iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66209

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Impact of Front Office Staffs Training in Patient Information Security and Privacy in Hospital Information Management System

Dr. Vishala Bodetti[1], Vimal Pumposh[2], Nrip Nihalani[3], Aditya Patkar[4]
Plus91 Technologies Pvt Ltd,

Abstract: ***The widespread adoption of digital systems in India's healthcare sector, including Hospital Information Management Systems (HIMS) and Electronic Health Records (EHRs), has revolutionized patient care delivery. Despite these advancements, safeguarding the privacy and security of sensitive patient information has become a significant challenge. Front office staff, often the initial point of contact for patients and key users of HIS, play a critical role in implementing digital health security measures. The aim of this study is to evaluate the impact of front office staff training on adherence to digital health security guidelines within the Indian healthcare system, focusing on its role in safeguarding patient privacy and mitigating data security breaches in hospital information systems (HIS). The study seeks to explore the relationship between training practices, compliance with security protocols, and improvements in patient privacy outcomes.Using a qualitative and exploratory research methodology, this research examines the need for front-office executive training evaluates their alignment with national and global security standards, and explores their outcomes. The study was well-researched by analyzing articles, research papers, and case studies available on Google and Google Scholar***

Adhering to digital health security guidelines is crucial in the Indian context, where increasing digitization coincides with rapid healthcare expansion under initiatives such as the Ayushman Bharat Digital Mission (ABDM). These guidelines ensure the protection of sensitive data, mitigate cyber threats and build trust between healthcare providers and patients. By focusing on enhancing training programs and aligning them with evolving digital security standards, this research provides actionable recommendations for improving patient privacy and data protection in India's healthcare ecosystem.

Keywords: Front office, Data Privacy, Compliance, Information security, Hospital information system

I. BACKGROUND

The Indian healthcare system has undergone a rapid digital transformation, with electronic health records (EHRs), telemedicine, and digital hospital management systems becoming ubiquitous. Despite these advancements, breaches of patient privacy and data security remain critical challenges.

In a hospital, the front desk is the initial point of contact, managing private patient data and coordinating with the HIS. The effective training of front office staff in digital health security guidelines is essential to mitigate risks.

The major responsibilities of front office staff are as follows:*[1]:*

A. Patient and Visitor Interaction:

1) Welcome and greet patients and visitors courteously.

2) Answer inquiries related to services, and assist patients in completing required forms and documentation.

B. Appointment Scheduling:

1) Schedule patient appointments with the correct doctors promptly and accurately.

2) Demonstrate effective time management to minimize patient wait times and enhance.

C. Follow-ups and Patient Outreach:

1) Contacting patients regarding their appointments and conducting regular follow-up calls.

2) Foster a positive reputation for the institution through proactive communication.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

D. Insurance and Eligibility Verification:

1) Screen patient information and insurance eligibility to prevent claim rejections and denials.

E. Administrative and Billing Responsibilities:

1) Maintain patient records, manage billing and payment documentation, and ensure confidentiality.
2) Review insurance policies and oversee financial records.
3) Record and collect patient charges, manage credit for patients, and handle third-party claims.
4) Copying, faxing, and e-mailing documents between clinics, hospitals, and clientele
5) Managing document transfers among clinics, hospitals, and their clients via email, fax, etc

F. Technical Skills and Software Usage:

1) Use digital software for the smooth functioning of daily tasks to save time, maintain confidentiality, and optimize efficiency.

Front office staff play a pivotal role in ensuring compliance with the DPDPA, as they are often the first point of contact for collecting and handling patient information. Proper training must be provided to front office personnel to familiarize them with the Act's guidelines, emphasizing the importance of obtaining informed consent, maintaining confidentiality, and managing data securely. This not only prevents lapses in compliance but also reinforces the hospital's commitment to ethical data management practice.

Digital Personal Data Protection Act, 2023[2] applies to the processing of digital personal data within the territory of India collected online or collected offline and later digitized

It encapsulates the following essential principles:

- Purpose Limitation – Personal data must be processed solely for a legitimate reason for which the data subject has provided consent, in compliance with the DPDP Act.
- Collection Limitation – Only the personal data that is essential should be gathered.

