

**DISSERTATION REPORT**

**AT**

**IIHMR Delhi**

**A REPORT ON**

**THE ROLE OF DATA SECURITY IN HEALTHCARE  
A SYSTEMATIC REVIEW**

**BY**

**DR TANISHA SONI**

**PG/22/134**

**Under the guidance of**

**DR PREETHA G S**

**PGDM (HOSPITAL AND HEALTH MANAGEMENT)**

**2022-2024**



**International Institute of Health Management Research, New D**

## **TABLE OF CONTENTS**

<b>Sno</b>	<b>TITLE</b>	<b>Page no</b>
<b>PART A</b>	<b>PREFACE</b>	
A	Title Page	1
B	Original Literary Work Declaration	3-8
C	Acknowledgement	9
D	About IIHMR Delhi	10-12
E	Abstract	13
<b>PART B</b>	<b>PROJECT REPORT</b>	
<b>SECTION 1</b>	<b>INTRODUCTION</b>	<b>15-17</b>
	Role of data security in healthcare	15
	Importance of Data security in healthcare	16
<b>SECTION 2</b>	<b>Rationale</b>	<b>19</b>
	Objectives	21
<b>SECTION 3</b>	<b>Methodology</b>	<b>22</b>
	Research Design	22
	Research Question	22
	Search Strategy	22-23
	Keywords	23
	Study duration	23
	Study Population	23
	Inclusion Criteria	23
	Exclusion Criteria	23
<b>SECTION 4</b>	<b>Results</b>	<b>25-32</b>
<b>SECTION 5</b>	<b>Discussion</b>	<b>34-36</b>
<b>SECTION 6</b>	<b>Conclusion</b>	<b>37</b>
<b>SECTION 7</b>	<b>References</b>	<b>38</b>

**(Completion of Dissertation from respective organization)**

The certificate is awarded to

**Name Dr Tanisha Soni**

in recognition of having successfully completed his/her  
internship in the department of

**Title Secondary Research**

and has successfully completed his/her Project on

**Title of the Project**

**THE ROLE OF DATA SECURITY IN HEALTHCARE A SYSTEMATIC REVIEW**

**Project Date: 01-04-2024 to 30-06-2024**

**Organisation: International Institute of Health Management Research**

He/She comes across as a committed, sincere & diligent person  
who has a strong drive & zeal for learning.

We wish him/her all the best for future endeavors.

  
**Dissertation Mentor  
Dr Preetha G S**

**TO WHOMSOEVER IT MAY CONCERN**

This is to certify that **Dr. Tanisha Soni** student of **PGDM (Hospital & Health Management)** from **International Institute of Health Management Research, New Delhi** has undergone internship training at **IIHMR Delhi** from 01-04-2024 to 30-06-2024.

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 his/her future endeavors.



Dr. Sumesh Kumar

Associate Dean, Academic and Student Affairs

IIHMR, New Delhi



Dr. Preetha G.S.

~~Associate~~ Professor, Mentor

IIHMR, New Delhi

### **Certificate from Dissertation Advisory Committee**

This is to certify that **Dr. Tanisha Soni**, a graduate student of the PGDM (Hospital & Health Management) has worked under our guidance and supervision. She is submitting this dissertation titled "**The Role of Data Security in Healthcare- A Systematic Review**" at "**IHMR Delhi**" in partial fulfilment of the requirements for the award of the PGDM (Hospital & Health Management). This dissertation has the requisite standard and to the best of our knowledge no part of it has been reproduced from any other dissertation, monograph, report or book.



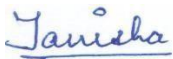
Institute Mentor

Dr Preetha G S  
Associate Professor

**INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH,  
NEW DELHI**

**CERTIFICATE BY SCHOLAR**

This is to certify that the dissertation titled **The Role Of Data Security in Healthcare- A systematic Review** and submitted by **Dr Tanisha Soni** Enrolment No. **PG/22/134** under the supervision of **Dr. Preetha G S** for award of PGDM (Hospital & Health Management) of the Institute carried out during the period from **01-04-2024 to 30-06-2024** 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.



**Signature**



### FEEDBACK FORM

Name of the Student: Dr Tanisha Soni

Name of the Organization in Which Dissertation Has Been Completed: IHMR Delhi

Area of Dissertation: The Role of Data Security in Indian Healthcare Sector

Attendance: 90%

Objectives achieved: Successful in completing the research.

Deliverables: did a secondary research & completed the report.

Strengths: Sincere, Hardworking.

Suggestions for Improvement: Could have used more publication papers.

Suggestions for Institute (course curriculum, industry interaction, placement, alumni):



Signature of the Officer-in-Charge/ organization Mentor (Dissertation)

Date: 11-07-2024

Place: New Delhi



## Certificate of Approval

The following dissertation titled "**The Role of Data Security in Healthcare- A systematic review**" at "**IIHMR Delhi**" is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of PGDM (Hospital & Health Management) for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation.

Name

Dr. Shiv

Dr. Sukesh

Dr. Nishikant

Signature

Shiv  
Sukesh  
Nishikant

Dissertation Writing

## ACKNOWLEDGEMENT

I would like to express my sincere gratitude and acknowledge the efforts and contributions of everyone involved in the completion of my dissertation.

First and foremost, I would also like to extend my appreciation to the faculty and staff of International Institute of Health Management Research (IIHMR) Delhi for creating an enriching academic environment and for providing the necessary resources and support.

I am deeply grateful for the invaluable guidance and support provided by Dr. Preetha G S throughout the course of this dissertation project. Her expertise and insightful feedback were instrumental in shaping this work.

I am profoundly thankful to my family for unwavering support and encouragement which gave me the strength to persevere. Their belief in my abilities has been a constant source of motivation.

Date: 11-07-2024



Dr Tanisha Soni

[PG/22/134]

## **ABOUT IIHMR DELHI**

The International Institute of Health Management Research (IIHMR), New Delhi is allied to the ‘Society for Indian Institute of Health Management Research’ which was established in October 1984 under the Societies Registration Act-1958. IIHMR-Delhi was set up in 2008 in response to the growing needs of sustainable management and administration solutions critical to the optimal function of the healthcare sector both in India and in the Asia-Pacific region. We are a leading institute of higher learning that promotes and conducts research in health and hospital management; lends technical expertise to policy analysis and formulation; develops effective strategies and facilitates efficient implementation; enhances human and institutional capacity to build a competent and responsive healthcare sector. Our multi-dimensional approach to capacity building is not limited to academic programs but offers management development programs, knowledge and skills-based training courses, seminars/webinars, workshops, and research studies. Our four core activities are... Academic courses at master’s and doctoral level in health and hospital management to meet the growing need of skilled healthcare professionals. Research that has high relevance to health policies and programs at national and global level. Continued education through management development programs and executive programs for working professionals to help them upgrade their knowledge and skills in response to the emerging needs of the industry. Technical consultation to the national and state-level flagship programs to address the gaps in planning as well as implementation.

