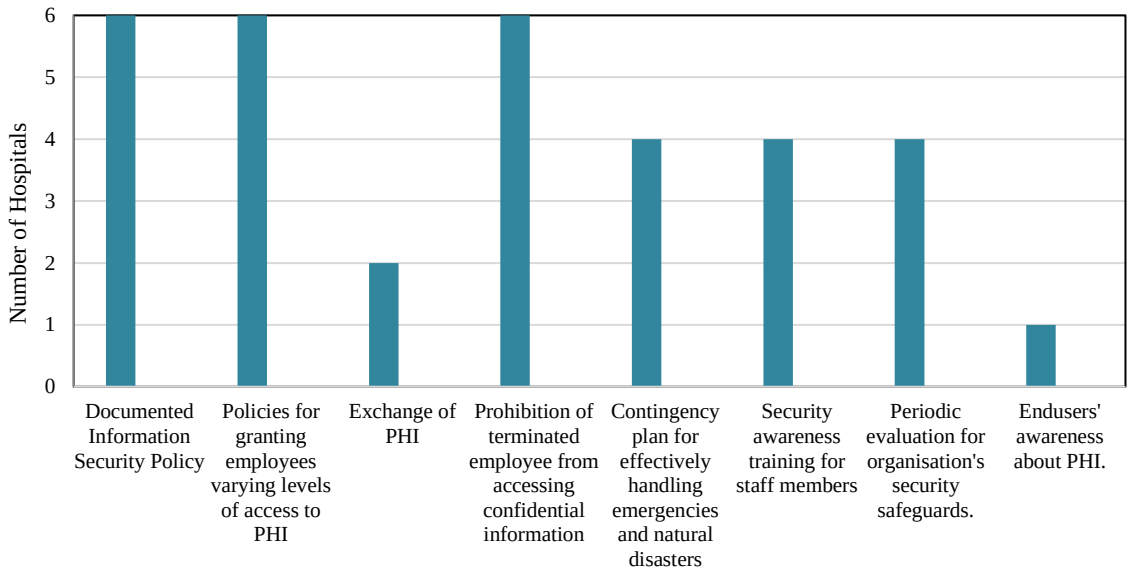
- Authorised Access to places where PHI is stored- Out of six hospitals surveyed, four hospitals were following the authorised access to places where patient's

protected health information is stored. The authorisation was generally for everyone in the hospital. Out of the six hospitals only two hospitals were not strictly following and there were no provisions for that as such.

- Workstation security including secured rooms, cabinets, and partitions- It was observed that all hospitals were following this kind of safeguard.
- User ID passwords for workstations on which PHI is stored- For accessing the patient health details, it was observed in all the hospitals individual user access logons were provided on every workstation. This user ID password is role based.
- Guidelines for workstations use procedure available for users- It was observed that there were proper documented guidelines available on each nursing station as well other administrative workstations too.
- Standard protocols for handling computer hardware and software, including proper disposal and storage- It was observed that four hospitals out of six had documented protocols for handling all the hardware of the computer systems. Basically, all the hardware and software handling should be done according to the rules, but it was not strictly followed rather two hospitals didn't had standards for that.
- Standard protocols for handling and disposal of paper records- It was found that five hospitals out of the six were having such protocols and the hospitals staff was also well versed with that.
- Inventory of the physical systems, devices and media used to store or contain ePHI- Almost equal responses were obtained for both yes and no, as three hospitals didn't have inventory for storing such devices and three were having storage provisions for physical systems, devices and media. It was observed that the inventories were found only in big hospitals who could afford such provisions.

5.1.2Administrative Safeguards-

Fig 3:Number of Indian Hospitals on Administrative safeguards Parameters



- Documented Information Security Policy- It was witnessed that all the hospitals surveyed had proper documented information for the security of patient data.
- Policies for granting employees varying levels of access to PHI- There were proper guidelines and policies to grant user access on role basis in the hospital.
- Exchange of PHI- Four of six hospitals was not exchanging patient personal health details and contact details with any other organisation or hospitals.
- Prohibition of terminated employee from accessing confidential information- It was found that all the hospitals which were surveyed had provisions for this parameter and they are following it too.
- Contingency plan for effectively handling emergencies and natural disasters- It was found that only two hospitals didn't had planning for such emergencies in terms of computerised PHI of the patient and other data related to departments of the hospitals.
- Security awareness training for staff members- Only four hospitals were found to have awareness for trainings conducted in the hospitals, that too was not periodical.
- Periodic evaluation for organisation's security safeguards-Only four hospitals were found to have

- End-users' awareness about PHI- In five hospitals it was found that the term PHI is not practised and were totally unaware about the concept. Only one hospital was known out of six was familiar with the concept.