Another key aspect of the DPDP Act is the penalty provision [3]. Data fiduciaries may face fines for failing to comply with its regulations, with penalties reaching up to INR 250 crore, Some of these are:

- Breach in observance of duty of data principal up to INR10,000
- Failing to uphold the duty of care towards data principals could lead to a fine of up to INR 10,000.
- If there is a failure to notify the data protection board and the impacted data principles after a personal data breach, the penalty may escalate to as much as INR 200 crore.
- Furthermore, violations of additional obligations related to children can also result in fines of up to INR 200 crore.

In India, the healthcare sector is experiencing a dual challenge: rapid digitization and the need to address unique vulnerabilities in data protection. Following digital health security guidelines is essential for several reasons [4][5]:

- *Protection of Patient Privacy:* Safeguarding sensitive personal health information from unauthorized access or breaches is fundamental to ensuring patients' rights and maintaining confidentiality.
- *Compliance with Legal Frameworks:* Adhering to guidelines like the DPDP compliance and DISHA helps healthcare institutions avoid legal and financial penalties
- *Preventing Cyber Threats:* With increasing instances of ransomware attacks and data breaches, robust security practices are critical to counteract sophisticated cyber threats targeting the healthcare industry.
- *Trust and Credibility:* Adherence to security guidelines strengthens patient trust in healthcare providers, which is vital for encouraging the use of digital platforms like telemedicine and online health records.
- *Support for Healthcare Expansion:* Initiatives like ABDM aim to integrate health services digitally across the nation. Following security guidelines ensure these platforms operate securely and effectively, fostering long-term digital growth in healthcare.[6]
- *International Standards Alignment:* India's healthcare sector must align with global data security standards (e.g., HIPAA, ISO 27001) to enhance its credibility and facilitate medical tourism and cross-border healthcare collaborations.

This study explores the impact of front office staff training on adherence to digital health security guidelines in India, focusing on its role in safeguarding patient privacy and evaluating the effectiveness of IT training in Hospital Information Systems (HIS).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

II. RESEARCH METHODOLOGY

The study is defined as qualitative and exploratory research, mainly drawing on information obtained from articles, eBooks, blogs, research papers, and case studies. This approach has been selected because of the broad scope of the research area and the variety of data sources available from different locations**.** To arrive at a conclusive idea of the larger picture on the impact of receptionist training on hospital information systems related to patient privacy security and concerns, analyzing the existing descriptive data would give a better result in finding the answers to the research question framed.

A. Research Objectives

1) *To Evaluate the Role of front office Training in Safeguarding Patient Information:* Analyze the specific contributions of receptionist/ front office training to patient data protection and compliance with privacy regulations in hospital information management systems (HIMS)
2) *To Investigate the Relationship Between Training and Compliance:* Explore how the level of training impacts the compliance of Front office staff with data privacy laws and hospital policies, such as the Digital Personal Data Protection Act (DPDP) and relevant digital health standards in India.

III. DESCRIPTION OF STUDY

A. Objective 1- To Evaluate the Role of front office Training in Safeguarding Patient Information

In a study by Rhee et al(2009) [7] mentions that information security is dependent on user activities and that sanctions for violations would have an insignificant impact. User security awareness, advocacy, and lobbying are crucial elements of information security strategies that play a significant role in the successful implementation of data privacy measures. All the staff handling patient information should have proper training on information security [8]- The study emphasized training for the users who are handling patient information on information security

The author did another study that assessed the performance of data privacy principles observed in health facilities in Nairobi. Data Privacy requires compliance with data accountability and data protection principles [Fig3.1]. The findings of the analysis were that 100% percent of respondents were fully compliant with data security compliances [Fig3.2][7]. The healthcare organization conducted a thorough risk assessment to ensure the protection of patient data through physical, logical, system, and technical security measures. It implemented all necessary actions to minimize errors and ensure the accuracy of patient data processing. Additionally, the organization introduced up-to-date user training programs, enabling respondents to achieve 100 % compliance with data security and privacy requirements.