## **International Institute of Health Management Research, New Delhi (IIHMR-Delhi)**

Over the years IIHMR-Delhi has emerged as an institute of repute both nationally and globally for producing socially conscious, skilled and vibrant top-class health care management professionals. Our graduates are well-matched for the ever-changing health care sector and evolving social milieu. The institute has progressed as a leader in research, teaching, training, community extension programmes and policy advocacy in the field of health care. IIHMR has carved out a niche for itself through its cutting-edge academic curriculum, infrastructure, accomplished multi-disciplinary faculty and research. The Institute as an autonomous body of international stature has been developing leaders for several years to shape tomorrow's healthcare by equipping the students in the fields of health, hospital, and health information technology. The Institute's dynamic health care research programmes provide rigorous training in management, health systems, hospital administration, health care financing, economics, and information technology.

### **Commitment to Inclusive Excellence**

As an institute, IIHMR-Delhi is committed to creating an environment of higher learning that can serve as the model for the kind of society it strives to build – one of equity, social justice and mutual support. We have also made a concerted effort to promote the ethos and philosophies amongst today's students and nurture them into growing as effective managers, to think both critically and ethically, to learn to cope with ethical dilemmas and apply systems-thinking approaches to serious and complex societal problems. Our internationally renowned faculty lead multidisciplinary health research in multifarious areas such as public health, health services, health economics, hospital management, social determinants of health, mental Health and other topics of global and national interest. The IIHMR is invited by various governmental and civil society organizations to provide technical support for

capacity building and policy research needs that culminates in developing innovative and equitable health care strategies and providing advocacy support for health policy and planning. The institute also responds to global health threats, natural disasters, conflict and related humanitarian crises. In addition to the master's and doctoral level programmes, IIHMR-D also offers several highly specialized and popular Management Development Programmes (MDP) to a wide range of health professionals in the country and overseas which largely addresses educational needs amongst in-service aspirants.

As an institute, IIHMR-Delhi is committed to creating an environment of higher learning that can serve as the model for the kind of society it strives to build – one of equity, social justice and mutual support. We have also made a concerted effort to promote the ethos and philosophies amongst today's students and nurture them into growing as effective managers, to think both critically and ethically, to learn to cope with ethical dilemmas and apply systems-thinking approaches to serious and complex societal problems. Our internationally renowned faculty lead multidisciplinary health research in multifarious areas such as public health, health services, health economics, hospital management, social determinants of health, mental Health and other topics of global and national interest. The IIHMR is invited by various governmental and civil society organizations to provide technical support for capacity building and policy research needs that culminates in developing innovative and equitable health care strategies and providing advocacy support for health policy and planning. The institute also responds to global health threats, natural disasters, conflict and related humanitarian crises. In addition to the Masters and doctoral level programmes, IIHMR-D also offers several highly specialized and popular Management Development Programmes (MDP) to a wide range of health professionals in the country and overseas which largely addresses educational needs amongst in-service aspirants.

## **ABSTRACT**

Due to the quick digitization of healthcare services and the increasing sophistication of cyberthreats, data security has taken on a more crucial role in the industry. The numerous facets of data security in the healthcare industry are examined in this systematic overview, including common risks, the consequences of data breaches, regulatory compliance, practical security methods, and technical advancements. Key cyberthreats like malware, phishing, and ransomware are identified in the review, along with insider risks that muddies the security picture. It draws attention to the serious effects that data breaches have on patient privacy, financial security, and company reputation.

To stay compliant, it is crucial to follow legal frameworks including HIPAA, GDPR, PIPEDA, and the Data Protection Act. These frameworks also require ongoing monitoring and adaptation.

Robust data security strategies must include effective security features including encryption, multi-factor authentication (MFA), role-based access controls (RBAC), frequent audits, and employee training. It also looks at how new technologies like blockchain and artificial intelligence (AI) might improve data security.

The review ends with a discussion of upcoming issues and directions, highlighting the necessity of ongoing development of patient-centric security measures, international collaboration, and continual improvement. This thorough research emphasizes that, in the digital age, data security is not just a technological problem but also a vital element of patient care and trust.

# SECTION 1

# **INTRODUCTION**

## **Role of Data Security in Healthcare**

Data security in healthcare is a critical issue as the sensitive nature of medical records and the increasing digitization of healthcare systems. Ensuring the protection of patient information is paramount for maintaining patient trust, adhering to legal requirements, and safeguarding against cyber threats.

When we visit the doctor, ask for medication, or sign up for surgery, we give healthcare organizations important data even if we don't realize it. For example, when we sign up for an appointment to get antibiotics, we also give healthcare organizations data regarding our current diet, our health concerns, and what type of medication we're likely to take soon.

Healthcare data encompasses a wide range of sensitive information, including personal identification details, medical histories, treatment plans, genetic data, and financial information. Given the nature of this data, it is not only valuable but also highly sought after by cybercriminals. The consequences of a data breach in the healthcare sector can be dire, affecting patient privacy, financial stability, and the overall trust in healthcare systems. Thus, ensuring the security of healthcare data is of paramount importance.

Digital data in healthcare is a double-edged sword. While on the one hand, digitalization has allowed for a wide variety of advancements, including teleconsultations, easy retrieval, and duplication of data for records, and development of applications such as machine learning, it has



also allowed for the possibility that the personal medical records of a patient can be accessed by several individuals.

The current trend toward digitizing healthcare workflows and moving to electronic patient records has seen a paradigm shift in the healthcare industry. The quantity of clinical data that is available electronically will then dramatically increase in terms of complexity, diversity, and timeliness, resulting in what is known as big data. It holds the promise of supporting a wide range of unprecedented opportunities and use cases, including these key examples: clinical decision support, health insurance, disease surveillance, population health management, adverse events monitoring, and treatment optimization for diseases affecting multiple organ systems.

The adoption of electronic health records (EHRs), telemedicine, and various digital health solutions has significantly enhanced the efficiency, accessibility, and quality of healthcare delivery. These advancements facilitate seamless data sharing among healthcare providers, improve patient outcomes through better data management, and enable remote patient monitoring and consultations, especially critical during events like the COVID-19 pandemic. However, this digital shift also introduces substantial risks related to the security of sensitive health information.

### **Importance of Data Security in Healthcare**

Data security in healthcare is crucial for many reasons:

- **Patient Privacy:** Protecting patient data ensures that personal health information is kept confidential, fostering a trusting relationship between patients and healthcare providers.
- **Legal and Regulatory Compliance:** Healthcare organizations must comply with various

regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. Non-compliance can result in significant penalties and legal consequences.

- **Operational Integrity:** Data breaches can disrupt healthcare operations, leading to potential delays in patient care, financial losses, and damage to the organization's reputation.
- **Financial Security:** Protecting data helps prevent financial losses from ransomware attacks, fraud, and other cyber threats.

