
A COMPARATIVE STUDY OF PATIENT DATA SAFETY CONSIDERING SECURITY AND PRIVACY STANDARDS BETWEEN INDIAN AND U.S. HOSPITALS

Presented by- Aditi Mathur

IIHMR, Jaipur



Introduction

- Privacy and Security Standards for patient data are interlinked.
 - Any health records system requires safeguards to ensure that the data is available when needed.
 - The information should not be used, disclosed, accessed, altered or deleted inappropriately while being stored or retrieved or transmitted.
 - The Security Standards work together with the Privacy Standards to establish appropriate controls and protections.
- 

Privacy

- The collection, storage, and use of personal information and analysing the authorised use of the patient's personal health information.

Confidentiality

- It addresses the issue of how to keep information exchanged in intimate relationship from not being disclosed to third parties.

Security

- Keeping health records safe from unauthorized use of health information by following procedural and technical measures.

Source- Nass SJ, Levit LA, Gostin LO, editors, "The Value and importance of Health Information Privacy", Washington(DC): National Academis Press (US); 2009

Rationale

- Privacy and security key to any patient health information system.
 - Lots of data and evidence already exists on data security standards in the US health care.
 - Limited data and Research on the issue
- 

Objectives

- To understand the differences between patient data safety standards between U.S and Indian hospitals.
 - To study Indian hospitals' perspective on application of data security standards.
 - To study the scope for implementing Health Insurance Portability and Accountability guidelines in Indian hospitals.
- 

Literature Review



- Health Insurance Portability and Accountability Act (HIPAA) was enacted on 21 August, 1996.
- The main agenda of this Act was to help reconstruct the health insurance sector 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 standards.

Source- Nass SJ, Levit LA, Gostin LO, "The Value and Importance of Health Information Privacy": The HIPAA Privacy Rules. 2009

Literature Review



- The Ministry of Health and Family Welfare (MoHFW) has envisioned the framework governing *Electronic Health Records Standards* in India.
- 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 confidentiality, integrity of e-PHI, to protect against threats, and disclosure and to ensure workforce to comply with security policies and procedures.
- There are number of rules and regulations like Clinical Establishments (Resgistration and Regulation) Act, made by Indian Government but very few can afford these private healthcare.

Source- 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

Methodology

- **Study Design-** Descriptive and Cross Sectional study
- **Study Duration** - Three months (February to April 2017)
- **Study Population-** Physicians (22), nurses (52), administrative staff (19) and IT staff (12) of the hospitals in Bangalore
- **Sampling Technique-** Convenient sampling
- **Number of Hospitals Surveyed** – 6 considering single, super and multispecialty hospitals as according to their availability and accessibility.

Methodology

- **Data Source and Data Collection Tool-**

- Journals, online articles and reports were reviewed for secondary data.
- Primary data was collected through semi-structured questionnaire and checklist.
- For analysis on Indian scenario, a checklist was developed which was divided into assessment parameters as under:
 - Physical Safeguards
 - Administrative Safeguards
 - Technical Safeguards

- **Data 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.

To understand the differences between patient data
safety standards between U.S and Indian hospitals



Findings

HIPAA Security Rule contains the standards that must be applied to safeguard and protect protected health information (PHI). There are three parts to the rules-

- Physical Safeguards
- Administrative Safeguards
- Technical Safeguards

There are number of segments within each of the applied rule which are mandatory to be achieved for establishment of hospitals in the US.

Safeguards in Indian Hospitals

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 organization's security safeguards
- Endusers' awareness about PHI