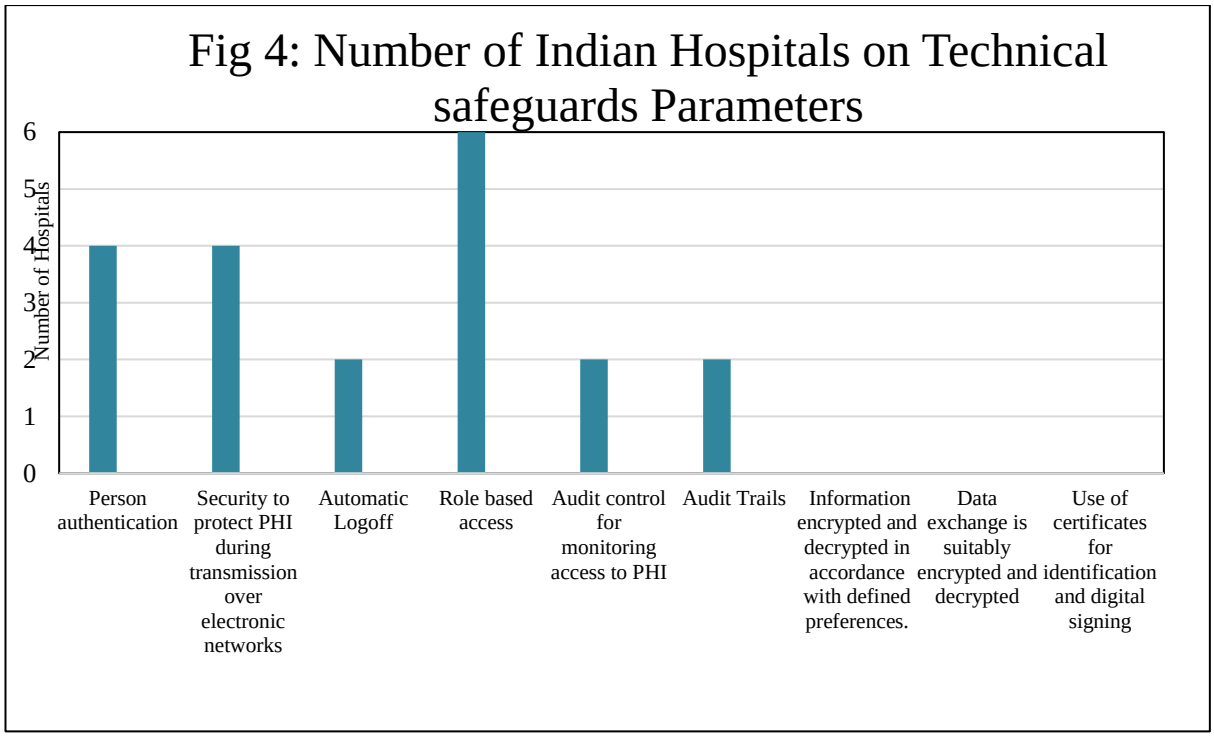
5.1.3Technical Safeguards–

Major observations were obtained which demonstrates the backwardness of Indian hospitals which are more inclined towards handling patient records physically not technically. Following were the observations:

a) Person authentication- Out of six hospitals only three hospitals were following the person authentication to ensure access to PHI
b) Security to protect PHI during transmission over electronic networks- Out of six hospitals it was found that there were security protocols for PHI during transmission over electronic networks. Only two hospitals were not practicing this.
c) Automatic Logoff-It was observed that automatic log provisions were not commonly used in the hospitals. Only in two hospitals it was found that automatic log off is actively working with the workflow of giving alerts in certain duration of time as per the HIS implemented in that particular hospital.
d) Role Based Access- Role based access is commonly practised in all the hospitals.
e) Audit Control for monitoring access to PHI- Differing trends are seen from this parameter. Only two hospitals had audit control or supervised by authoritative person to monitor the access to PHI. Rest of them were not aware so didn't practised.
f) Audit Trails- Audit trails here means that provision of verification of the entered data in to the HIS about alteration, deletion and modification of data. Some hospitals that are four of six were found that that they didn't followed audit trailing. And two out them were practising.
g) Information encrypted and decrypted in accordance with defined preferences- No such provisions are there for data encryption and decryption in any of the hospital.

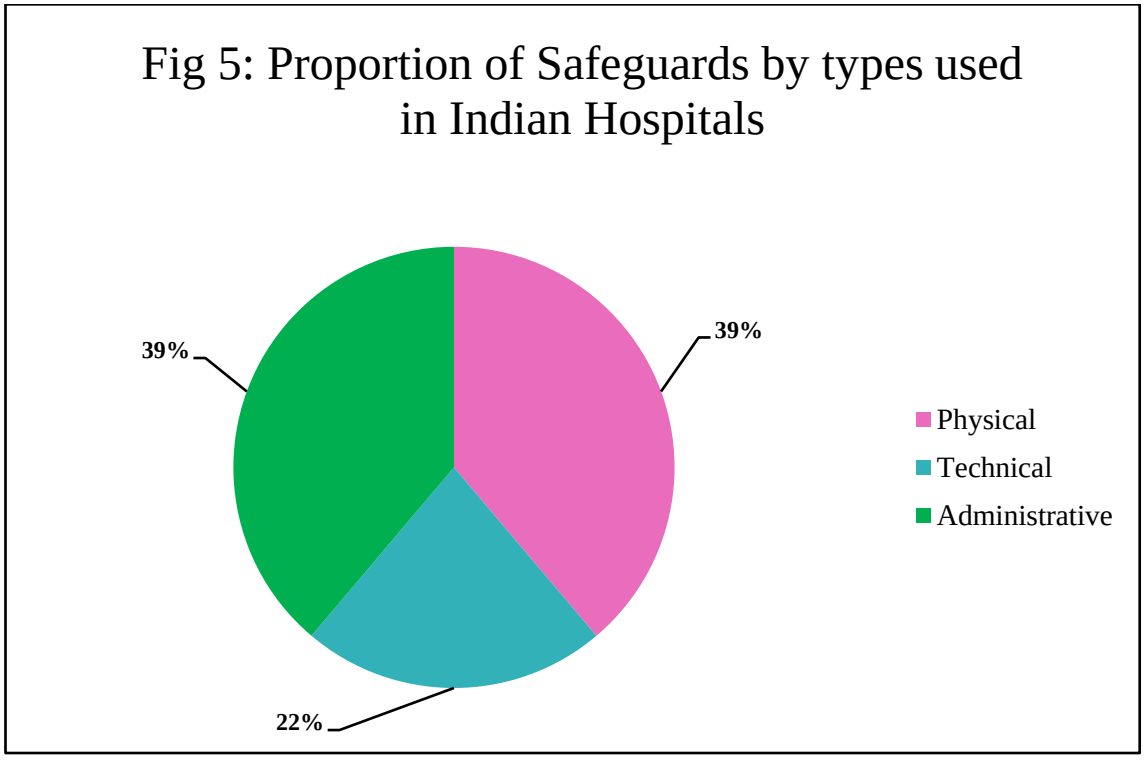
h) Data exchange is suitably encrypted and decrypted- This parameter was not followed and hospital was unaware about the parameter.

i) Use of certificates for identification and digital signing- Use of certification was not practised and concept was not known in any of the hospitals.



Therefore, it was found that in India physical safeguards are more popularly adopted. Administrative safeguards are also adopted equally with 39% adoption rate. Mainly these physical safeguards are considered more reliable as doctors and nurses still consider paper records are more comfortable and easy for data handling of patients. They are rather more reliant over paper records than HIS systems because they find data entry and order placements are easier to do in paper records. One more reason behind the problems in adopting technical safeguards is that not all hospitals can afford high quality security levels.

FIGURE 5 PROPORTION OF SAFEGUARDS BY TYPES USED IN INDIAN HOSPITALS



Indian state of privacy and security can be improved by implementing mandatory and strict rules to maintain patient data. More emphasis should be laid on technical safeguards for storage and maintenance of patient health information. Regular mandatory trainings should be conducted for all the staff members of the hospitals periodically. The process of security access and data transfer like reports, discharge summaries, orders placement in the systems should be streamlined and easy to understand. Indian hospitals are capable of adopting such measures but the sensitivity of

privacy, confidentiality and security are yet to realise among common masses as well within the hospitals staff. These all requirements can be fulfilled if the Indian governance should take charge by transforming rules and regulations into concrete legal framework where all the rules are made compulsory and mandatory for the hospitals.