Every country in the world has acknowledged that patient privacy is the most significant issue and jurisdiction, and that safeguarding people's privacy must be done at any costs. The fundamental right to privacy belongs to all people. Many countries place a high priority on privacy policies, notably in the USA and Europe. Well-known laws such as GDPR and HIPAA provide people assurance about their privacy concerns and help them build trust.

India also has access to large amounts of unstructured healthcare data. Furthermore, there may be privacy violations because of the issues with data transformation and storage.

# **SECTION-2**

## **RATIONALE**

Healthcare data security is a critical issue that has wide-ranging effects on patient safety, adherence to the law, and the integrity of healthcare institutions overall. Because it deals with such sensitive data financial, medical, and personal identity details the healthcare sector is a prime target for cyberattacks.

### **Need for a Systematic Review**

A systematic review on the role of data security in healthcare is necessary to provide a comprehensive and evidence-based understanding of the current landscape. It will address several critical questions:

#### **□ Challenges in Data Security:**

- Identifying the specific challenges healthcare institutions face in ensuring data security will help in understanding the root causes of vulnerabilities and breaches.

#### **□ Effectiveness of Current Measures:**

- Evaluating the effectiveness of existing data security measures will provide insights into what is working well and where there are gaps.

#### **□ Strategies and Technologies:**

- Documenting and analysing the various strategies and technologies currently employed in healthcare data security will offer a benchmark for best practices.

#### □ **Future Directions:**

- Identifying future directions for improving data security will ensure that healthcare institutions are prepared to address emerging threats and challenges.

### **Research Gaps and Contributions**

Existing literature on data security in healthcare often focuses on specific aspects such as technology adoption, regulatory compliance, or case studies of breaches. However, there is a need for a comprehensive review that synthesizes these disparate studies into a cohesive understanding of the broader landscape. This systematic review aims to fill this gap by:

#### **1. Integrating Diverse Perspectives:**

- Bringing together findings from numerous studies to provide a holistic view of the state of data security in healthcare.
- Highlighting common themes and identifying unique challenges across different healthcare settings.

#### **2. Providing Evidence-Based Recommendations:**

- Offering practical, evidence-based recommendations for healthcare managers and policymakers to enhance data security.
- These recommendations will be grounded in a thorough analysis of the current challenges, strategies, and effectiveness of existing measures.

### **3. Guiding Future Research:**

- Identifying areas where further research is needed to advance the understanding and practice of data security in healthcare.
- Encouraging the exploration of innovative solutions and emerging technologies to address ongoing and future security challenges.

### **OBJECTIVES OF THE STUDY**

1. To identify common themes, challenges, and strategies in healthcare data security.
2. To assess the effectiveness of current data security measures in healthcare settings.

# **SECTION 3**

## **METHODOLOGY**

### **RESEARCH DESIGN:**

This research is conducted as a systematic review. This methodology involves a structured and comprehensive approach to identifying, evaluating, and synthesizing relevant research studies and data sources.

This methodical approach will be applied to the study of the function of data security in the healthcare industry.

### **RESEARCH QUESTION:**

What strategies and technologies are currently used in healthcare institutions to protect healthcare data?

### **SEARCH STRATEGY:**

Secondary research methods have been the focus of this report's search. Data will be acquired through analysis of research papers available on sites such as PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar for the relevant literature on the data privacy in healthcare.

The review limiting to text between 2020 and 2024 for the relevant literature on the data privacy in healthcare. Publications are meticulously selected to incorporate a wide range of contexts within the data security in healthcare, ensuring comprehensive coverage of the topic.



Data security, healthcare, data protection, cybersecurity, electronic health records, patient information, and HIPAA compliance would be certain combination of keywords that would be use for the search.

The study would ensure that analysis and interpretation of data contains authentic and relevant information, allowing the formulation of informed insights and conclusions.

### **KEYWORDS:**

Data security, healthcare, data protection, cybersecurity, electronic health records, patient information, and HIPAA compliance are certain combinations of keywords.

### **STUDY DURATION:**

2020-2024

### **STUDY POPULATION:**

### **INCLUSION CRITERIA:**

- Recent articles are included focusing on data security in healthcare that are published in peer-reviewed journals.

### **EXCLUSION CRITERIA:**

- Articles that do not specifically address data security and is not peer-reviewed are excluded.
- Studies lacking relevance to the research question and objectives are outlined in the systematic review.
- Publications containing outdated information regarding healthcare data security, particularly those published before 2020

# **SECTION 4**

## **RESULTS**

This systematic review's results section offers a thorough examination of the research findings from the chosen papers and other literature about data security in healthcare.

The key results are categorized into:

- The types of data security threats
- The impact of data breaches on healthcare
- Regulatory frameworks, security measures, and technological innovations in the healthcare sector.
- Trends in Healthcare data breach statistics

### **I. Type of Data Security Threats:**

<b>Cyber Attacks</b>	<ul style="list-style-type: none"><li>• <b>Ransomware:</b> A ransomware assault involves the employment of software by a hacker to take over a computer or network, after which the perpetrator demands a ransom to unlock the affected system.  According to studies, the frequency of ransomware attacks in the healthcare industry has increased, tripling between 2017 and 2022.</li><li>• <b>Phishing:</b> involves a hacker deceiving someone into disclosing confidential information. They entice the person by posing as a dependable friend, associate, or business associate.</li><li>• <b>Malware:</b> Malware that includes trojans and worms has been a cause for 25% of data breaches. These malicious software</li></ul>
----------------------	--

	<p>applications can penetrate healthcare systems and seriously compromise the availability and integrity of data.</p>
<p><b>Insider Threats</b></p>	<ul style="list-style-type: none"> <li>• <b>Intentional Insider Threats:</b> In the healthcare industry, acts like data theft or sabotage make up almost 15% of all data breaches. Because insiders are trusted, it is difficult to identify and stop these dangers.</li> <li>• <b>Unintentional Insider Threats:</b> Roughly 20% of data breaches are caused by human mistakes, which includes configuration issues and unintentional data sharing. One of the main contributing factors to these accidents is staff members' inadequate training and awareness.</li> </ul>
<p><b>Data Interception</b></p>	<ul style="list-style-type: none"> <li>• A serious risk that has been recognized is the interception of health data in transit, particularly when encryption is not used correctly. Research indicates that 10% of unencrypted data transmissions are intercepted, which can result in data breaches and unauthorized access.</li> </ul>

## II. **Data Breaches Impact:**

The analysis emphasized the various ways that data breaches affect the healthcare industry:

- **Patient Privacy:**

In addition to jeopardizing patient confidentiality, data breaches can result in fraud, identity theft,

and other types of personal injury. According to the review, 60% of patients impacted by data breaches had their personal information misused in some way.

- **Financial Cost:**

Data breaches have serious financial repercussions. IBM's 2022 analysis indicated that the average cost of a healthcare data breach was \$9.23 million. This covers expenditures for penalties, legal fees, breach mitigation, and recovery initiatives.