Physical Safeguards

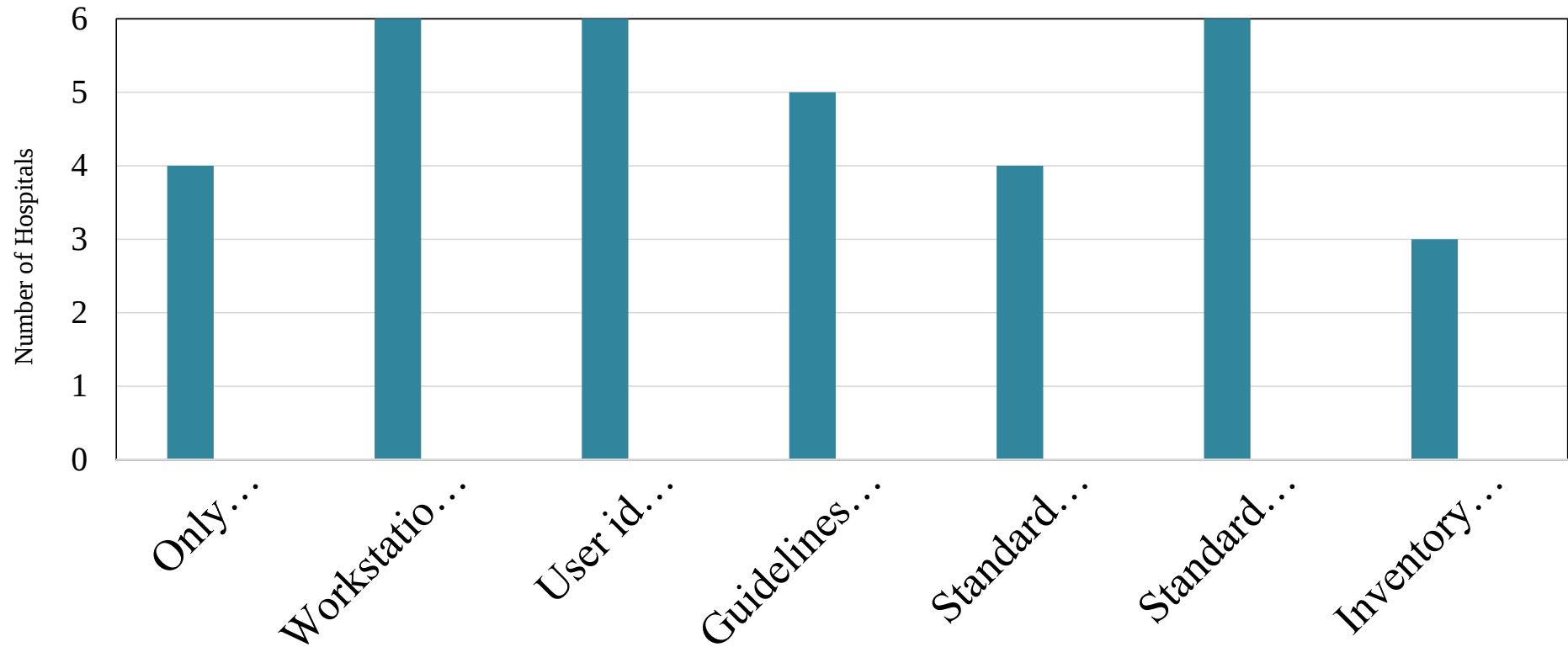
- Only authorized access to places where PHI is stored
- Workstation security that includes secured rooms, cabinets, partitions
- User id passwords for workstations on which PHI is stored
- Guidelines for workstations use procedures available for users
- Standard protocols for handling computer hardware & software, including proper disposal and storage
- Standard protocols for handling and disposal for paper records
- Inventory of the physical systems, devices, and media that are used to store or contain ePHI

Contd....

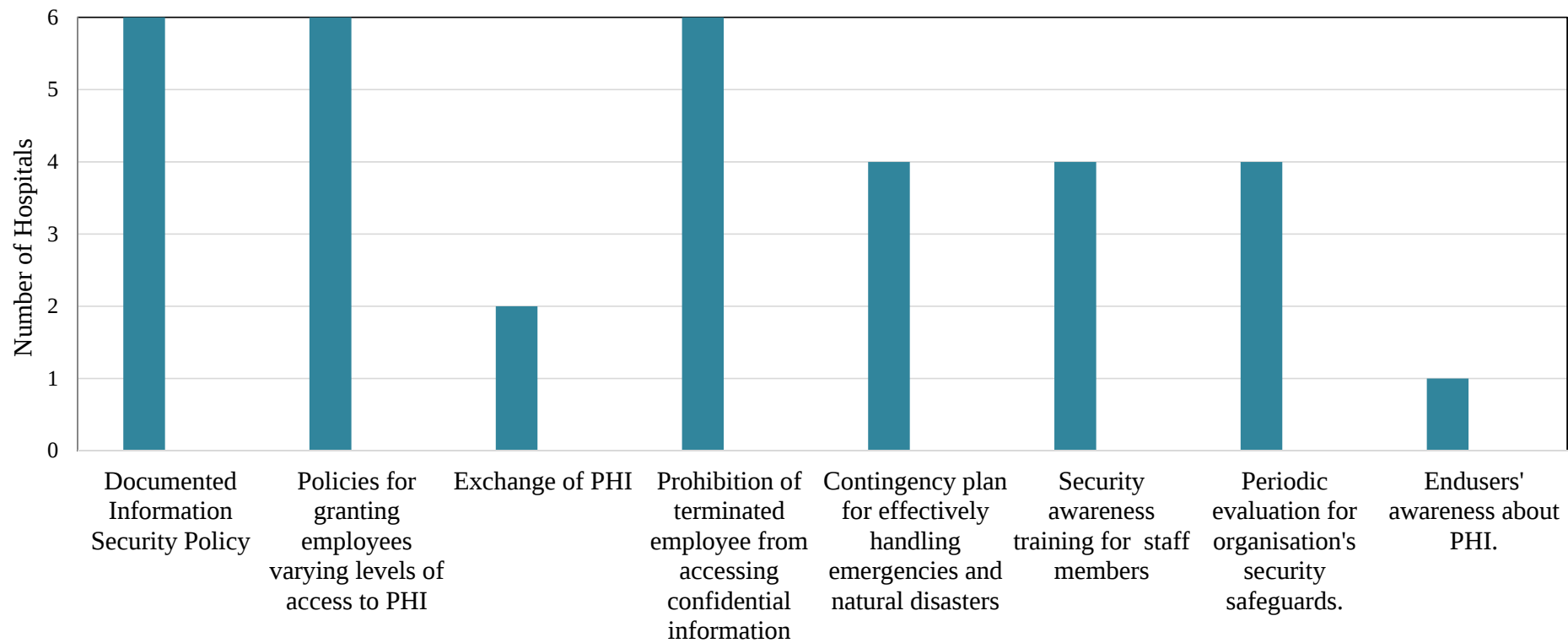
Technical Safeguards

- Person authentication
 - Security to protect PHI during transmission over electronic networks
 - Automatic Logoff
 - Role based access
 - Audit control for monitoring access to PHI
 - Audit trails
 - Information encrypted and decrypted in accordance with defined preferences.
 - Data exchange is suitably encrypted and decrypted
 - Use of certificates for identification and digital signing
- 