Data Accountability and Protection Requirements	Agree	% - Agree	Dis-agree	% -Dis agree	Total	%
Does your health facility carry out a comprehensive risk assessment that recommends accountability measures and responsibility allocation?	33	100	0	0	33	100
Is patient data at rest and in transit protected by physical, logical, system and technical security safeguards?	33	100	0	0	33	100
Are all steps taken to eliminate errors and ensure that patient data processing is accurate, complete and up-to-date?	33	100	0	0	33	100
Do your patient data privacy control measures include implementation of user training programmes and adherence to approved codes of conduct?	33	100	0	0	33	100

Source: Author (2021)

Fig.3.1: Questionnaires asked to respondents on Data Protection

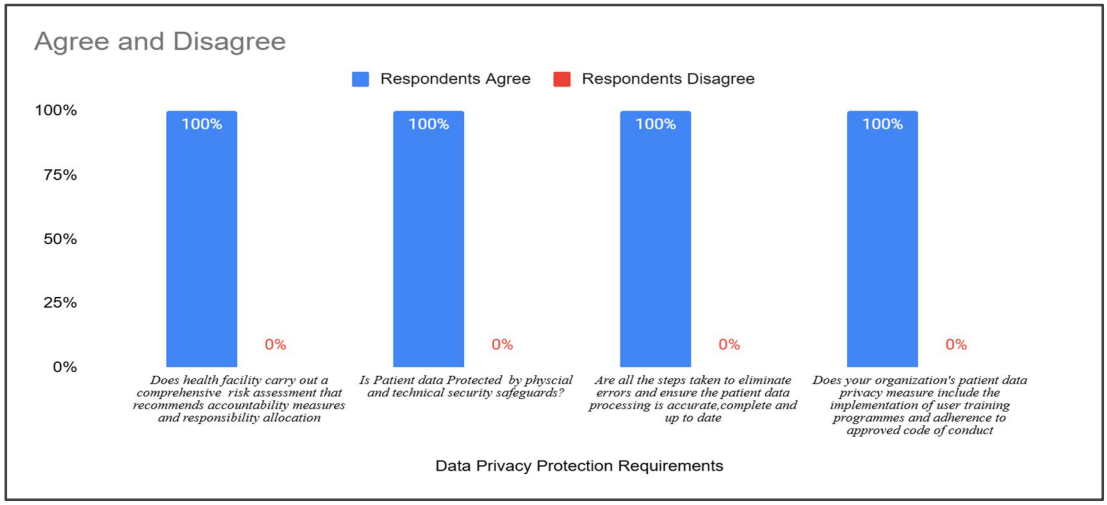


Fig. 3.2: Analysis of Respondents on Data Protection

In a research study [8], the author emphasized that the success of health organizations in ensuring information security relies on two key factors:

Technical aspects, which address vulnerabilities in the information systems, and Organizational and human factors involve the misuse or unauthorized access of patient information by internal staff abusing their privileges.

This study classifies threats to patient information security into two primary categories:

1) *Technical threats* arising from weaknesses in the technical infrastructure of information systems.
2) *Organizational and human threats*, stemming from improper or unauthorized access by internal personnel exploiting their access rights.

To address these threats, technical challenges can be mitigated through the implementation of advanced technical solutions that safeguard against unauthorized system access and data breaches. Conversely, organizational and human threats can be managed through strategies such as staff training on data protection, continuous monitoring to prevent rule violations, and fostering ethical practices by promoting the principles of workplace ethics. In this study, technical and physical protection measures are grouped under the technical aspects of information security. Meanwhile, factors such as staff training, ethical behavior, and monitoring are considered organizational determinants of perceived security. Many employees do not have a strong understanding of the security technologies in place, leading them to evaluate the organization's data protection measures based on varying criteria. This phenomenon is called perceived security. To alleviate individuals' worries regarding the safety of their information, it is essential to improve the factors that significantly influence their sense of security. The author conducted a quantitative study to examine the relationship between organizational and human factors and the impact of training. To meet this objective 12 hypotheses were proposed the data was collected using a cross-sectional and self-administered survey [Fig 3.3][8], distributed among patients across 9 hospitals. A total of 382 questionnaires were collected and after the pilot study, the results revealed that staff training has positive results on patient trust in hospitals and some researchers indicate that enhancing staff training in security skills is anticipated to mitigate security risks within organizations [Fig3.4][9][10][11]

.