Indian hospitals should take note from the best practices from developed countries with mature and strong governance systems which focus on implementing and analyzing the after effects of the same.

Understanding Indian hospital's perspective on application of data security standards.

The purpose of the questionnaire was to analyse the perception and awareness of hospitals staff towards patient data safety. Various questions were included in the questionnaire. The textual content derived was sorted according to distinct categories. Broadly, the analysis of the open ended questions was able to identify the perception level from the participation of the six hospitals and their respondents. The respondents were categorised as physicians, nurses, administrative staff and IT staff, which are relevant to evaluate the perception and knowledge level towards there hospital's functioning over patient health information security and confidentiality.

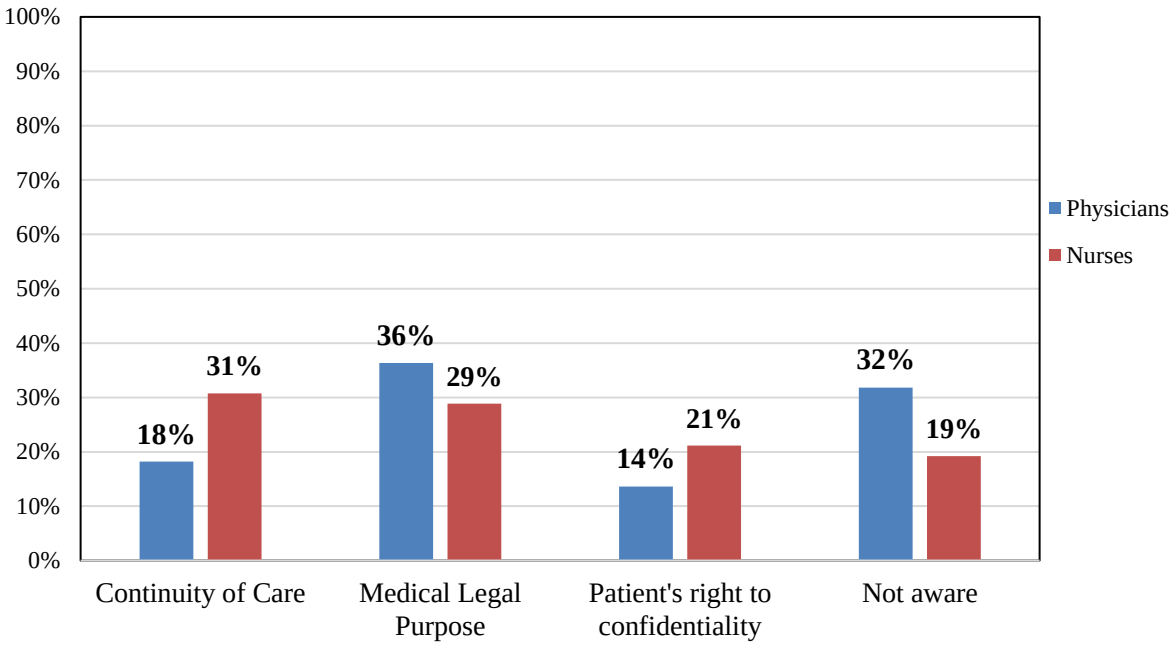
The survey involved broadly four types of the respondents namely physicians, nurses, administrative staff and IT staff. Out of them 21% were physicians, 50% were nurses, 18% were administrative staff, and 11% were IT staff. The numbers of respondents were interviewed according to the availability of the staff members.

5.2.1 PHI (Protected Health Information)**:**

First of all, on being asked if the respondents had ever heard about Protected Health Information (PHI), the responses were mostly negative as very few knew about the details of it. But on asking about what all is included in it, they were pretty much near to the details. One such response was that, the privacy rule defines PHI as individual identifiable health information. Majority of them said that protected health information is patient's basic health information that helps in identifying the patient and healthcare status of patient, payment related details, health advices, and discharge process.

5.2.2 Important to secure patient data

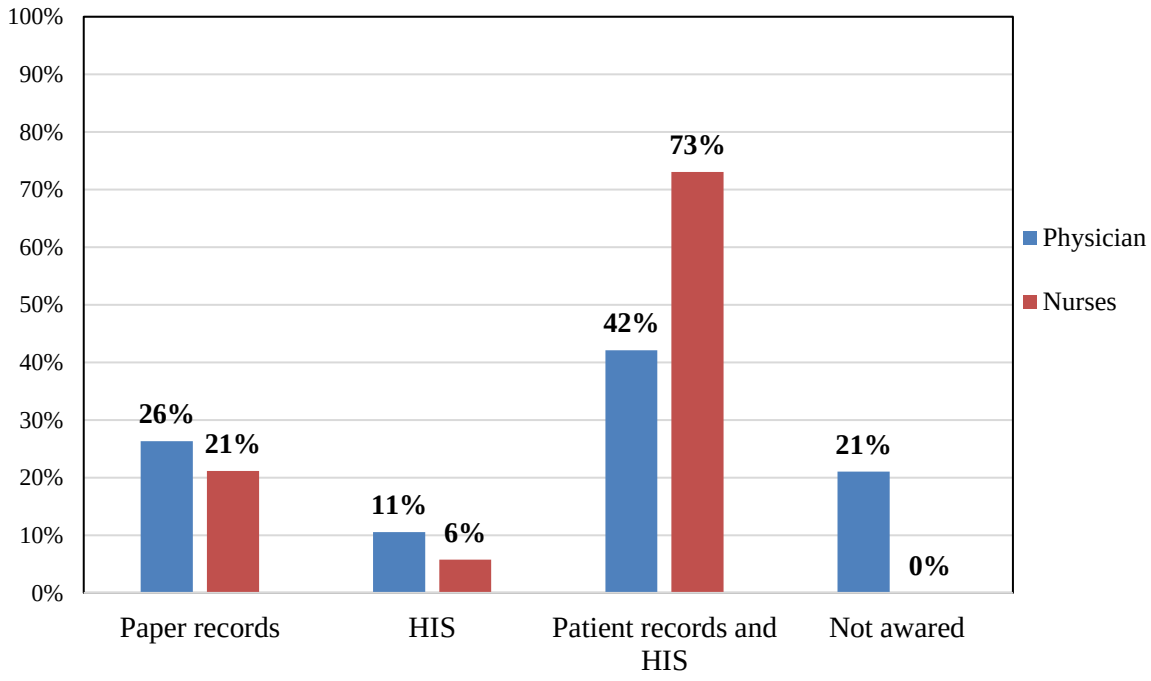
Fig 6: Percent distributions of the respondents by physicians and nurses towards importance to secure patient data



- So as to analyse among staff members about their perception towards importance to secure patient data, it was found that all the respondents considered the significance of protecting patient data. They categorised into following reasons for it.
- 36% of physicians and 29% of nurses considered patient data safety is important for medical legal purpose.
- 31% of nurses and 18% of physicians considered continuity of care as the important reason to protect patient records for future follow up.
- 14% of physicians and 12% of nurses considered patient right to confidentiality as important to secure patient data safety.