- **Damage of reputation:**

Healthcare firms suffer severe reputational damage because of data breaches. According to the review, there is frequently a 5–10% decrease in patient trust and retention in firms that have data breaches. The long-term viability and success of the organization may be affected by this lack of trust.

### III. **Regulatory Frameworks:**

Different types of regulatory frameworks of data security in healthcare across various countries:

Country/Region	Data Security Measures	Description
United States	HIPAA Compliance	Administrative, physical, and technical safeguards to protect health information.
	HITECH Act	Promotes EHR adoption and enhances HIPAA protections.

	NIST Cybersecurity Framework	Guidelines for preventing, detecting, and responding to cyber-attacks.
<b>European Union</b>	General Data Protection Regulation (GDPR)	Comprehensive data protection framework including consent, access, erasure, and breach notification.
	ENISA	Supports policy development and collaboration on cybersecurity.
	ISO/IEC 27001	International standard for information security management.
<b>United Kingdom</b>	Data Protection Act 2018	Enacts GDPR into UK law with specific provisions.
	NHS Data Security and Protection Toolkit	Self-assessment tool for measuring data security performance.
<b>Canada</b>	PIPEDA	Regulates how private sector organizations handle personal information.
	Provincial Regulations	Additional regulations, e.g., Ontario's PHIPA.
<b>Australia</b>	My Health Records Act 2012	Regulates health information in the My Health Record system.

	Privacy Act 1988	Regulates handling of personal information by government and private sectors.
<b>Japan</b>	Cybersecurity Strategy	Guidelines for securing healthcare data developed by NISC.
	Act on the Protection of Personal Information (APPI)	Requires protection of personal information from leaks, loss, or damage.
<b>Middle East (e.g., UAE)</b>	Health Information Law (Dubai)	Regulates the use and security of health data with measures like encryption and access controls.
	General Data Protection Law (Abu Dhabi)	Aligns with international standards like GDPR, focusing on consent, data minimization, and security.

#### **IV. TRENDS IN HEALTHCARE DATA BREACH STATISTICS (U.S. & INDIA)**

Over the last 14 years, there has been an increasing trend in the number of data breaches; in 2021, more data breaches were recorded than in any other year since OCR (Office for Civil Rights) began publishing information in United States.

In 2022, there was an upsurge in data breaches once more, with 720 data breaches involving 500 or more records reported to OCR. Cyberattacks on healthcare institutions in United States continued uninterrupted in 2023, setting two new records: the highest number of reported data breaches and the

highest number of breaches overall. Over 133 million records were exposed or improperly released in 725 data breaches that were reported to OCR in 2023.

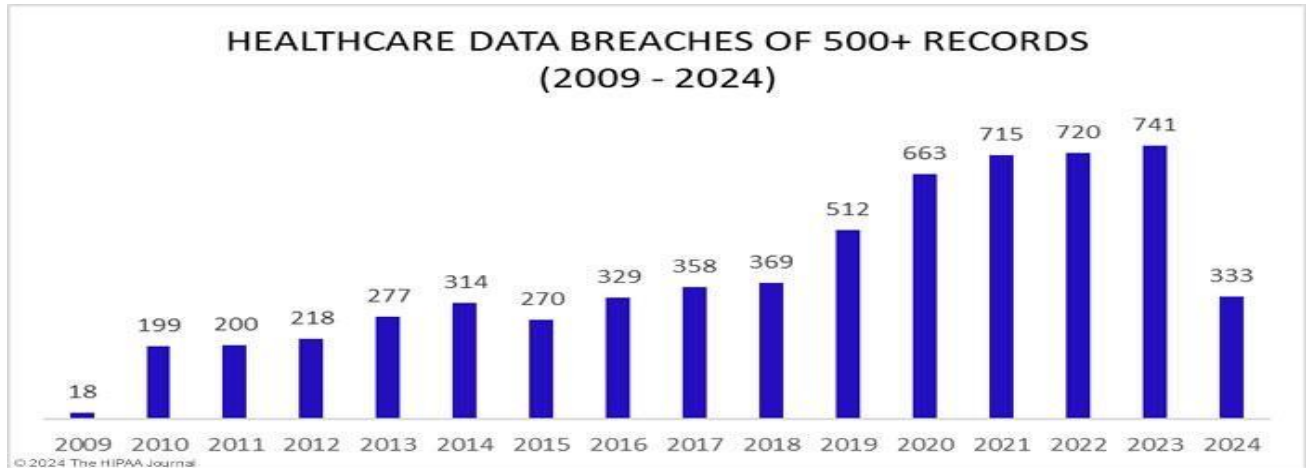


Figure 4.1: Healthcare data breaches in United States(2009-2024)

There were 5,887 healthcare data breaches involving 500 or more records reported to OCR between 2009 and 2023. 519,935,970 healthcare records have been exposed or improperly disclosed because of the breaches. That is equivalent to over 1.5 times the population of the US. A healthcare data breach involving 500 or more records was reported every day on average in 2018. After five years, the rate has increased by almost 100%. In 2023, there were 1.99 recorded daily healthcare data breaches of 500 or more records, and each day there were 364,571 healthcare record breaches on average.

## V. TRENDS IN CYBER ATTACKS ON INDIAN HEALTHCARE INDUSTRY



According to cyber security intelligence company CloudSEK, India saw 7.7% of all cyberattacks against the healthcare sector in 2021, making it the country with the second-highest frequency of attacks worldwide.

The US healthcare industry was targeted by 28% of all cyberattacks worldwide, according to a CloudSEK analysis titled "Increased Cyberattacks on the Global Healthcare Sector."