Hypothesis		Std Beta	Std Error	t-value	Decision
H1	Training - > Perceived Security	0.160	0.068	2.350***	Supported
H2	Monitoring - > Perceived Security	0.186	0.065	2.862***	Supported
H3	Physical protection- > Perceived Security	0.024	0.042	0.587	Not Supported
H4	Ethics - > Trust	0.187	0.059	3.176***	Supported
H5	Physical protection- > Trust	0.121	0.052	2.317**	Supported
H6	Technical - > Trust	0.123	0.058	2.107**	Supported
H7	Training - > Trust	0.212	0.057	3.693***	Supported
H8	Monitoring - > Trust	0.313	0.067	4.638***	Supported
H9	Ethics - > Perceived Security	0.181	0.064	2.845***	Supported
H10	Training - > Ethics	0.461	0.052	8.914***	Supported
H11	Trust - > Perceived Security	0.060	0.042	1.420*	Supported
H12	Technical - > Perceived Security	0.238	0.068	3.526**	Supported

Fig 3.3: Results based on hypothesis tests

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

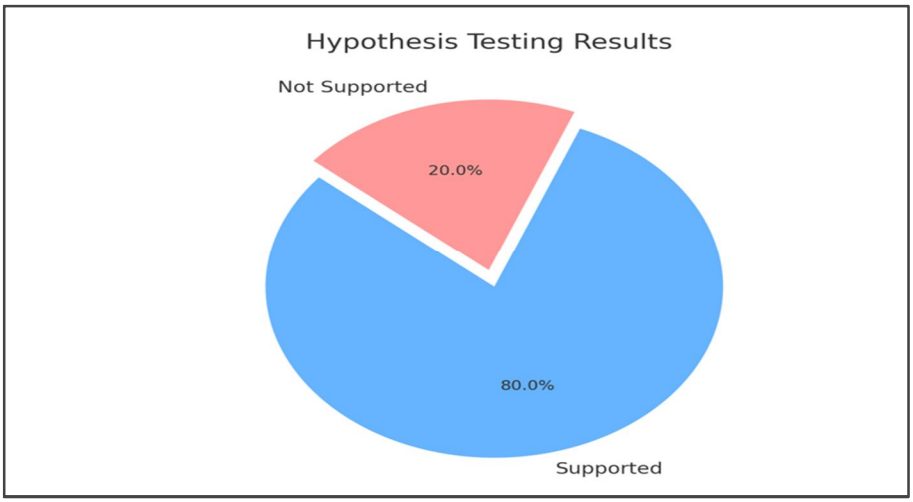


Fig 3.4: Hypothesis Results showed training has a positive impact on security measures.

The findings of the study have numerous practical implications like Health organizations should establish policies to train their employees on various information security aspects, including identifying potential threats and penetration methods, understanding their responsibilities in safeguarding information, developing the necessary skills to address security challenges, and being aware of relevant legal considerations. Furthermore, to positively influence patients' perceptions of how well their sensitive information is protected, hospitals should actively communicate these employee training policies to their patients. This transparency can help alleviate patients' concerns about potential breaches of their information security and develop trust for the organization.

In a pilot project conducted by the Department of Obstetrics, Gynecology, and Reproductive Sciences (University of Pittsburgh) [12] to evaluate a systems-based practice experience designed to introduce residents to front-office responsibilities and stimulate suggestions for front-office improvements. Twenty-three residents participated in the program, and each spent 8.5 hours total in the front office with one or two front office preceptors. Each resident completed both the pre-and post-surveys and Surveys of the 23 residents who all believed the front office staff to be “important” or “vital” to the success of a practice. Nineteen out of 23 (83%) residents answered post-experience that the front office staff was “much more important” to the patients than their own medical care of patients. The average score for one specific question showed a notable change from pre-experience to post-experience on how well-trained front office can perform their daily responsibilities. The study clearly showed the front office staff to be an important part of patient care and the functioning of the Hospital.

According to Medbridge[13] mentioned the importance of compliance training. Healthcare compliance training is a critical aspect of any medical organization, serving as a protective measure on multiple fronts. It helps shield organizations from legal repercussions, equips employees with essential knowledge about the rules and regulations governing their roles, and safeguards patients by minimizing risks associated with negligence or inadequate training. Compliance training is not only a legal requirement for organizations to operate but also plays a key role in reducing the likelihood of sanctions and financial penalties.

B. Objective 2- To Investigate the Relationship Between Training and Compliance

The level of training provided to hospital receptionists plays a pivotal role in ensuring compliance with data privacy laws and hospital policies, particularly in the context of India’s evolving regulatory landscape. Training equips receptionists or front offices with the knowledge and skills required to handle sensitive patient information securely, aligning their practices with frameworks such as the Personal Data Protection Bill (PDPB) and relevant digital health standards. Effective training programs ensure that receptionists understand the nuances of privacy regulations, such as obtaining informed consent for data collection, safeguarding electronic health records (EHRs), and preventing unauthorized data access.