5.2.3Ways in data managed in hospital

Fig 7: Percent distributions of the responses by physicians and nurses on ways in which data is manage in hospitals

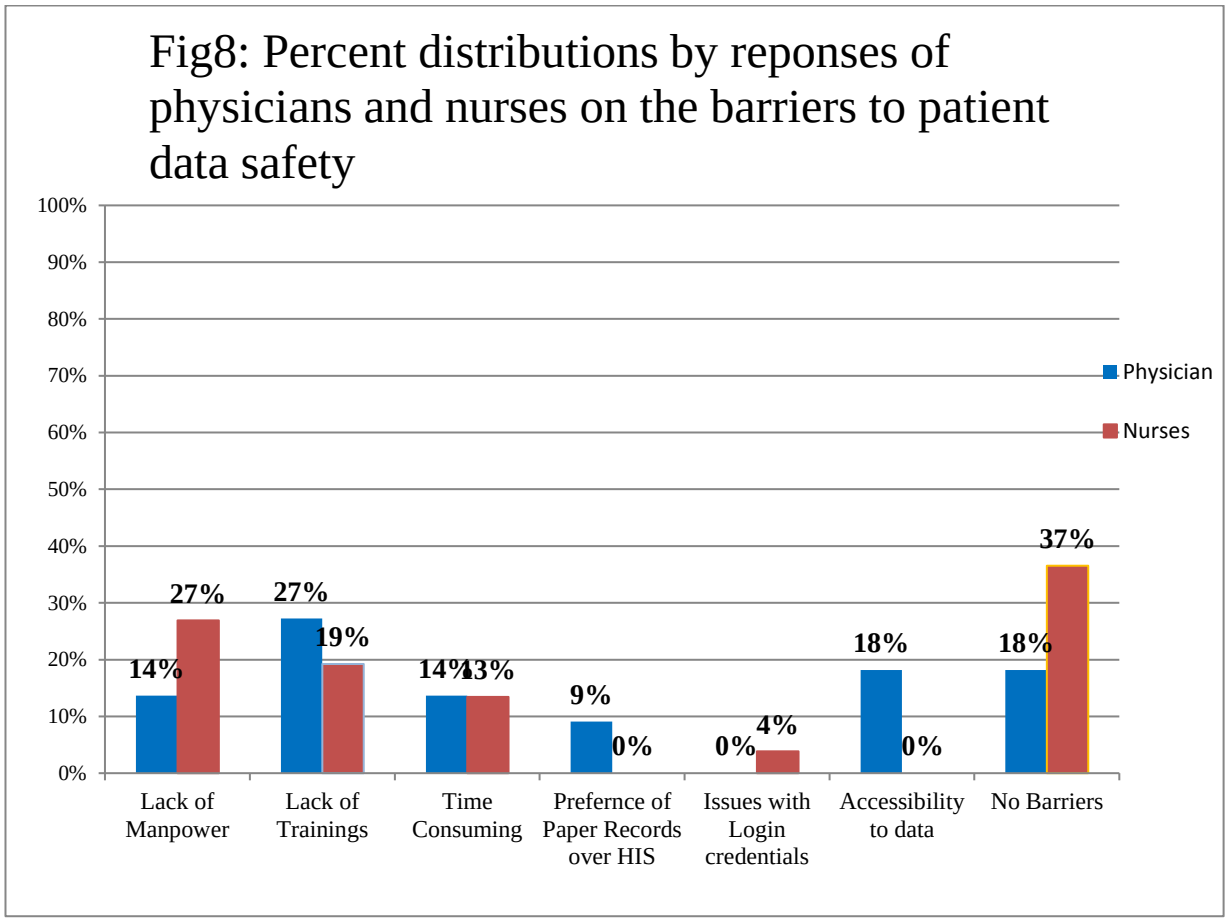


On the factor to analyse the perception of hospital staff about means to manage and store data in the hospital it was found that

- Maximum percentage of responses was for both patient records and health information system gaining 42% responses from physicians and 73% responses from nurses.
- 26% of physicians and 21% of nurses considered that patient data is well managed and easily handled in patient's paper records
- From the graph it is clear that nurses were fully aware about managing and storing patient records, but about 21% of physicians were not clearly aware about this.

5.2.4. Barriers and challenges to patient data security

For question about the challenges in treating patients while maintaining information security, both the physicians and nurses gave varied responses:

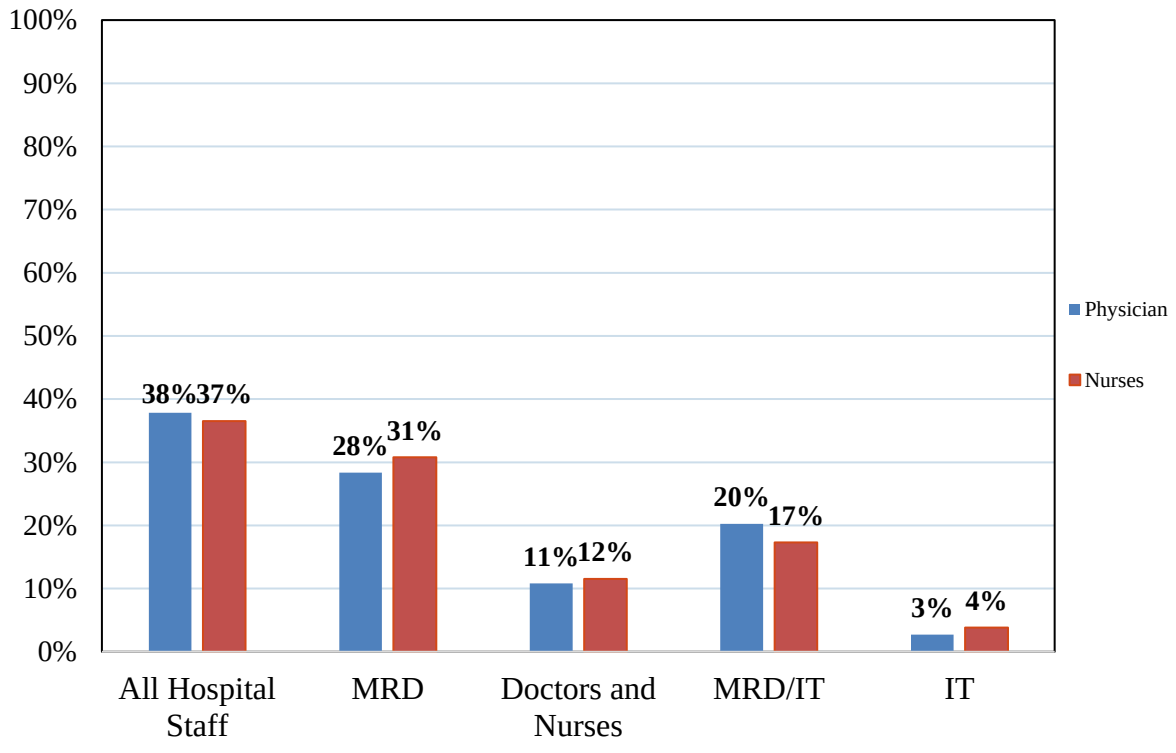


- The process of maintaining files and data entry is time consuming which is being compromised on patient care delivery as very less time is devoted to patients.
- Around 14% of the physicians and majorly 27% of the nurses respondents were considering lack of manpower in the hospital to deal with maintaining patient health records and there security.
- It has been observed from the interviews that lack of trainings among staff members is the cause of not being able to operate HIS and other patient security related tasks smoothly. Therefore, there periodic trainings were not conducted in the hospitals.
- Among number of responses of barriers, time consuming became one of them, as both physicians and nurses find entering, storing and maintaining health data is very time consuming.

- Over 9% of physicians preferred paper records over HIS, as Indian doctors are comfortable and find it easier to enter patient details whether in consent forms or discharge summaries. They rely more on physical records.
- Nurses often face problems with login credentials, as they are the one who are entering same patient data in paper as well as HIS of the hospitals. Many a times, the username or passwords are not accepted by the system or they forget to reset it after certain period of time as per hospitals policies. So they operate on their colleagues logins to access patient data.
- Often user access is restricted to the type of the user like nurses, doctors, administrative etc. So it is not easy to access previous health data or reports of the patient easily. This many a times hinder in patient care delivery process because security process is required to be followed.
- Around 37% of the physicians don’t consider any challenge.

5.2.5 Responsible for maintaining information security

Fig 9: Percent distributions on the responses by physicians and nurses on person responsibility to ensure patient data



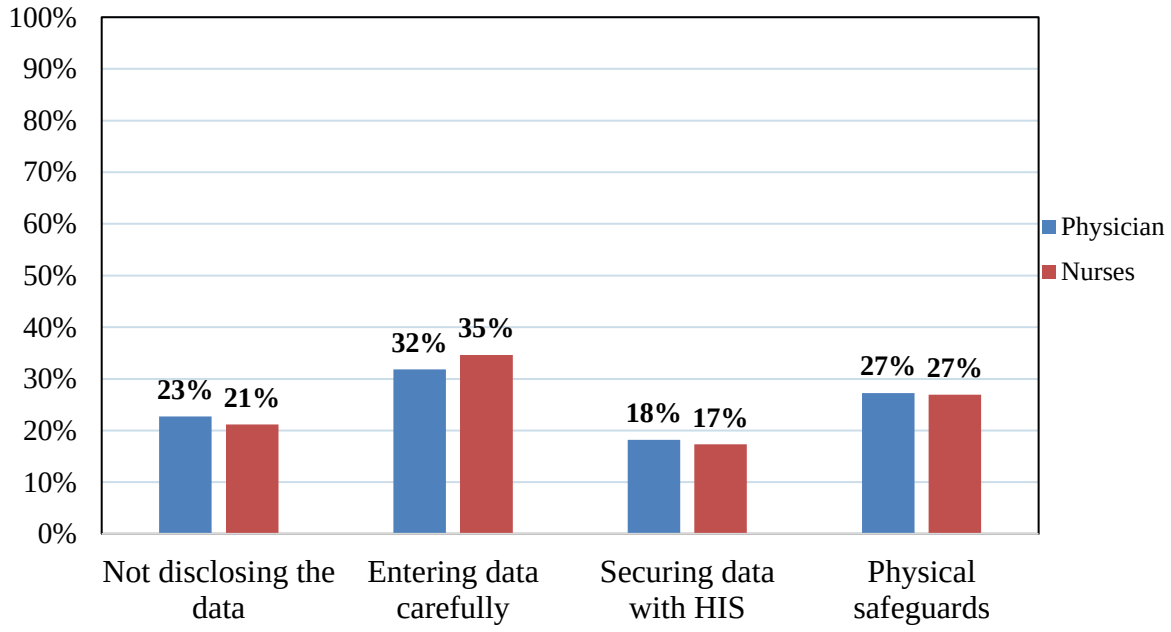
Varied responses were obtained on been asked about the responsibility in the hospital to maintain and ensure patient data safety.

- Physicians and nurses came up with different categories of responses. Major category aroused as it is the responsibility of all the staff members of the hospital according to physician's responses contributing to 38% and nurses to 37%.
- 28% of physicians and 31% of nurses think that it is the responsibility of the medical records department.
- Around 20% of physicians and 17% of nurses considered that it is the responsibility of both the medical records department and the IT department.
- 11% and 12% of physicians and nurses respectively considered that it is their own responsibility to ensure data safety.

- Very few physicians 3% and nurses 4% consider that only IT department of the hospital is responsible for maintaining information security.

5.2.6 Steps taken by physicians and nurses to ensure data safety

Fig 10: Percent distributions of responses for the steps adopted by physicians and nurses to ensure patient data



- One of the questions was to evaluate the perception of the physicians and nurses about the steps taken by them to ensure patient data privacy and safety.
- About 23% of physicians and 21% of nurses believes not disclosing the patient details to others.
- Almost equal responses were obtained from nurses and doctors about carefully entering data into the patient paper records and health information systems.
- About 18% of the physicians and 17% of the total respondents find securing data in HIS is the only way to ensure patient data safety.
- By securing patient data in paper records is the way to ensure patient data safety in the hospital.

5.2.7. Improving Information Security**:**

According to the respondents on the question about the scope of improvement in maintaining information security in the hospital, some responded that

- Limited access should be given to specific staff, because practically it is not being practised.
- Scope is high but it needs more manpower and skills to carry forward. More knowledge and awareness about importance of information security should be practiced.
- More reliance should be on HIS as compared to paper records.
- There should be more organised usage of computers in documenting patient data with utmost privacy and security.
- Some were in favour of the existing process and recommended that maintaining data through such procedures should be made easy and less time consuming.
- More people should be assigned to check this process

5.2.8 Following safeguards adopted by hospital-

There was multiple category selection from the same respondent. Varied responses were obtained when asked about the adoption rates on data security measures, which has five sub categories namely:

a) Username and Password Protected Workstations- For the first category that is username and password protected workstation around 80% of the respondents from hospital A and E were known and were aware about usage of this safeguard being adopted in the hospital. For the hospitals B, C, D and F everybody was aware and practicing this kind of safeguard in their respective hospitals.
b) Standard guidelines for storage of Medical records- In hospitals B, C and D everyone from the hospital staff were adopting and were pretty much aware about the guidelines and protocols of medical records department's storage and securing policies for paper records particularly. Only hospital A and E showed low awareness level towards the standards being followed for storage of medical records department.
c) Controlled Access for users to data sensitive locations- Very few hospitals in India adopt technical safeguards for securing patient data and so it is visible in the adoption trends as only two hospitals out of six adopted higher level of security for sensitive data locations. Maximum staff responses were very low on the subject of adoption and awareness of such safeguard being used in hospitals.
d) Locked cabinets and storage lockers- Maximum hospitals responses were mostly using storage lockers for storing patient records. It was found that record files of the patient were kept in open cabinets of the nursing stations of the floors. Only two hospitals showed truly positive responses towards proper usage of this type of storage. Rather respondents were only considering the lockers systems to be confined to medical records department where files are sent after discharge of the patient.
e) Periodic supervision and auditing of stored patient files- In this category of safeguard; it was observed that respondents were not aware of the auditing and supervision of stored files being practised by the hospitals. Only administrative and IT staff were well versed by the procedure. They too responded the

existence of very less strict rules for checking and supervising of the records. Only three hospitals out of six, that too only for hospitals A and C were on 80% in favour of the safeguards and 75% for hospital C considered the importance and awareness about auditing of patient records and the rest were very low on call by 57% for hospital E, 40 % for C and 20% for B.

5.2.9 Guidelines or training programs for end users awareness and for information security

The highest numbers of descriptive answers were found from the question about the guidelines or training programs for end users awareness and for information security. This question was for administrative and IT staff members who were known about the trainings being conducted according to the protocols and norms of the hospital.

- The trainings were not conducted periodically.
- Moreover, when asking about the questions they were just mentioning the protocols.
- Basically the trainings were conducted whenever new staff is appointed so as to handle the procedure.
- Although in some hospitals it was observed that for IT and administrative staff, proper trainings sessions were scheduled. But in case for nurses and doctors, very few hospitals conducted trainings for them, and not on periodic basis.

5.2.10Policies in the event of equipment failure, theft, and site disaster with respect to patient data

In question about knowing the policies about securing patient data in the event of equipment failure, theft, and disaster,

- It was observed that periodic data backup in separate servers considered more frequently answered among all the responses.
- Data backup is considered one of the most reliable ways to store and secure patient data. Scanned copies of the paper records are also stored in soft copies and can be the effective way of handling data in case of any site disaster.
- Not only backup is the option for data security in such cases but responses were also for storage of paper records in medical records department, in which after certain period of defined time frame the paper records are kept in different

warehouse or store room so as to store files along with the hospital's information system.

5.2.11Disciplinary processes for employees who have violated your security policies and procedures

- Some responses were about the warnings generation against the particular employee, who has violated the policies. In this procedure first of all human resources department along with IT department sends a warning letter to that employee. In this process signature is derived from that employee in the presence of HR and IT staff on the consent letter and in written format about explaining the recursions of breaking the rules are specified. But very few were known about this fact.
- Rather they were just responding that punishment against violation is the decision of top or senior level management.
- Some were not known about the policies and procedures which are documented.

5.2.12 Technical safeguards

- Data backup is performed periodically daily, monthly and yearly depending upon the policies of the hospital.
- Proper user based access is practiced.
- Individual user access is provided to all staff. Username and passwords are generated and patient data is entered into concerned modules of the patient.
- Paper records are maintained and stored in medical records department. Coding of the diagnosis is not done; rather scanning of the whole patient file is carried out. User access is granted to every user and is enlisted in separate groups. They are not allowed to be shared. IT staff takes backup of data periodically in servers.
- Responses were also on data entry in paper and HIS with utmost care will ensure there technical safeguards.
- Some also responded that data access is given and is restricted by authentication. Network is secured through firewall

5.2.13Guidelines to destroy redundant data

- Responses were often framed in context to medical records department's role that there are certain procedures for destroying paper records in medical records department. For IPD, OPD files are dumped after certain span of time. MLC cases file are kept for lifelong.
- Some also responded with more clarity about this, that there are proper guidelines for destroying data within particular period of time. They were aware but MRD in medico-legal cases which are kept for lifetime, OP/IP files are kept for 5 years and PACS data are kept for minimum 5 years.
- Maximum responded that not a single data in the hospital is destroyed.

5.2.14 Workflow for password management

It was seen that maximum IT and administrative staff respondents were able to answer about the actual process.

According to them username and passwords are made by the permission given by HR department and then IT department comes into role. Users need to access from IT departments granted passwords and after that they need to change according to their ease. For new hirers, new username & password are allotted. After that they need to change their passwords once they first login. The password will get expire within 60 days if not used; we need to unlock and then reset the password. Some responses were also there who were not known about the process and told that it is the responsibility of IT and HR department.

5.2.15Measures to control user's access to patient specific data

In case of question related to the measures to control user's access to patient data specific data respondents were much clear about the role of username and password for accessing into the systems.