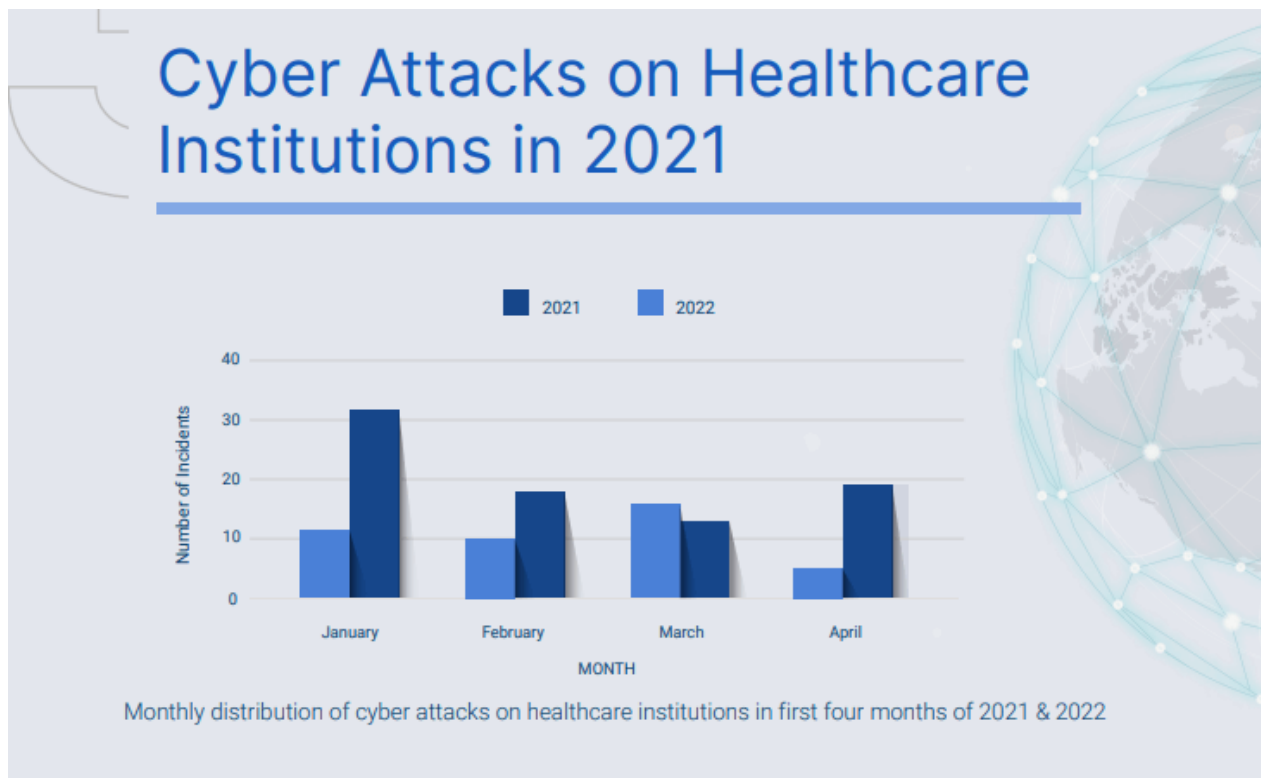
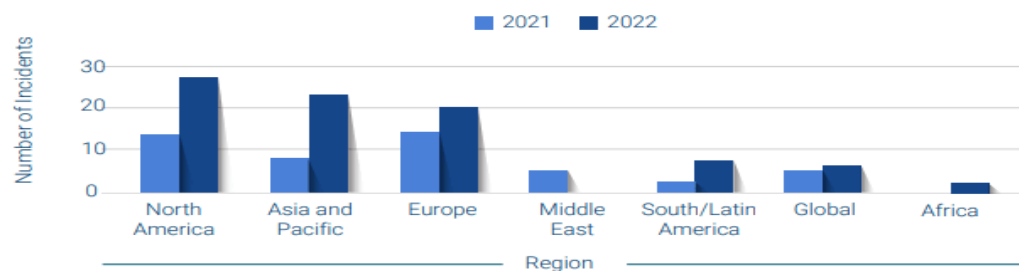
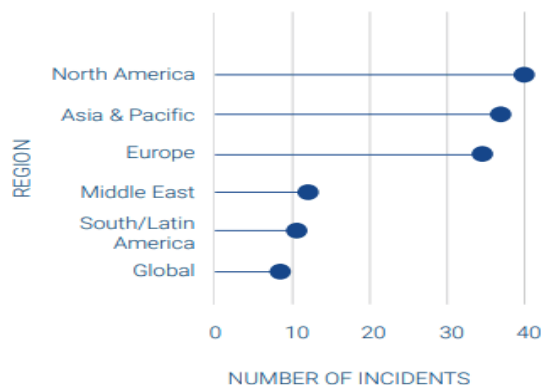


Figure 4.2: Cyber Attacks on Healthcare Institutions in 2021 and 2022



Region wise number of recorded cyberattacks targeting the healthcare sector in first four months of 2021 and 2022



Region wise number of recorded cyberattacks targeting the healthcare sector in 2021

**32.1%**

of total attacks recorded worldwide in 2022 occurred in the USA.

**7.1%**

India, China, and Italy tied for the second place, with each having 7.1% of total attacks.

Figure 4.3: Region wise number of cyberattacks targeting healthcare sector in 2021

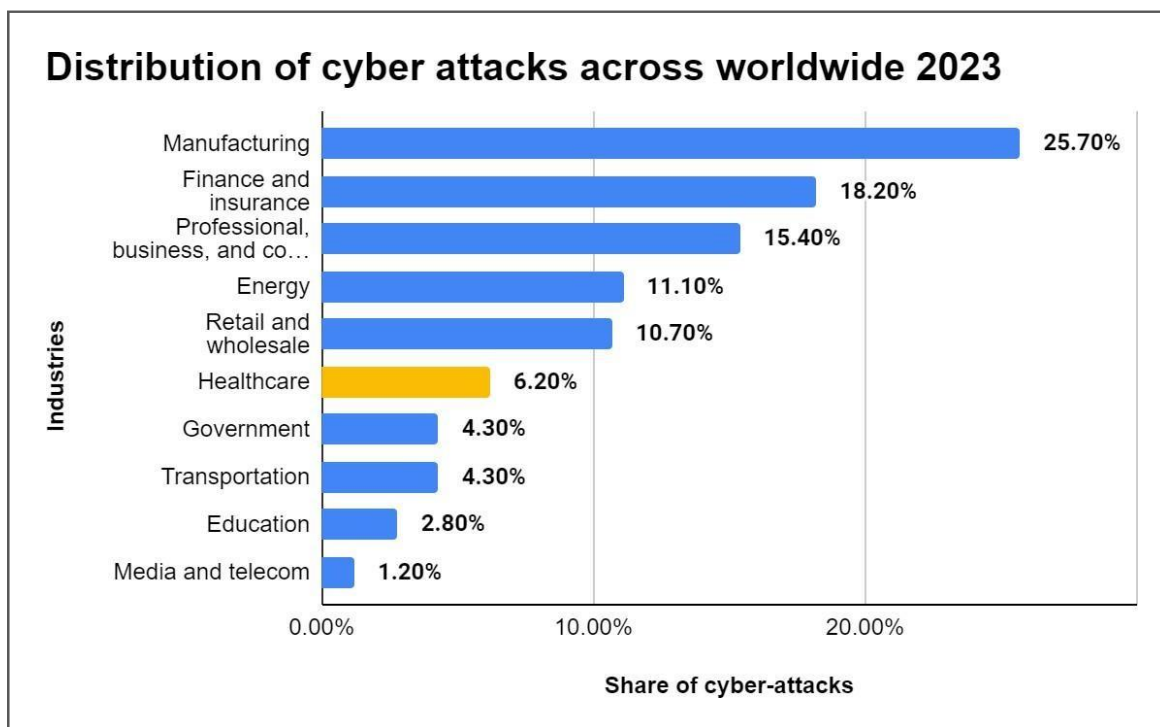


Figure 4.4: Distribution of Cyberattacks worldwide (2023)

Among the top global industries in 2023, cyberattacks affected the manufacturing sector the most. In the year under review, manufacturing firms experienced over 25% of all cyberattacks. At about 18%, finance and insurance companies were next. Third place went to professional, business, and consumer services, with 15.4% of cyberattacks reported.

# SECTION 5

## **DISCUSSION**

The discussion part provides an interpretation of the systematic review's findings, emphasizing the consequences for healthcare organizations, the efficacy of the available data security solutions, and potential future paths for this field's practice and study.

To improve cyber security in this crucial industry, this discussion section explores the issues in more detail and offers some possible solutions.

Some Challenges that are curveballs in the data security in healthcare industry and the recommendations to those:

Challenges	Description
<b>Complex IT Environments</b>	Healthcare facilities often operate within intricate IT ecosystems, comprising numerous interconnected devices, software applications, and databases. This complexity increases the potential attack surface for cyber threats and makes it challenging to secure all components effectively.
<b>Regulatory Compliance</b>	Complying with stringent data protection regulations requires healthcare organizations to implement comprehensive security measures, conduct regular audits, and maintain documentation. These tasks demand significant resources and ongoing vigilance.
<b>Cyber Threats</b>	The healthcare sector is a lucrative target for cybercriminals due to the high value of health data on the black market. Common threats include ransomware attacks, phishing schemes, malware infections, and insider threats. These threats are continually evolving, becoming more sophisticated and harder to detect.

<b>Resource Constraints</b>	Many healthcare organizations, particularly smaller clinics and rural hospitals, often struggle with limited financial and human resources. This constraint makes it difficult to invest in advanced security technologies, hire skilled IT personnel, and conduct regular security training for staff.
-----------------------------	---

Recommendations	Examples
<p><b><u>Adopt a Multi-Layered Security Approach</u></b></p> <p>Implement multiple layers of security controls to protect data at various points in the system. This includes firewalls, intrusion detection systems, encryption, and secure access controls.</p>	Using encryption for data in transit and at rest, combined with strong access controls and regular system monitoring.
<p><b><u>Invest in Advanced Cybersecurity Technologies</u></b></p> <p>AI for threat detection, blockchain for secure data sharing, and biometric authentication.</p>	Implementing AI-driven systems that can detect unusual activity and alert security teams in real-time
<p><b><u>Regular Security Training for Staff</u></b></p> <p>Provide ongoing training and awareness programs for all healthcare staff on the importance of data security and best practices.</p>	Conducting quarterly training sessions on phishing awareness and secure password practices.

<p><b><u>Perform Regular Security Audits and Assessments</u></b></p> <p>Conduct regular internal and external security audits to identify and address vulnerabilities.</p>	<p>Hiring external cybersecurity firms to perform penetration testing and vulnerability assessments.</p>
--	--

In the case of healthcare information systems, it must be mandatory to adopt all appropriate safety measures to protect the most important data ever.

- **IMPLICATIONS**

<b>For Healthcare Management</b>	<b>For Policy Makers</b>
<p>Healthcare management will gain evidence-based insights into data security practices from this review's conclusions. To successfully protect patient information, this knowledge will help prioritize expenditures in technology, training, and policy development.</p>	<p>Policy makers will benefit from the review's recommendations, which will inform the development of regulations and guidelines that address the evolving data security landscape in healthcare.</p>

# **SECTION 6**



## **CONCLUSION**

The systematic study highlights that even while health data security has come a long way, ongoing work is still required to improve security protocols and counter new threats. Healthcare institutions need to take a proactive, all-encompassing approach to data security, incorporating cutting-edge technology, thorough personnel training, and strict regulatory compliance. To create and execute efficient data security solutions in the constantly changing digital ecosystem, collaboration between healthcare providers, technology developers, and regulatory agencies is essential.

Overall, the research indicates that cyber security is a continuous effort rather than a one-time fix for healthcare industry. Here, a multifaceted approach is needed, including raising awareness among healthcare institutions, updating infrastructure, securing apps, working with stakeholders, and fortifying the regulatory environment. In the digital age, healthcare organizations may safeguard confidential patient information, guarantee the provision of critical services, and cultivate patient trust by placing a high priority on cyber security.

In conclusion, data security in healthcare is an essential element of patient care and trust, not only a technical problem. Healthcare companies may preserve patient confidence, guarantee regulatory compliance, and safeguard patient information by making data security a top priority.

Maintaining a commitment to data security will help the healthcare industry safely traverse the challenges of the digital era while maintaining its high standard of care.

## **REFERENCES**

1. Churi P, Pawar A, Moreno-Guerrero AJ. A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study. *Inventions*. 2021 Sep;[cited 2024 May 17]. Available from: <https://www.mdpi.com/2411-5134/6/3/45>
2. Aravamudhan P, T K. A novel adaptive network intrusion detection system for internet of things. *PLoS One*. 2023 Apr 21;[cited 2024 May 17]18(4):e0283725. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10121003/>
3. Prasuna A, Rachh A. A study on challenges of data security and data privacy in the healthcare sector: Swot analysis. *Asia Pacific Journal of Health Management*. 2023 Mar;[cited 2024 May 4]18(1):283–9. Available from: <https://search.informit.org/doi/abs/10.3316/informit.014727326511420>
4. Nirmala AP, Asha V, Ramesh BN, Chandana K, Chandana GR, Alam A. A Systematic Review on classification of Cyber Attacks and its Prevention techniques to improve Cyber Security. In: 2023 International Conference on Computer Communication and Informatics (ICCCI) [Internet]. 2023 [cited 2024 May 4]. p. 1–6. Available from: <https://ieeexplore.ieee.org/abstract/document/10128642>
5. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*. 2022 Nov [cited 2024 May 4]1;34(10, Part A):8176–206. Available from: <https://www.sciencedirect.com/science/article/pii/S1319157822002762>
6. Vijarania M, Gupta S, Agrawal A, Misra S. Achieving Sustainable Development Goals in Cyber Security Using AIoT for Healthcare Application. In: Misra S, Siakas K, Lampropoulos G, editors. *Artificial Intelligence of Things for Achieving Sustainable Development Goals* [Internet]. Cham: Springer Nature Switzerland; 2024 [cited 2024 May 4]. p. 207–31. Available from: [https://doi.org/10.1007/978-3-031-53433-1\\_11](https://doi.org/10.1007/978-3-031-53433-1_11)
7. Najjar AA, Naik S M. Covid-19 Impact on Cyber Crimes in India: A Systematic Study. In: 2022 IEEE India Council International Subsections Conference (INDISCON) [Internet]. 2022 [cited 2024 May 4]. p. 1–8. Available from: <https://ieeexplore.ieee.org/abstract/document/9862935>
8. Sharma A, Gupta S. Cyber Crimes during COVID-19 Pandemic in India and World. *Supremo Amicus*. 2022; [cited 2024 May 4]; 29:[147]. Available from: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/supami29&div=16&id=&page=>
9. Chithaluru P, Tanwar R, Kumar S. Cyber-Attacks and Their Impact on Real Life: We

Do About Them? In: Information Security and Optimization. Chapman and Hall/CRC; 2021.