The Government introduced the Digital Information Security in Healthcare Act (DISHA) as India's counterpart to the Health Insurance Portability and Accountability Act (HIPAA) before the DPDP Act 2023 was enacted. DISHA's main goals are to establish uniform standards for the protection, privacy, and security of healthcare data, to create the National Electronic Health Authority (NeHA), and to promote Health Information Exchanges. Although DISHA has not yet been put into effect, it seeks to foster the broad adoption of e-health standards throughout India.[14][15]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

On August 11, 2023, India implemented the Digital Personal Data Protection Act, 2023 (DPDP Act) [2][3]. This Act regulates the management of personal data within the country, with the primary objective of safeguarding individual privacy while creating a structure for data accountability and governance. The DPDP Act is poised to profoundly influence the Indian healthcare industry, which is currently undergoing initial phases of digital transformation. It is important to note that the DPDP Act specifically addresses digital personal data and does not extend its provisions to non-personal data.

Training programs for information security are essential for all organizations to safeguard their valuable assets. Employees play a crucial role in ensuring the security of information. As organizations face evolving threats and challenges in information security, training programs must remain adaptable and flexible to address both current and future needs. Establishing a sustainable training framework is vital to anticipate future requirements. These programs enable users to understand the significance of sensitive and personal data, the organization's security objectives, policies, and the skills necessary for effective information security management [16] Given that training programs are proven to be effective in mitigating risks associated with electronic health systems [16], healthcare organizations can develop tailored training modules aimed at employees. These modules focus on creating awareness about compliance requirements in accordance with legislative policies and regulations [17]

A research was conducted to assess the impact of an information security training program within a private hospital [18]

The study was carried out in a private hospital that had a total of 403 employees. The number of HIMS users was 313 in the hospital. Among them, 100 users participated in the study. Pre-tests were applied before information security training. Then, the training was performed. A week later, post-tests were carried out. The data was collected through a structured questionnaire. Additionally, employees were asked about their involvement in HIMS training. The health manager selected three subgroup scores related to "Security Policy," "Access and Authorization," and "Security Applications."

The results of the study were that no significant difference was found in the pre-test and post-test scores of those who received HIMS training and those who did not. The use of HIMS has ensured the achievement of many purposes such as creating a cost advantage, saving time by efficiently using time, producing quality service, and protecting and improving health. In particular, it has enabled the service provision to the patient at the right time [19]. In this respect, HIMS training is of great importance. However, according to the results of the study, HIMS training is not sufficient in terms of providing information security and privacy. These results could be predicted since the outlines of information security training are different from HIMS. The results outline the importance of information security training for the staff and how it differs from Hospital information system training.

Employees, particularly front office staff, must be trained to handle information responsibly in accordance with established guidelines and to understand the potential consequences of their actions. As front office staff serve as the first point of contact and regularly interact with sensitive patient data, their role in maintaining information security is critical. Security training and awareness programs are essential components of any robust information security policy, especially in healthcare settings where data breaches can have significant legal and ethical implications.

To enhance the effectiveness of these programs, it is vital to motivate employees, including front office staff, to apply the skills they have learned to their daily tasks. These staff members, who frequently use Hospital Information Management Systems (HIMS), must be educated about the risks and vulnerabilities associated with information security. Targeted training helps front office personnel mitigate risks such as unauthorized data access or improper handling of patient records. Consequently, security policies should be designed to align with employees' levels of awareness, emotional readiness, and the specific conditions of their work environment, ensuring that front office staff are well-equipped to safeguard sensitive information.

IV. RESULTS

A. *Objective I findings*

The study highlights the critical role of front office training in enhancing patient data protection and compliance within hospital information systems**.** As the first point of contact for patients, the front office is critical in managing sensitive information and setting the tone for institutional trust. Several key findings emphasize its importance:

1) *Training and Awareness:* Studies, including those by Rhee et al. (2009) and other researchers, stated that effective information security practices hinge on user awareness rather than mere sanctions for violations. Given that front office staff are at the forefront of handling patient information, their training ensures compliance with data accountability principles and reinforces robust security measures. In a study where healthcare organizations in Nairobi achieved 100% compliance with data security protocols after implementing structured training programs. This reflects the effectiveness of risk assessments and up-to-date user education in safeguarding patient data.