- There are provisions for separate user access for front desk users like reception and administrative staff. Each and every department has security groups for nurses, doctors, and administrative as well as IT staff. The user access is well defined on role based. This is done with the approval of the head of that department and HR department through mail exchange of mails.

- Some also considered the task responsibility is on IT department only. IT department has access to all kind of patient related information or any other department.

5.2.16 Health information exchange happening in the hospital

For question on whether the information exchange is happening in the hospital, respondents knew that not a single data is being sent and received from any other organisation. Data exchange is functional within the same branches of the hospital.

6Limitations of the study

The study included both observational and interviewing methods to conduct the study. During the procedure there was limitation of the time frame that allowed only six hospitals of Bangalore to survey. Most of the clinical staff was not available to answer the questions in detailed manner because of lack of knowledge and interest in the subject. Therefore some responses were prone to biasness. There was also resistance from the hospitals to respond to certain aspects of data security issues due to lack of understanding on the subject and considering privacy breach of hospital's sensitive data.

7 Conclusion

To maintain intimate and trustworthy interactions, confidentiality and privacy are very essential for the foundation of doctor-patient relationships. Healthcare is extremely information sensitive and intensive industry. Breaching of large scale patient health data is a genuine threat because such kind of information is in excessive demand especially in research sector and various pharmaceutical industries. As medical privacy involves vigorous data workflows it also comes up with problems of illegal use, breaches and violations.

US healthcare is very well equipped with strict rules of security, privacy and confidentiality under HIPAA laws. So as to understand the differences between US and Indian hospitals scenario, it was observed that for US healthcare there are successful adoption rates of administrative, physical and technical safeguards. It was found that there were special provisions in the case of any violations or mishandling of patient data .Whereas in case of Indian hospitals there are significant technical, administrative, and physical safeguards in Indian hospitals to secure patient data in India as well. It was found that adequate security according to the type of safeguards were not adopted as per mentioned by the rules. This is due to lack of concrete framework mandating rules to be implemented and lack of awareness about the same. Privacy confidentiality and security of health information are constitutional rights, but the sensitivity of such rules are not realised in Indian legal framework. So the scene in Indian scenario is somehow different. So as to know the perception level of the hospital staff about the rules and procedures being applied in their respective hospital it was found that there are no such terms and concepts related to the patient data security, commonly used and adopted in Indian hospitals. There are number of challenges for such safeguards implementation like lack of manpower, and lack of trainings in the hospitals for it. Also there is lack of active legal framework and there are no laws in India mandating hospitals to disclose security breaches. Although hospitals are moving towards adopting HIS but they are still reluctant on giving up on paper based records which creates a double burden of maintaining data. Other shortcomings include unauthorized audit trailing of health information, lack of dedicated manpower for HIS, low focus on training the staff.

8 References

1) Ministry of Health and Family Welfare. “Data Privacy and Security”.National Health Portal:NHP CC DC; [cited 2015 Jun 03]. Available from:http://nhp.gov.in/data-privacy-and-security_mtl
2) Ojha Srishti and Rahul Mishra. “India: Data Privacy Laws – A Compliance-Centric Analysis”.2016.Available from: http://www.mondaq.com/india/x/498170/Data+Protection+Privacy/DATA+PRIVACY+LAWS+A+COMPLIANCECENTRIC+ANALYSIS
3) ISO/DIS 17090-5(en)., Public Key infrastructure-Part 5: Authentication using Healthcare PKI credentials; 2015. Available from: https://www.iso.org/obp/ui/#iso:std:iso:17090:-5:dis:ed-1:v1:en
4) Nass SJ, Levit LA, Gostin LO,editors, “The Value and importance of Health Information Privacy”, Washington(DC): National Academis Press (US); 2009. Available from:https://www.ncbi.nlm.nih.gov/books/NBK9579/
5) Prater S. Valerie. “Confidentiality, Privacy and Security of Health Information: Balancing Interests”.2014.Available from: http://healthinformatics.uic.edu/resources/articles/confidentiality-privacy-and-security-of-health-information-balancing-interests/
6) Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS Quarterly, 33(2), 339-370.
7) Valerie S. Prater, MBA, RHIA, Clinical Assistant Professor, December 8, 2014. Confidentiality, privacy and security of health information: Balancing interests
8) AHIMA (American Health Information Management Association) The state of HIPAA privacy and security compliance. 2006.
9) Nass SJ, Levit LA, Gostin LO, (2009) Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Washington (DC): National Academies Press (US)
10) Ajit Appari and M.Eric Johnson; 2008 Aug, “Information Security and Privacy in Healthcare: Current State of Research”, Center for Digital Strategies, Institute for Security Technology Studies at Dartmouth College, Hanover NH. Available from-

https://pdfs.semanticscholar.org/5480/27201bed4a7f0a0f9f811357b6f7947a5bed.pdf

11) Wang Jason. "How Do I Become HIPPA Compliant? (A Checklist)".2013.Available from: https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html

12) Korgaonkar Basra Ranjeeta. "Adoption of Information System by Indian Hospitals; Challenges and Roadmap.2014.volume 5.Available from: http://www.ijser.org/paper/Adoption-of-Information-System-by-Indian-Hospitals.html

13) Rezaeibagha Fatemeh, Win Than Khin, Susilo Willy. "A Systematic Literature Review on Security and Privacy of Electronic Health Records Systems: Technical Perspectives".2015. Availablefrom:http://journals.sagepub.com/doi/abs/10.1177/1833358315044003 04?journalCode=himd

14) Nahra Kirk. "A Privacy and Data Security Checklist for All".2015.Available from: http://www.wileyrein.com/media/publication/129_A%20Privacy%20and%20Data%20Security%20Checklist%20for%20All.pdf

15) Deo Akhil. "Without Data Security and Privacy Laws, Medical Records in India Are Highly Vulnerable".2017.Available from: https://thewire.in/102349/without-data-security-and-privacy-laws-medical-records-in-india-are-highly-vulnerable/

16) Kumar Ankush. "India Needs Regulatory Standards on Privacy and Security of Health Records: Arvind Sivaramakrishna, CIO, Apollo Hospitals Group".2016.Available from: http://computer.expressbpd.com/news/india-needs-regulatory-standards-on-privacy-and-security-of-health-records/17281/

17) Mani Tanvi. "Privacy in Healthcare: Policy Guide".2014.Available from: http://cis-india.org/internet-governance/blog/privacy-in-healthcare-policy-guide