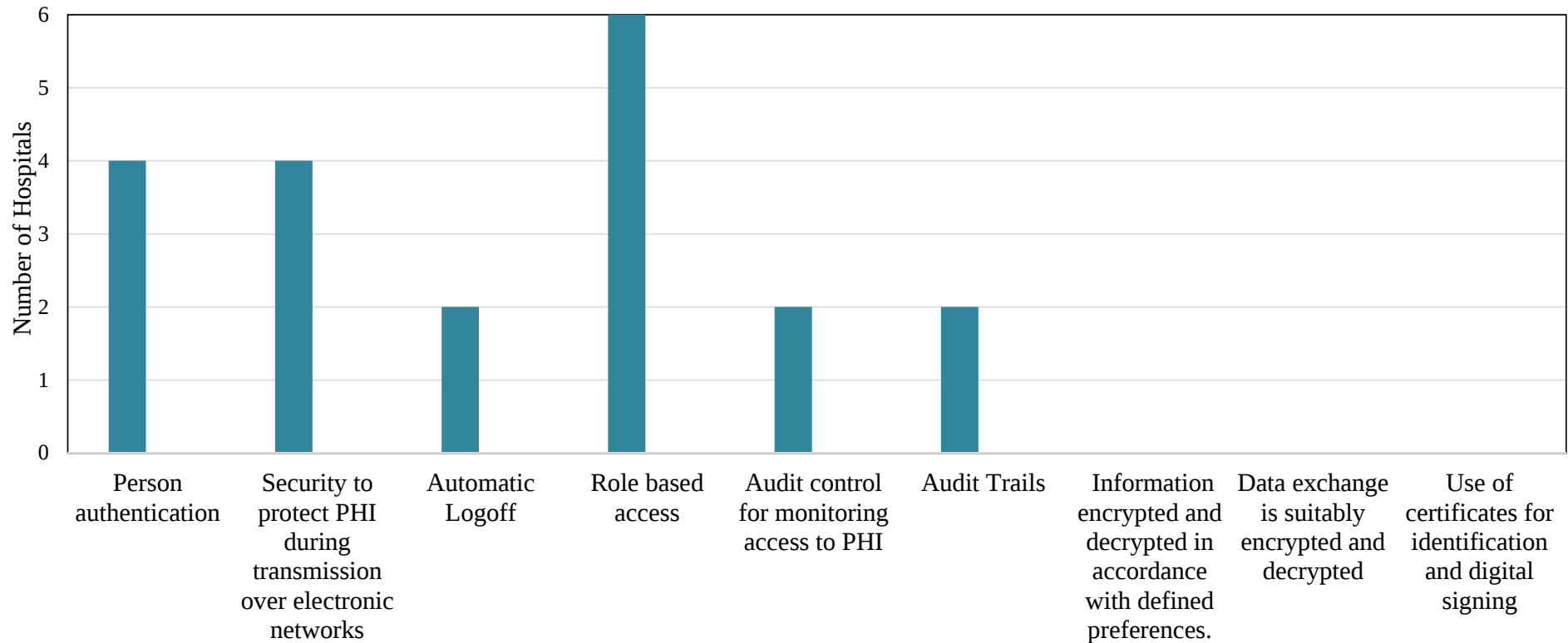
Number of Indian Hospitals on Physical Safeguards Parameters