2) *Threat Mitigation:* Front office training plays a dual role in addressing both technical and organizational threats. While technical threats can be countered with advanced system protections, organizational risks—stemming from internal misuse or privilege abuse—require interventions such as continuous monitoring, ethics training, and fostering a security-conscious workplace culture. The front office's unique position as gatekeepers of data makes their role indispensable in identifying and mitigating these risks.
3) *Patient Trust:* As the first point of interaction, the front office significantly influences patient perceptions of an institution's data security. Staff training directly correlates with enhanced patient trust. Transparent communication of training policies reassures patients about the security of their sensitive information. A pilot project at the University of Pittsburgh demonstrated that trained front office staff were perceived as significantly vital to patient care, even surpassing clinical interactions in importance.
4) *Practical Implications:* The study advocates comprehensive training tailored to the front office's responsibilities. This includes identifying vulnerabilities, understanding legal requirements, and developing skills for mitigating security challenges. These measures not only bolster patient confidence but also reinforce the front office's crucial role in institutional credibility and operational efficiency. By ensuring their preparedness, hospitals can bridge the gap between organizational vulnerabilities and technical safeguards

B. Objective II findings

The study focuses on the impact of training programs on adherence to data privacy laws and hospital policies, particularly within the context of India's evolving regulatory framework

1) *Regulatory Alignment:* Training ensures that front office staff align guidelines under laws such as the Digital Personal Data Protection Act (DPDP) and DISHA. These laws emphasize obtaining informed consent, secure data handling, and preventing unauthorized access, all of which are critical for operational compliance.
2) *Program Effectiveness:* Research in private hospitals demonstrates that while HIMS (Hospital Information Management Systems) training enhances operational efficiency, it is insufficient for robust information security. This highlights the need for specialized information security training to bridge gaps in compliance.
3) *Security Outcomes:* Studies show a positive relationship between targeted security training and improved compliance outcomes. For example, a study involving 100 HIMS users revealed significant advancements in understanding security policies and applications post-training. However, it noted the importance of tailoring training programs to address specific data protection challenges.
4) *Employee Motivation:* Effective security policies must consider employees' readiness and workplace conditions. Motivating front office staff to implement learned skills in daily tasks enhances adherence to security protocols. This approach minimizes risks such as unauthorized access and improves overall organizational security.

V. DISCUSSION

The study explores the significant impact of receptionist training in hospitals, particularly in safeguarding patient information and enhancing the quality of service in hospital information management systems (HIMS). Training the front office staff is vital because they are the first point of contact for patients and families and act as custodians of sensitive information. The findings emphasize that well-trained receptionists can bridge the gap between technical and organizational vulnerabilities by:

1) *Enhancing Patient Trust and Security Perceptions:* Studies have demonstrated a positive correlation between staff training and patient trust. Proper training not only equips employees to handle sensitive information but also improves patients' perception of the institution's commitment to data security.
2) *Facilitating Compliance with Regulatory Frameworks:* With the enactment of the Digital Personal Data Protection Act (DPDP) and the earlier DISHA guidelines, hospitals in India face increasing responsibilities to ensure adherence to privacy regulations. Training programs tailored to these requirements empower staff to fulfill legal and ethical responsibilities.
3) *Mitigating Security Risks:* Technical and human threats to patient information security demand multifaceted strategies. While advanced IT solutions address technical vulnerabilities, organizational and human factors require targeted interventions like ethics training, awareness programs, and hands-on experience in handling patient data securely.
4) *Improving Service Quality:* Training receptionists enhances their ability to manage appointments, communicate effectively, and provide timely assistance, thereby improving overall patient satisfaction.

VI. CONCLUSION

The findings of this study show the vital role of front office training in safeguarding patient information and ensuring compliance with digital health security guidelines within the healthcare ecosystem. As the first point of interaction for patients, the front office staff are pivotal in managing sensitive patient data, promoting trust, and ensuring operational efficiency.