18) Ghosh Abantika. "In a First, Health Department Plans Privacy Law to Guard Patients Data".2016.Available from: http://indianexpress.com/article/india/india-news-india/in-a-first-health-department-plans-privacy-law-to-guard-patients-data-3060711/

19) Rich Cynthia. "Privacy Laws in Africa and the Middle East".2015.Available from: https://media2.mofo.com/documents/150615bloombergprivacyafricamiddleeast.pdf

20) Greene H. Adam, Williams L. Rebecca, Thompson Bryan. "HIPPA Enforcement Actions BY Numbers".2016.Available from: http://www.privsecblog.com/2016/06/articles/healthcare/hipaa-enforcement-actions-by-the-numbers/

21) Bourke Julius. "Confidentiality".2008.Available from: http://www.bmj.com/content/336/7649/888

22) Greenhalgh Trisha. "Introduction of Shared Electronic Records: Multi-site Case Study Using Diffusion of Innovation Theory".2008.Available from: http://www.bmj.com/content/337/bmj.a1786\

23) Mandi D Kenneth, Szolovits Peter, Kohane S Isaac. "Public Standards and Patients Control: How to Keep Electronic Medical Records Accessible but Private".2001.Available from: "http://www.bmj.com/content/322/7281/283

24) Limb Matthew. "Accuracy of Patients Records may be Bigger Issue Than Security Breaches".2014.Available from: http://www.bmj.com/content/348/bmj.g2598

25) Wilkowska Wictoria, Ziefle Martina. "Privacy and Data Security in E-Health: Requirements from the Users Perspective".2012.Available from: https://pdfs.semanticscholar.org/b888/43af4b849d1f2db8095e1264cc51696e6058.pdf

9 Annexure

Annexure 1:Checklist for Indian Hospitals

CHECKLIST FOR INDIAN HEALTHCARE FACILITIES			
Areas	Assessment Parameters	Yes/No/ Not sure/NA	Observation/Remarks
Administrative Safeguards	Documented Information Security Policy		
	Policies for granting employees varying levels of access to PHI		
	Exchange of PHI		
	Prohibition of terminated employee from accessing confidential information		
	Contingency plan for effectively handling emergencies and natural disasters		
	Security awareness training for staff members		
	Periodic evaluation for organisation's security safeguards.		
	Endusers' awareness about PHI.		
Physical Safeguards	Only authorised access to places where PHI is stored.		
	Workstation security that includes secured rooms, cabinets, partitions.		
	User id passwords for workstations on which PHI is stored.		
	Guidelines for workstation use procedures available for users		
	Standard protocols for handling computer hardware & software, including proper disposal and storage		
	Standard protocols for handling and disposal of paper records		
	Inventory of the physical systems, devices, and media that are used to store or contain ePHI?		
Technical safeguards	Person authentication to ensure only authorized access to PHI		
	Security to protect PHI during transmission over electronic networks		
	Automatic Logoff		
	Role based access for different care providers		
	Audit control for monitoring access to PHI		
	INTEGRITY- Verification of Modifed data information in accordance with the standard		
	Is information encrypted and decrypted in accordance with defined preferences.		
	Data exchange is suitably encrypted and decrypted		
	Use of certificates for identification and digital signing		

Annexure 2: Questionnaire for Clinical Staff

GENERAL QUESTIONNAIRE

HOSPITAL PERSPECTIVE ON PATIENT DATA SAFETY STANDARDS

(The data collected and the identity of the respondents will be kept confidential and will be used for the purpose of this study only. Only the researcher will have access to the data.)

NAME OF ORGANISATION-	DEPARTMENT-
NAME OF RESPONDENT-	AGE-
DESIGNATION-	

I am a student of IIHMR, Jaipur. The topic of my project**"**A comparative Study of patient safety considering security and privacy standards between Indian hospitals with its guidelines and U.S healthcare facilities with HIPAA compliance". The objective of this study is to understand the perspective, knowledge among hospital's doctors and nurses about patient data safety and privacy standards and to what extent they are being followed.

1) Have you heard of Protected Health Information?
   YES ☐ NO ☐
2) What all is included in Protected Health Information?
   _____
   _____
3) Do you think that it is important to secure patient data in your hospital setting? If yes, Why?
   _____
   _____
4) In what ways is the data is managed (stored) in your hospital?
   _____
   _____
5) What according to you are the barriers and challenges to patient data security

6) Are there any challenges in treating patients while maintaining information security? If yes please elaborate.

7) Who all are responsible for maintaining information security in your hospital?

8) What are the different steps taken by you to ensure data safety and privacy?

9) According to you what is the scope of improvement in maintaining information security in your hospital?

Annexure 3: Questionnaire for Administrative and IT Staff

QUESTIONNAIRE

HOSPITAL PERSPECTIVE ON PATIENT DATA SAFETY STANDARDS

(The data collected and the identity of the respondents will be kept confidential and will be used for the purpose of this study only. Only the researcher will have access to the data.)

NAME OF ORGANISATION-	DEPARTMENT-
NAME OF RESPONDENT-	AGE-
DESIGNATION-	

I am a student of IIHMR, Jaipur. The topic of my project**"**A comparative Study of patient safety considering security and privacy standards between Indian hospitals with its guidelines and U.S healthcare facilities with HIPAA compliance". The objective of this study is to understand the perspective, knowledge among hospital's administrative and I.T staff about patient data safety and privacy standards and to what extent they are being followed.

10) Have you heard of Protected Health Information?

YES ☐ NO ☐

11) What all is included in Protected Health Information?

_____

_____

12) Which of the following safeguards are adopted by your hospital:

a. Username & Password Protected workstations ☐
b. Standard guidelines for storage of Medical Records ☐
c. Controlled Access for users to data sensitive locations ☐
d. Locked Cabinets and storage lockers ☐
e. Periodic supervision and auditing of stored patient files ☐

13) What are the challenges in implementing patient data security measures in your hospital?

14) Are there any guidelines or training programs for end users awareness and for information security?

15) What are your policies in the event of equipment failure, theft, and site disaster with respect to patient data?

16) What are your hospital's disciplinary processes for employees who have violated your security policies and procedures?

17) What are the technical safeguards to secure patient data in your hospital?

18) What are the various guidelines to destroy redundant data?

19) What is the general workflow for password management? Please elaborate on password resetting and expiry system.

20) What are the measures to control user's access to patient specific data?

21) Is there any health information exchange happening in the hospital. If yes please elaborate on the security measures in place?

_____

_____