10. Chandani P, Rajagopal S, Bishnoi AK, Verma V. Cyber-Physical System and AI Strategies for Detecting Cyber Attacks in Healthcare. *International Journal of Intelligent Systems and Applications in Engineering*. 2023 Jul 11;11(8s):55–61.
11. Bhukya CR, Thakur P, Mudhivarthi BR, Singh G. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. *Sensors (Basel)*. 2023 Sep 27;23(19):8107.
12. Mohamad Al-Aboosi AM, Huda Sheikh Abdullah SN, Murah MZ, AL Dharhani GS. Cybersecurity Trends in Health Information Systems. In: 2022 International Conference on Cyber Resilience (ICCR) [Internet]. 2022 [cited 2024 May 4]. p. 01–4. Available from: <https://ieeexplore.ieee.org/abstract/document/9995952>
13. Chintala SK. DATA PRIVACY AND SECURITY CHALLENGES IN AI-DRIVEN HEALTHCARE SYSTEMS IN INDIA.
14. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel)*. 2020 May 13[cited 2024 May 4];8(2):133. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/>
15. Statista [Internet]. [cited 2024 May 4]. India: regulation impact on cybersecurity 2023. Available from: <https://www.statista.com/statistics/1428306/india-impact-of-regulations-on-cybersecurity/>
16. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors (Basel)*. 2021 Mar 5;21(5):1809.
17. Dubey A, Tiwari G, Dixit A, Mishra A, Pandey M. Leveraging Innovative Technologies for Ransomware Prevention in Healthcare: A Case Study of AIIMS and Beyond. In: Chaturvedi A, Hasan SU, Roy BK, Tsaban B, editors. *Cryptology and Network Security with Machine Learning*. Singapore: Springer Nature; 2024. p. 711–30.
18. Making India's healthcare sector cybersecurity - ProQuest [Internet]. [cited 2024 May 5]. Available from: <https://www.proquest.com/docview/2874610517/citation/AF230932D6ED4177PQ/1?sourcetype=Trade%20Journals>
19. Overcoming cybersecurity challenges in healthcare - ProQuest [Internet]. [cited 2024 May 5]. Available from: <https://www.proquest.com/docview/2814599977/AF230932D6ED4177PQ/2?sourcetype=Trade%20Journals>
- Studies [Internet]. [cited 2024 May 4];1(1). Available from: <https://hcommons.org/deposits/item/hc:43075/>
20. Kakarla S, Rao DN, Kakarla G, Gorla S. Statistical Trend in Cyber Attacks and

Security Measures. In: Computational Intelligent Security in Wireless Communications. CRC Press; 2023[cited 2024 May 17]. Available from: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003323426-14/statistical-trend-cyber-attacks-security-measures-shirisha-kakarla-deekonda-narsinga-rao-geeta-kakarla-srilatha-gorla>

21. Dhanare R, Sharma PC, Kumar Srivastava D. Vulnerabilities, Attacks and Solutions of Cybersecurity in Medical Domain. In: 2021 International Conference on Computational Performance Evaluation (ComPE) [Internet]. 2021 [cited 2024 May 4]. p. 034–9. Available from: [https://ieeexplore.ieee.org/abstract/document/9751911\(1\)](https://ieeexplore.ieee.org/abstract/document/9751911(1))
22. Statista [Internet]. [cited 2024 May 5]. Cyber attacks in healthcare sector worldwide by type 2022. Available from: <https://www.statista.com/statistics/1362863/cyber-attacks-on-healthcare-organizations-worldwide-by-type/>
23. Statista [Internet]. [cited 2024 May 5]. Cybersecurity: market data & analysis. Available from: <https://www.statista.com/study/124902/cybersecurity-report/>
24. IBM Newsroom [Internet]. [cited 2024 May 5]. IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. Available from: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>
25. IBM India News Room [Internet]. 2019 [cited 2024 May 17]. IBM Report: Average cost of a data breach in India touched INR 179 million in 2023. Available from: <https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023>
26. Data Security Council of India (DSCI) [Internet]. 2023 [cited 2024 May 17]. DSCI: India Cyber Threat Report. Available from: [https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023\\_0.pdf](https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf)
27. Statista [Internet]. [cited 2024 May 5]. India: estimated cybersecurity market size 2028. Available from: <https://www.statista.com/statistics/1197074/india-estimated-cybersecurity-market-size/>
28. Statista [Internet]. [cited 2024 May 5]. India: government spending on cybersecurity 2023. Available from: <https://www.statista.com/statistics/1428411/india-government-spending-on-cybersecurity/>
29. Statista [Internet]. [cited 2024 May 17]. Global cyberattacks in industries 2023. Available from: <https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>
30. Statista [Internet]. [cited 2024 May 5]. India: number of cyber crimes related to data theft 2022. Available from: <https://www.statista.com/statistics/875925/india-number-of-cyber-crimes-related-to-data-theft/>
31. Statista [Internet]. [cited 2024 May 5]. India: number of digital forgery incidents by leading state 2022. Available from: <https://www.statista.com/statistics/1098541/india->

[number-of-digital-forgery-incidents-by-leading-state/](#)

32. 5 cyber security trends that we may see in 2024. The Times of India [Internet]. 2024 Jan 24 [cited 2024 May 5]; Available from: <https://timesofindia.indiatimes.com/gadgets-news/5-cyber-security-trends-for-2024-insights-and-predictions/articleshow/107093195.cms>
33. Statista [Internet]. [cited 2024 May 5]. India: opinion on cybersecurity budgets in 2024. Available from: <https://www.statista.com/statistics/1349789/india-opinion-on-cybersecurity-budgets/>
34. Statista. [cited 2024 May 5]. Topic: Cyber crime in India. Available from: <https://www.statista.com/topics/5054/cyber-crime-in-india/>
35. Cybersecurity is a requisite for unleashing 5G's potential in healthcare | McKinsey [Internet]. [cited 2024 May 5]. Available from: <https://www.mckinsey.com/br/en/our-insights/all-insights/ciberseguranca-e-condicao-para-destravar-potencial-da-saude-com-5g>
36. Cybersecurity trends: Looking over the horizon | McKinsey [Internet]. [cited 2024 May 5]. Available from: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon>
37. 5 cyber security trends that we may see in 2024. The Times of India [Internet]. 2024 Jan 24 [cited 2024 May 5]; Available from: <https://timesofindia.indiatimes.com/gadgets-news/5-cyber-security-trends-for-2024-insights-and-predictions/articleshow/107093195.cms>
38. (6) Healthcare Sector is the Biggest Target for Cyber Attacks | LinkedIn [Internet]. [cited 2024 May 5]. Available from: <https://www.linkedin.com/pulse/healthcare-sector-biggest-target-cyber-attacks-prof-r-s-nehra/>
39. Biggest Healthcare Industry Cyber Attacks | Arctic Wolf [Internet]. [cited 2024 May 5]. Available from: <https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/>
40. Lohchab H. Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: report. The Economic Times [Internet]. 2023 Nov 3 [cited 2024 May 5]; Available from: <https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr>
41. Digital India Act: Here's how it should fix India's cybersecurity weaknesses [Internet]. [cited 2024 May 5]. Available from: <https://www.moneycontrol.com/news/opinion/digital-india-act-heres-how-it-should-fix-indias-cybersecurity-weaknesses-11038701.html>
42. Business Today [Internet]. 2023 [cited 2024 May 5]. India is the 10th most affected country by cyberattacks in 2022 with healthcare sector most impacted: Report. Available from: <https://www.businesstoday.in/technology/news/story/india-is-the-10th-most-affected-country-by-cyberattacks-in-2022-with-healthcare-sector-most->