This research highlights that well-structured training programs enhance front office staff's ability to address technical and organizational vulnerabilities. By equipping them with the skills to handle data securely, adhere to legal frameworks such as the Digital Personal Data Protection Act (DPDP), and align with global standards, healthcare institutions can mitigate risks associated with data breaches and cyber threats. Additionally, the emphasis on fostering patient trust through transparent communication of training policies reinforces the front office's role in institutional credibility. By bridging the gap between operational vulnerabilities and advanced technical protections, trained front office personnel significantly contribute to a hospital's reputation and seamless care delivery. In conclusion, continuous investment in targeted, adaptive training modules for front office staff is imperative for maintaining patient privacy, ensuring regulatory compliance, and achieving excellence in healthcare service delivery. Future initiatives should prioritize integrating security-conscious practices with operational training to empower staff to navigate the evolving landscape of healthcare digitization effectively

REFERENCES

[1] Puri I. A study on the role of front office administration in Max Super Specialty Hospital Bathinda. Journal of Ayurveda and Integrated Medical Sciences [Internet]. 2024 Sep 28;5(06):321–9. Available from: **https://jaims.in/jaims/article/view/16281**

[2] Government of India. (2023, August 11). Ministry of Electronics and Information Technology, Government of India | Home Page. Www.meity.gov.in. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[3] DPM. "India's Digital Personal Data Protection Act - DPDP – Data Privacy Manager." Data Privacy Manager, 5 Oct. 2023, dataprivacymanager.net/dpdp-india-digital-personal-data-protection-act

[4] Arora Vanshika," Protection of User Healthcare Data in India the DISHA Bill: Substantive Takeaways from GDPR" NUALS Law Journal,1Oct2022,nualslawjournal.com/2022/10/01/protection-of-user-healthcare-data-in-India-vis-a-vis-the-disha-bill-substantive-takeaways-from-gdpr

[5] Mahajan AG. Breach or Betrayal: Analyzing the Legal Framework on India's Biggest Healthcare Data Leak - Libertatem Magazine [Internet]. LibertatemMagazine.2023.Availablefromhttps://libertatem.in/blog/breach-or-betrayal-analyzing-the-legal-framework-on-indias-biggest-healthcare-data-leak

[6] "NHA | Official Website Ayushman Bharat Digital Mission." Abdm.gov.in, 2024, abdm.gov.in/resources.

[7] Ayugi, E. D. (2021). Information Security Strategies and Patient Data Privacy Among Health Facilities in Nairobi. E repository.uonbi.ac.ke. **http://erepository.uonbi.ac.ke/handle/11295/157072**

[8] Peikari, H. R., T., R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. BMC Medical Informatics and Decision Making, 18(1). https://doi.org/10.1186/s12911-018-0681-z

[9] Parssian, Amir, et al. "Impact of the Union and Difference Operations on the Quality of Information Products." Information Systems Research, vol. 20, no. 1, Mar. 2009, pp. 99–120, https://doi.org/10.1287/isre.1070.0161.

[10] Farzandipour, Mehrdad, et al. "Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study." Journal of Medical System Vol. 34, no.4,1Apr. 2009,pp. 629-642, paramedicine.kaums.ac.ir/uploaded flies/article/frazandipoor/security-requirements_EHR.pdf, https://doi.org/10.1007/s10916-009-9276-7.

[11] Ifinedo, Princely. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition." Information & Management, vol. 51, no. 1, Jan. 2014, pp. 69–79, https://doi.org/10.1016/j.im.2013.10.001.

[12] Sulkin, Gary. "Resident Front Office Experience: A Systems-Based Practice Activity." Medical Education Online, vol. 13, 2008

[13] Role of Front Office Staff In Keeping Your Practice Reputation And Financial Health Safe. (n.d. https://practolytics.com/blog/front-office-staff-practice-reputation-financial-health-safe/

[14] Group, Compliancy. "DISHA and HIPAA, How Do They Compare?" Compliancy Group, 26 Oct. 2023, compliancy-group.com/disha-and-hipaa-how-do-they-compare/?utm_source.