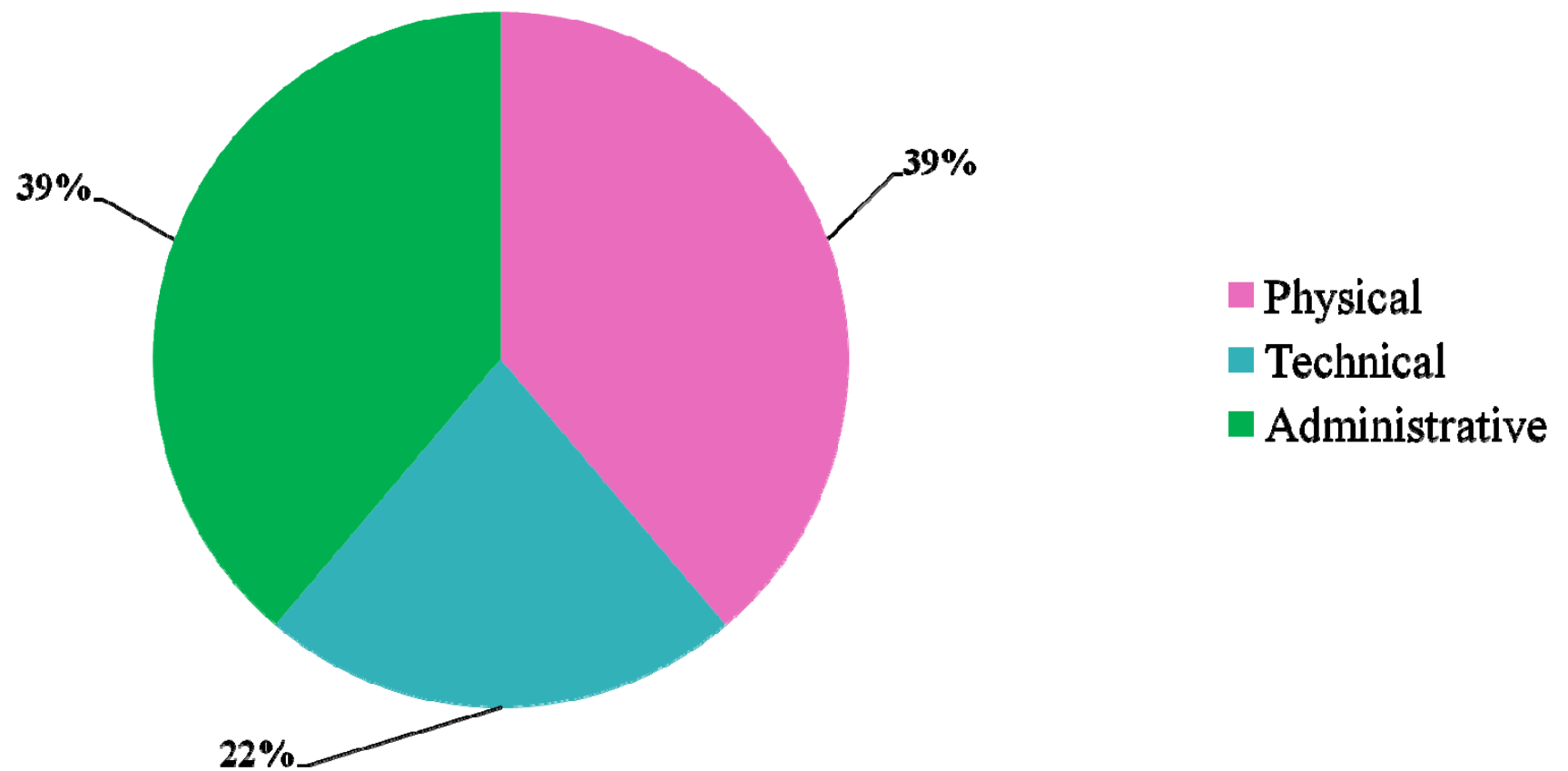
Number of Indian Hospitals on Administrative safeguards Parameters



Number of Indian Hospitals on Technical safeguards Parameters



Proportion of Safeguards by types used in Indian Hospitals





- It was observed that there are appropriate amount of rules and regulations for handling patient data safety which helps to govern the US hospitals
- There are separate physical, administrative and technical safeguards
- Rules are there for mandating US hospitals to disclose data breaches
- Strict penalties and punishments

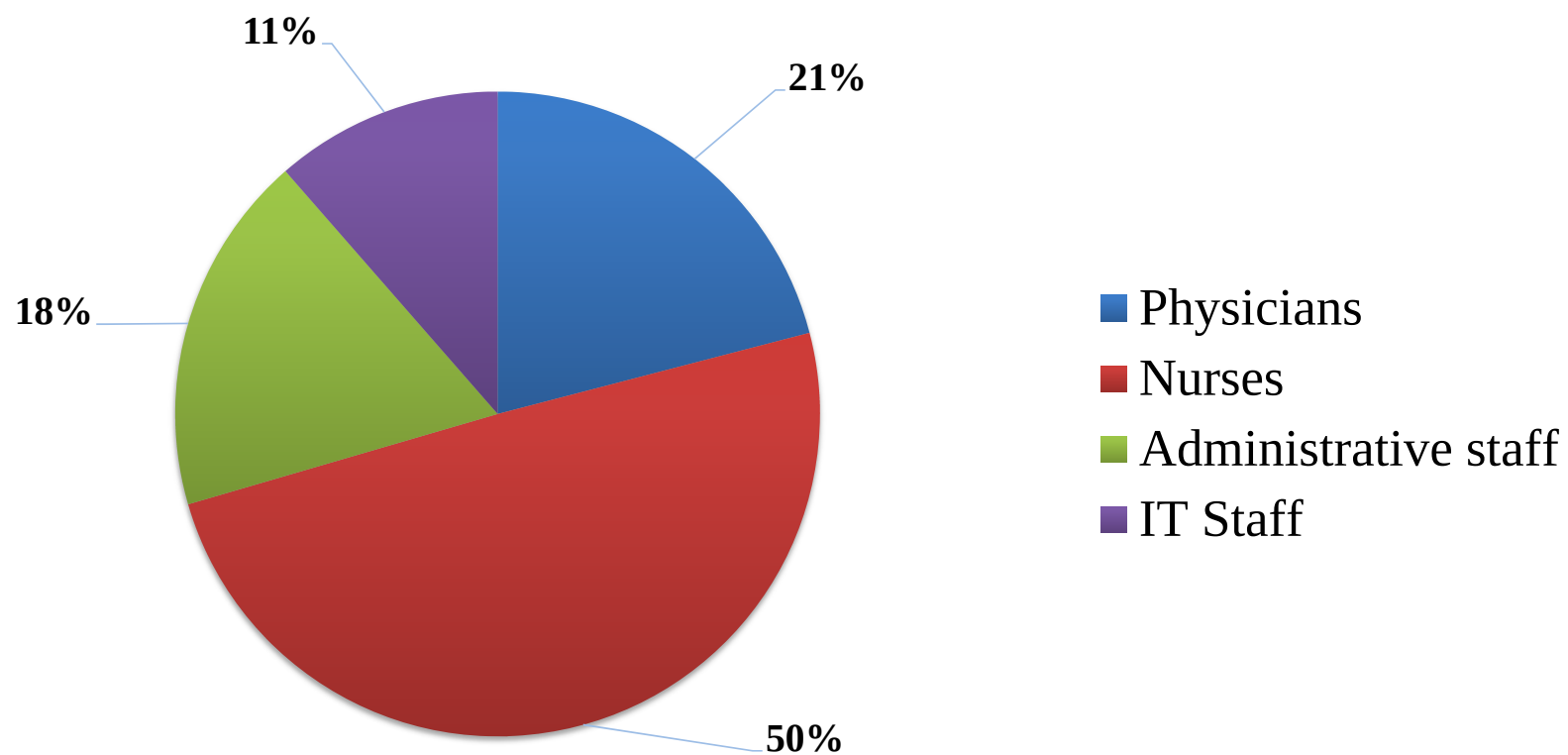


- It was observed that there are rules and regulations for handling patient data but lacks effective implementation.
- There are no rules mandating Indian hospitals to disclose data breaches
- There are very less awareness about patient data safety rules and implementation of penalties and violations of the rules

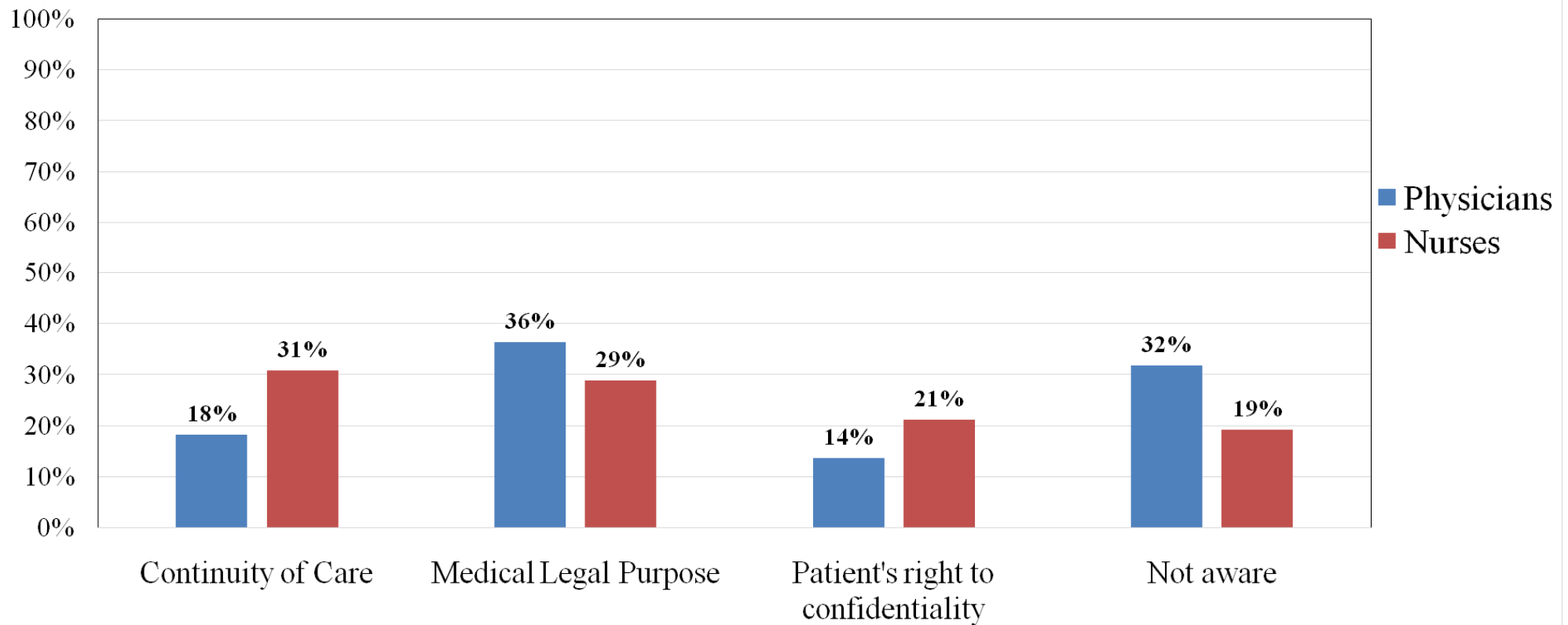
Analysis for Indian Hospitals to understand
perception level of the staff members



PERCENT DISTRIBUTION OF RESPONDENTS BY THEIR CATEGORIES

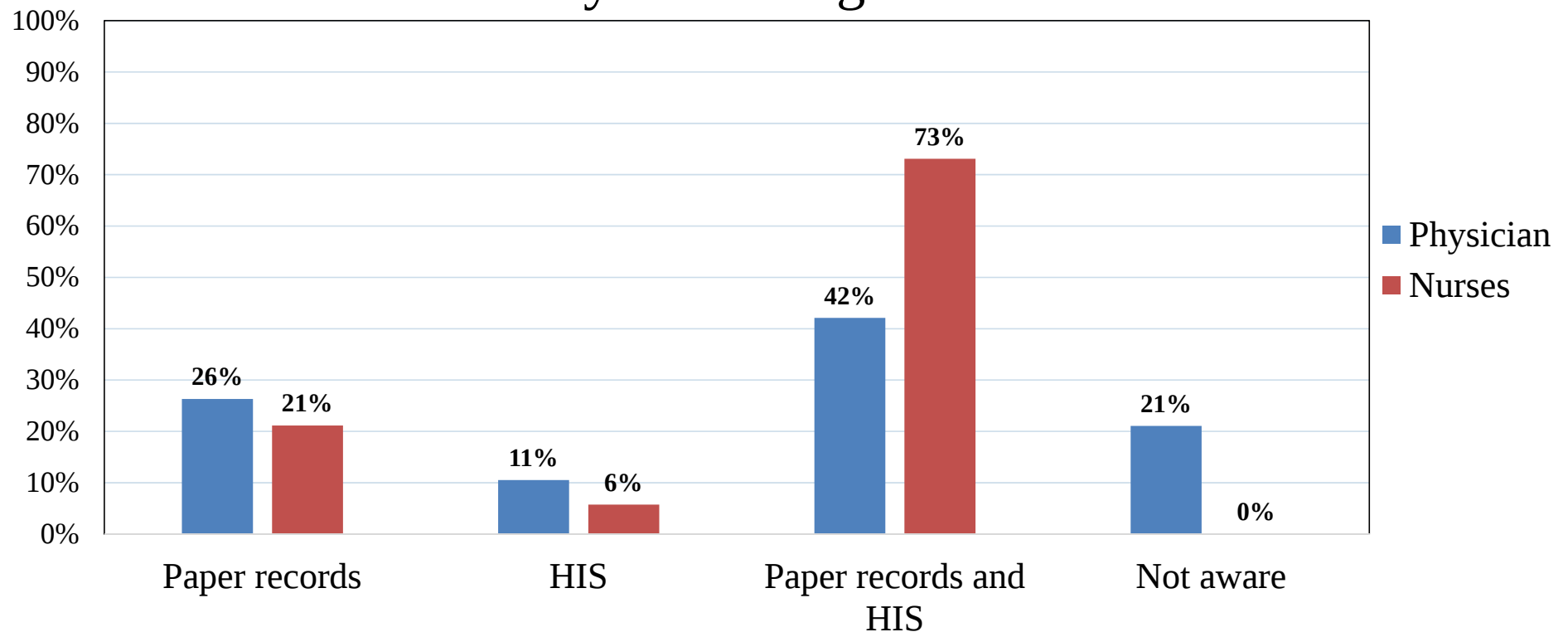


Per cent Distribution of Respondents by their understanding of reasons to Secure Patient Data



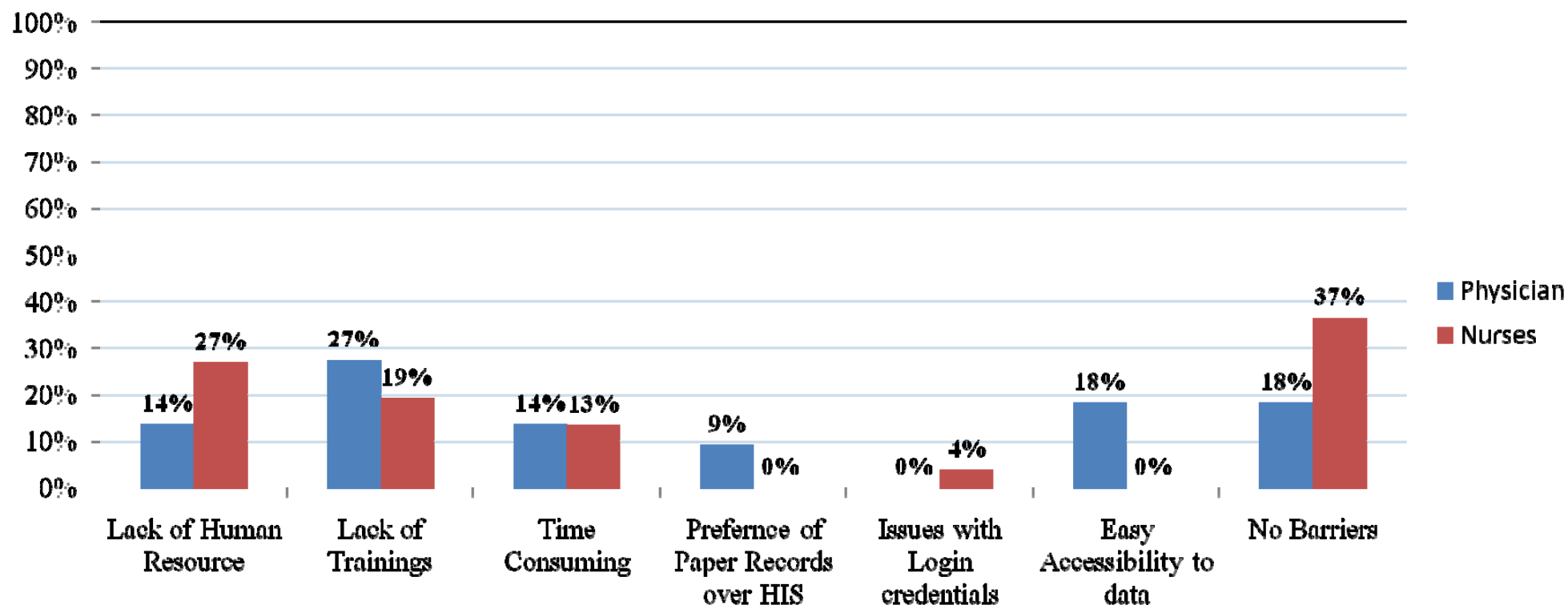
Physicians (n= 22), Nurses (n=52)

Percent distribution of respondents by their understanding on the ways to manage data



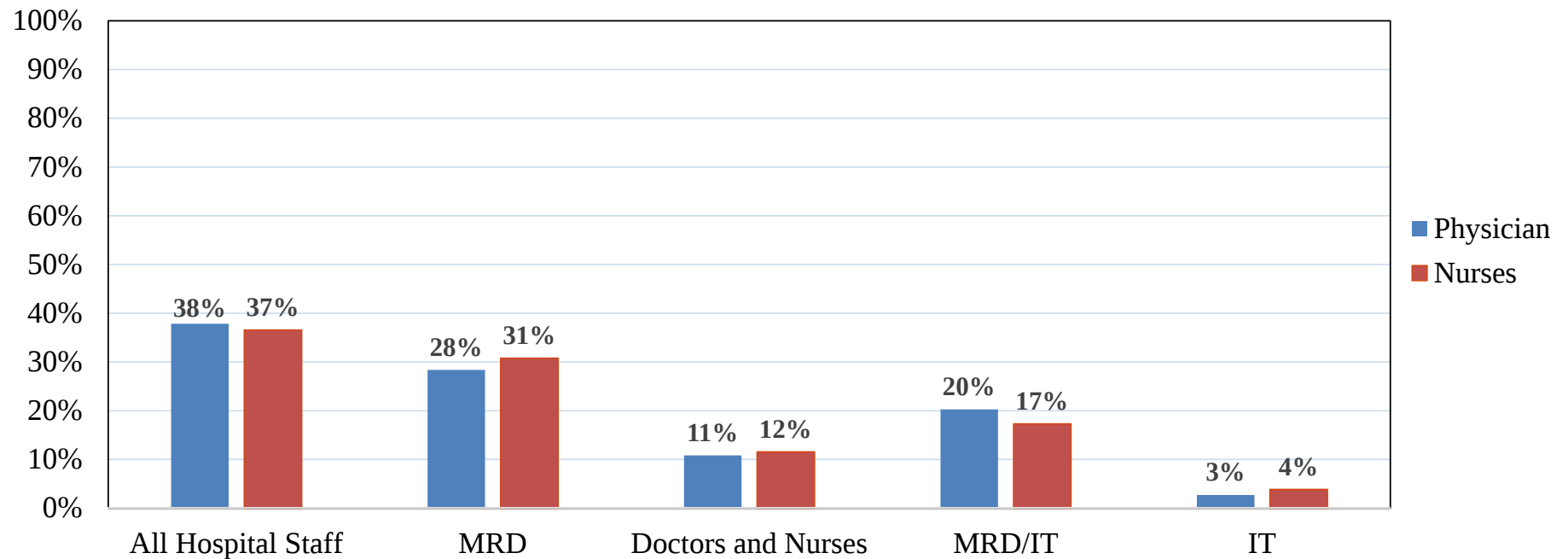
Physicians (n= 22), Nurses (n=52)

Percent distribution of respondents by their understanding on barriers to patient data safety



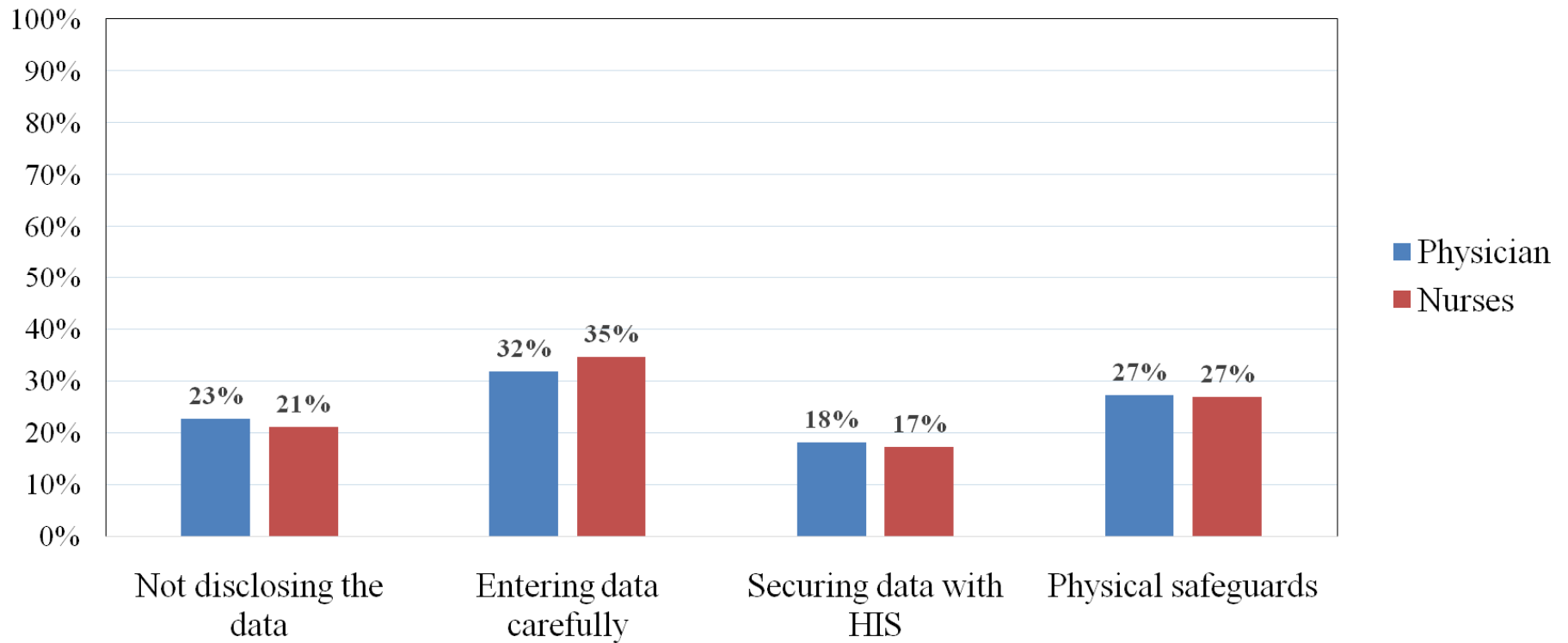
Physicians (n= 22), Nurses (n=52)

Per cent Distribution of Respondents by their understanding of responsibility to ensure Patient Data Safety



Physicians (n= 22), Nurses (n=52)

Per cent Distribution of Respondents by their understanding of Steps to ensure Patient Data Safety



Physicians (n= 22), Nurses (n=52)

Contd....

-
- **Training on privacy and security standards in the hospitals**
 - **Scope of improvement** –Role based access, more organized use of computers in documenting patient data, dedicated manpower for HIS
 - **Policies against employees for violating rules** Human resources department along with IT department sends a warning letter against the employee.
 - 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 repercussions of breaking the specified rules.
 - **Workflow for Password Management-** Permission is generated by HR and then IT department provides user access with temporary password. Expiration of password is done in case of terminated employee. Resetting of password is carried out in accordance with IT staff.
- 

Contd...

- **Technical safeguards-** User based access is practised. Data backup is performed periodically depending upon the policies of the hospital. Scanned copies of patient files are also maintained.
- **Guidelines to destroy redundant data-** Proper guidelines for destroying data within particular period of time. Patient record of medico-legal cases are kept for lifetime, OP/IPD and PACS data are kept for 5 years.
- **Control user's access to patient specific data-** Each department has security groups and access is confined for nurses, doctors, and administrative as well as IT staff. Role based user access is well defined.

Scope for implementing Health Insurance Portability and Accountability guidelines in Indian hospitals

- Adherence to the technical safeguards for storage and maintenance of patient health information.
- Continuous capacity building- Regular mandatory trainings for all the staff members of the hospitals periodically.
- Establish system for security access process and data transfer like reports, discharge summaries, orders placement and make it easy to understand.
- Monitoring and supervision- Indian hospitals need to learn lessons from the best practices in developed countries having strong governance systems which monitor regularly

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.
 - Lack of active legal framework
 - Double burden of maintaining HIS data
 - Other shortcomings include unauthorized audit trailing of health information, lack of dedicated manpower for HIS, low focus on training the staff.
- 

Limitations of the study

- The study was conducted only in private hospitals of Bangalore.
 - Scientific study requires more rigorous process (sample size and sampling) but only six hospitals were included.
 - Resistance in hospitals to respond to certain aspects of data security due to lack of understanding on the subject.
- 

THANK YOU