43. Ahaskar A. mint. 2022 [cited 2024 May 5]. Indian healthcare sector suffers 1.9 million cyberattacks in 2022. Available from: <https://www.livemint.com/technology/tech-news/indian-healthcare-sector-suffers-1-9-million-cyberattacks-in-2022-11669878864152.html>
44. Standard B. Indian websites faced over 5 billion cyberattacks in 2023, shows data [Internet]. 2024 [cited 2024 May 5]. Available from: [https://www.business-standard.com/india-news/indian-websites-faced-over-5-billion-cyberattacks-in-2023-shows-data-124021501548\\_1.html](https://www.business-standard.com/india-news/indian-websites-faced-over-5-billion-cyberattacks-in-2023-shows-data-124021501548_1.html)
45. Ford N. IT Governance UK Blog. 2024 [cited 2024 May 5]. List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached. Available from: <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>
46. Page not found [Internet]. IHF. [cited 2024 May 5]. Available from: <https://ihf-fih.org/artificial-intelligence-and-cybersecurity-in-healthcare/>
47. Ransomware is highest cyber threat in India: Report – India TV [Internet]. [cited 2024 May 5]. Available from: <https://www.indiatvnews.com/technology/news/ransomware-is-highest-cyber-threat-in-india-report-2024-03-21-922569>
48. 5 Ways Indian Medical Administrations Can Boost Hospital Cyber-security - Forbes India [Internet]. [cited 2024 May 5]. Available from: <https://www.forbesindia.com/article/iim-calcutta/5-ways-indian-medical-administrations-can-boost-hospital-cybersecurity/84397/1>
49. Desk DW. Deccan Herald. [cited 2024 May 5]. Data of 81.5 crore citizens up for sale in “biggest” data breach in India: Report. Available from: <https://www.deccanherald.com/india/data-of-815-crore-citizens-up-for-sale-in-biggest-data-breach-in-india-report-2749794>
50. Statista [Internet]. [cited 2024 May 5]. India: number of cyber crimes related to data theft 2022. Available from: <https://www.statista.com/statistics/875925/india-number-of-cyber-crimes-related-to-data-theft/>
51. Indian Government Doubles Cybersecurity Funding from Rs 400 Cr to Rs 750 Cr in 2024 Interim Budget: Industry Leaders Strongly Advocate [Internet]. [cited 2024 May 17]. Available from: <https://cxotoday.com/specials/indian-government-doubles-cybersecurity-funding-from-rs-400-cr-to-rs-750-cr-in-2024-interim-budget-industry->

## ORIGINALITY REPORT

11%

SIMILARITY INDEX

%

INTERNET SOURCES

7%

PUBLICATIONS

8%

STUDENT PAPERS

## PRIMARY SOURCES

1

Submitted to Cypress College

Student Paper

2%

2

Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, Mostafa Saadi. "Big data security and privacy in healthcare: A Review", Procedia Computer Science, 2017

Publication

1%

3

Submitted to Truckee Meadows Community College

Student Paper

1%

4

Submitted to University of Gloucestershire

Student Paper

1%

5

"Cryptography and Network Security with Machine Learning", Springer Science and Business Media LLC, 2024

Publication

1%

6

Shabnam Kumari, Aderonke Thompson, Shrikant Tiwari. "chapter 7 Cyber Security in Internet of Things-Based Edge Computing", IGI Global, 2024

Publication

1%

7	Anubhav Gupta, Ankur Sharma, Deepak Kumar Jha. "Overcoming Obstacles STEP By STEP: A Comprehensive Review of Challenges and Strategies in Implementing Hospital Management Information Systems in India", Springer Science and Business Media LLC, 2024 Publication	1%
8	Submitted to American Public University System Student Paper	<1%
9	Submitted to Herzing University Student Paper	<1%
10	Shishir Kumar Shandilya, Agni Datta, Yash Kartik, Atulya Nagar. "Digital Resilience: Navigating Disruption and Safeguarding Data Privacy", Springer Science and Business Media LLC, 2024 Publication	<1%
11	Submitted to University College Dublin (UCD) Student Paper	<1%
12	Submitted to University of Ulster Student Paper	<1%
13	Submitted to Symbiosis International University Student Paper	<1%



14 Muhammad Shahzad Aslam, Saima Nisar. "chapter 14 Policy Guidelines Post ChatGPT Era in Education, Research, and Public Administration", IGI Global, 2023  $<1\%$

---

Publication

15 R. Anitha, M. Rajkumar, B. Jothi, H. Mickle Aancy, G. Sujatha, B. Sam. "chapter 10 Convergence of AI and Self-Sustainability", IGI Global, 2024  $<1\%$

---

Publication

16 Julija Gavėnaitė-Sirvydienė. "Development of cyber security assessment tool for financial institutions", Vilnius Gediminas Technical University, 2024  $<1\%$

---

Publication

17 Meenu Vijarania, Swati Gupta, Akshat Agrawal, Sanjay Misra. "Chapter 11 Achieving Sustainable Development Goals in Cyber Security Using AIoT for Healthcare Application", Springer Science and Business Media LLC, 2024  $<1\%$

---

Publication

---

Exclude quotes On

Exclude matches Off

Exclude bibliography On



INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH (IIHMR)  
Plot No. 3, Sector 18A, Phase- II, Dwarka, New Delhi- 110075  
Ph. +91-11-30418900, [www.iihmrdelhi.edu.in](http://www.iihmrdelhi.edu.in)

### CERTIFICATE ON PLAGIARISM CHECK

Name of Student (in block letter) Dr/Mr./Ms.:

Enrolment/Roll No.	PG/22/ 134	Batch Year	2022-2024
Course Specialization (Choose one)	Hospital Management	Health Management	Healthcare IT
Name of Guide/Supervisor	Dr/ Prof.: Preetha G S		
Title of the Dissertation/Summer Assignment	The Role of Data security in Healthcare A systematic Review		
Plagiarism detects software used	"TURNITIN"		
Similar contents acceptable (%)	Up to 15 Percent as per policy		
Total words and % of similar contents Identified	11%		
Date of validation (DD/MM/YYYY)			

Guide/Supervisor

Name:

Signature:

Report checked by

Institute Librarian

Signature:

Date:

Library Seal



Student

Name: Dr Tanisha Soni

Signature: Tanisha

Dean (Academics and Student Affairs)

Signature:

Date:

(Seal)