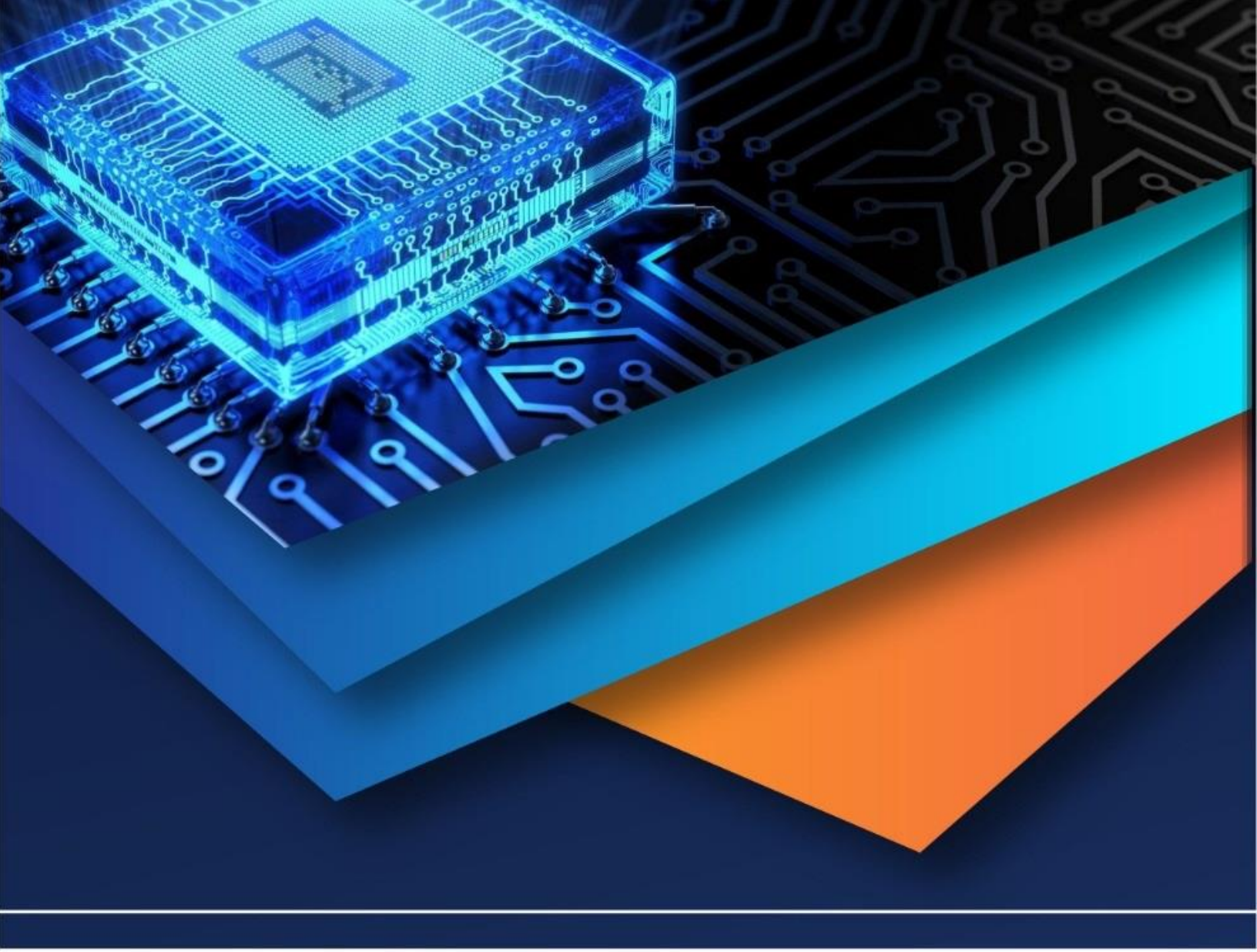
[15] Wadhwa, Manisha. National EHealth Authority (NeHA) ICT India Working Paper #29. 2020.

[16] Oyelami, J., & Ithnin, N. B. (n.d.). [PDF] People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization | Semantic Scholar. Semanticscholar.org. https://www.semanticscholar.org/reader/d2c0a18b2abcb8a68d356b3ca6bc6fd5c64152b**e**

[17] Arain, MA., Tarraf, R. and Ahmad, A. (2019). Assessing, Staff Awareness and Effectiveness of Educational Training on IT Security and Privacy in a Large Healthcare Organization, Journal of Multidisciplinary Healthcare

[18] Gonca MUMCU. (2020). Evaluation of the Effects of Information Security Training on Employees: A Study from a Private Hospital. International Journal of Health Management and Tourism. https://www.academia.edu/97519790/Evaluation_of_the_Effects_of_Information_Security_Training_on_Employees_A_Study_from_a_Private_Hospital

[19] Mumcu, G., Köksal, L., Şişman, N., Çatar, RÖ. and Tarım, M. (2014). The Effect of Pharmacy Information Management System on Safety Medication Use: A Study from Private Hospitals in İstanbul. Marmara Pharmaceutical Journa**l**



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY