GRIFFITH COLLEGE DUBLIN

Assignment Cover Sheet

Learner name(s):	SALINI CHEMMENGATTUVALAPPIL MOHANDAS
Learner number(s):	[redacted]
Assignment Type:	**Individual:** YES **Group:**
Course:	MSC IN MEDICAL DEVICE TECHNOLOGY AND BUSINESS **Stage/year:** 2025
Module:	DISSERTATION
Study Mode:	Full time YES Part-time
Lecturer Name:	MINA GHAHREMANZAMANEH
Assignment Title:	UNMASKING INSIDER THREATS IN ELECTRONIC HEALTH RECORDS (EHR): A COMPREHENSIVE ANALYS OF RISKS, IMPACTS, AND STRATEGIC MITIGATION MEASURES FOR ENHANCED HEALTHCARE DATA
No. of pages:	113
Uploaded to Moodle:	Yes ✓ No
Additional Info:	
Date due:	12/05/2025
Date submitted:	12/05/2025

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understood the college policy on plagiarism. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this assignment, or if I have knowingly plagiarised my work or allowed others to plagiarise my work.

I hereby certify that this assignment is my own original work, based on my personal study and/or research, it is all written in my own words and I have acknowledged all references and sources used in its preparation. I also certify that the assignment has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

I have also not used any third parties, AI tools or websites to generate any parts of my assignment.

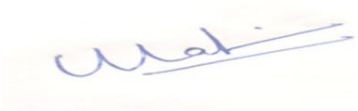
Signed & dated: 

*Please note: Students **MUST** retain a hard / soft copy of **ALL** assignments as well as a receipt issued as proof of submission.*

CANDIDATE DECLARATION

I hereby declare that the dissertation entitled: **"UNMASKING INSIDER THREATS IN ELECTRONIC HEALTH RECORDS (EHR): A COMPREHENSIVE ANALYSIS OF RISKS, IMPACTS, AND STRATEGIC MITIGATION MEASURES FOR ENHANCED HEALTHCARE DATA SECURITY" submitted** in partial fulfilment of MSc in Medical Device Technology and Business is the result of my own work and due acknowledgment is given. I also assure that I have not plagiarised anyone else's work.

Candidate name: SALINI CHEMMENGATTUVALAPPIL MOHANDAS
Date: **12/05/2025**

Candidate Signature: 

Supervisor Name: Mina Ghahremanzamaneh Date: **12/05/2025**

Supervisor signature:

ACKNOWLEDGEMENTS

I want to express my deepest gratitude to God, whose grace and strength have been my guiding force throughout this journey, for which I am eternally thankful.

I would also like to extend my heartfelt gratitude to my supervisor, **Mina Ghahremanzamaneh**, whose invaluable guidance, encouragement, and support have helped me prepare for this work. Your feedback and patience have motivated me to strive for excellence. Thank you for the knowledge and experience you have shared throughout the journey.

I'd like to express my heartfelt gratitude to the Griffith College faculty for building an academic environment that has guided my growth professionally and personally. Your dedication to education and commitment to student success have greatly contributed to my development.

To my parents, words cannot express how thankful I am for your unwavering love, support, and belief in me. Your constant encouragement has been a source of inspiration and strength during even the most challenging times.

Lastly, to my dear friends, thank you for your companionship, understanding, and moral support. Your encouragement have kept me grounded and focused.

SALINI CHEMMENGATTUVALAPPIL MOHANDAS

TABLE OF CONTENTS

DECLARATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	viii
1.INTRODUCTION	1
1.1 Background	1
1.2 Purpose of the study	2
1.3 Research Context	2
1.4 Significance and Justification	3
1.5 Research Objectives	3
1.6 Research Question	3
1.7 Dissertation Structure Overview	4
2. LITERATURE REVIEW	6
2.1 Introduction	6
2.2 Understanding Insider Threats in EHR Security	7
2.2.1 Insider Threat Taxonomies and Classifications	7
2.2.2 Unintentional Insider Threats and AI driven Taxonomy	8
2.2.3 Behavioural analysis and detection of Insider Threats	9
2.2.4 Insider Threats in Healthcare and the need for specialised taxonomy	10
2.3 The Impact of Insider Threats on healthcare institutions	11
2.3.1Financial consequences	11
2.3.2 Regulatory and legal ramifications	14
2.3.3 Operational and reputational damage	16
2.4 Current security measures and their limitations	17
2.4.1 Behavioural Monitoring and User activity tracking	17
2.4.2 Anomaly detection systems	18
2.4.3 Access control and encryption	19
2.5 Suggested mitigation strategies for insider threats	20
2.5.1 Policies and governance	20
2.5.2 Training and awareness programmes	21
2.5.3 Advanced security technologies	21
2.6 Conceptual Framework	22
3. METHODOLOGY	25
3.1 Overview	25
3.2 Research Philosophy and approach	29
3.3 Methodological Choice	30
3.4 Research Strategy	31
3.5 Collection of primary data	33
3.6 Data analysis	34
3.7 Conclusion	35
4. FINDINGS AND ANALYSIS	37
4.1 Overview	37
4.2 Demographics of respondents	37

4.2.1 Jobe Role distribution 37
4.2.2 Experience level of respondents 38
4.2.3 Familiarity and frequency of usage of EHR system 39
4.3 Awareness of Insider threats 41
4.3.1 Insider threats types and its frequency of occurrence 42
4.3.2 Frequency of threat perception 43
4.4 Impact of insider threats 45
4.4.1 Impact distribution 45
4.4.2 Concern about insider threats to patient data security 49
4.4.3 Belief in financial Impact 51
4.4.4 Perceived impact on patient trust 52
4.4.5 Impact of Clinical Quality 53
4.4.6 Impact on Operational Efficiency 54
4.5. Organizational Security Measures for Insider Threat Mitigation 55
4.5.1 Presence of Insider Threat Policies 55
4.5.2 Implemented Security Measures for EHR Protection 56
4.5.3 Perceived Effectiveness of Security Policies 57
4.5.4 Frequency of Security Training 58
4.5.5 Access Control Mechanisms in Use 59
4.5.6 Monitoring Tools for Suspicious Activity 60
4.6 Mitigation Strategies 61
4.6.1 Perceived Effectiveness of Mitigation Strategies Against Insider Threats 61
4.6.2 Additional Strategies 63
4.7 Discussions 65
5.CONCLUSION AND RECOMMENDATIONS 69
5.1 Summary of Main Findings and Their Implications 69
5.2 Summary of Key Differences from Literature 70
5.3 Practical Recommendations 70
5.4 Academic Recommendations 70
5.5 Limitations of the Research 71
5.6 Contributions of the Research 71
5.7 Suggestions for Further Research 71
5.8 Final Reflections 71
REFERENCES 72
APPENDIX A: SURVEY QUESTIONS A1
APPENDIX B: ETHICS FORM A12

LIST OF FIGURES

Figure 2.1:	Conceptual framework	22
Figure 3.1:	Overview of research process	26
Figure 3.2:	Saunder Research Onion	28
Figure 4.1:	Distribution of Survey Participants by Job Role	37
Figure 4.2:	Frequency distribution of experience and type of institution	38
Figure 4.3:	Record of Familiarity and frequency of Usage	39
Figure 4.4:	Awareness and Personal Encounter with Insider Threats among Respondents (N = 359)	41
Figure 4.5:	Frequency of Insider Threat Types by Category	42
Figure 4.6:	Respondents' Perception of Insider Threat Risk Frequency in EHR Systems	43
Figure 4.7:	Box plot for the statistical information	44
Figure 4.8:	Frequency distribution of thematic analysis of data breach incidents	45
Figure 4.9:	Percentage Impact of Insider threat	46
Figure 4.10:	Concern Level of Insider threats to patient data security	49
Figure 4.11:	Impact Levels on Patient Trust: Distribution by Percentage	52
Figure 4.12:	Distribution of Impact Levels on Clinical Quality	53
Figure 4.13:	Distribution of Impact Levels on Clinical Quality	55
Figure 4.14:	Organizational Policies to Address Insider Threats: Response Distribution	55
Figure 4.15:	Frequency Distribution of Implemented security measures for EHR system	56
Figure 4.16:	Perceived Effectiveness of Policy Assessment Measures	57
Figure 4.17:	Frequency Distribution of security training perceived	58
Figure 4.18:	Mean and Standard Deviation of Security Techniques for EHR Protection	60
Figure 4.19:	Frequency of Implementation: Security Policies, Employee Training, and AI-Driven Security Measures	62
Figure 4.20:	Frequency of Key Security Themes in EHR Protection Strategies	64

List of Tables

Table 2.1:	Summary of Financial Impact caused by Insider threat	11
Table 2.2:	Legal Consequences and regulatory framework impact summary	15
Table 4.1:	Distribution of Survey Participants by Years of Experience	39
Table 4.2:	Familiarity Level and Frequency of Usage	40
Table 4.3:	Chi-Square Test	40
Table 4.4:	Descriptive Statistics of Insider Threat Frequency Perception	44
Table 4.5:	Statistical summary of Impact of insider threat	47
Table 4.6:	Ranked Perceptions of Consequences of Insider Threats in EHR Systems	48
Table 4.7:	Frequency of Concern level (N=359)	49
Table 4.8:	Distribution of Concern level about insider threat by job level	50
Table 4.9:	Chi-Square test Concern level Vs Job role	50
Table 4.10:	Belief in Financial Impact Due to Insider Threats	51
Table 4.11:	Patient_trust_impact_distribution	52
Table 4.12:	Chi-Square test Jobe role Vs Perceived impact on insider threat.	54
Table 4.13:	Policy_awareness_responses	56
Table 4.14:	Implementation of Security Controls in EHR Systems	57
Table 4.15:	Statistics of Effectiveness of Policies	58
Table 4.16:	Summary Statistics of Security Control Implementation	59
Table 4.17:	Monitoring Tools Usage Frequency for Suspicious Activity	60
Table 4.18:	Adoption Frequency of Security Policies, Employee Training, and AI-Driven Security Measures	61
Table 4.19:	Frequency Distribution of Key Security Themes and Their Descriptions	64

LIST OF ABBREVIATION	
EHR	Electronic Health Record
NIST	National Institute of Standards and Technology.
ENISA	European Union Agency for Cybersecurity
PHI	Protected Health Information
HITEC	Health Information Technology for Economic and Clinical Health
HIPAA	Health Insurance Portability and Accountability Act
BAA	Business Associate Agreement
HHS	Health and Human Services
GBPR	General Data Protection Regulation
EHDA	European Health Data Space
RBAC	Role-Based Access Control

ABSTRACT

The difficulties that insider threats present to healthcare Electronic Health Records (EHR) systems are examined in this research, with particular attention to Kerala, India. Insider threats pose serious hazards to the security and integrity of patient data since they come from authorized persons including administrators, IT staff, and clinicians. While exterior intrusions have received a lot of attention, insider breaches tend to go unreported yet can have serious repercussions, such as financial losses, medical blunders, and data theft. This study looks into the types, prevalence, and effects of insider threats in EHR systems in an effort to pinpoint the main causes of these breaches. The study draws attention to the flaws of EHR systems, including unreliable access controls, a lack of training, and organizational shortcomings. The study investigates the efficacy of current security measures in reducing insider threats by conducting a thorough survey of Kerala's healthcare professionals. The results emphasize how important it is to have more robust security frameworks that include administrative regulations, behavioral treatments, and technical protections. This dissertation offers practical suggestions for healthcare institutions looking to improve the security of their EHRs, with an emphasis on improved monitoring, user access control, and ongoing employee education. The ultimate goal of this research is to help create stronger plans for protecting private health data and guaranteeing the privacy and accuracy of EHR systems in the medical field.

Keywords*: Electronic Health Records (EHR), Insider Threats, Healthcare Cybersecurity, Data Breach, Access Control, Patient Data Privacy, Information Security, Kerala Healthcare, Risk Mitigation, Health Information Systems.*

1.INTRODUCTION

1.1 Background

EHRs, have revolutionized healthcare through improved care coordination, increased medical research, and easier patient data management. Because patient information is now digitized, health care professionals may access real-time data, make better judgments, make fewer mistakes, and enhance patient outcomes. EHR integration into sectors like biotechnology and pharmaceuticals has made healthcare more efficient and linked. However, the transition to digital records has also resulted in significant security difficulties(Ellen Kim MD, MPH, 2019). EHR systems support better coordination among healthcare providers, facilitate research, and increase the accuracy of medical decisions (WHO, 2017). EHR implementation is continuously increasing in India, especially in Kerala, which is renowned for its strong public health system and digital governance(Mishra *et al.*, 2024).

An important and frequently overlooked danger to the security and integrity of Electronic Health Records (EHR) systems is insider threats. Although external cyberattacks are a known threat, insider breaches—which come from reliable healthcare networks—present a special difficulty because of permitted access and system familiarity. These risks can include malevolent activities like data theft, manipulation, or sabotage as well as inadvertent data breaches brought on by carelessness. Even though there could be serious repercussions, such as invasions of patient privacy, monetary losses, and lowered standards of care, current security and research frameworks place an undue emphasis on external threats. This creates a significant knowledge vacuum about the precise type, frequency, and consequences of insider threats in the healthcare industry, especially with regard to EHR systems. The nuanced and intricate dynamics of insider-originated breaches are frequently too difficult to detect and mitigate with current detection and prevention techniques. In order to close this crucial gap, our study will look into the following.

- With a large percentage of data breaches attributable to insiders, the true frequency and type of insider threats attacking EHR systems in healthcare settings continue to be a major issue.
- EHR security can be jeopardized by specific insider acts, such as system manipulation, data exfiltration, and unauthorized access.

- These risks result in data breaches, medical errors, monetary losses, and regulatory infractions, which have an effect on EHR integrity, patient privacy, and healthcare operations.
- Implementing efficient mitigation solutions, such as administrative, behavioural, and technical safeguards, is necessary to reduce the risk of insider breaches(Bhartiya and Mehrotra, 2013).

In Kerala, where hospital infrastructure is gradually integrating EHR systems, there is still a lack of awareness and readiness about insider threats. While lacking comprehensive internal controls, the majority of healthcare organizations still prioritize perimeter security against external attackers (Nifakos *et al.*, 2021). By addressing these points, the study hopes to offer insightful analysis and useful suggestions for bolstering EHR security frameworks and better safeguarding private patient data against insider threats for healthcare organizations, legislators, and cyber security specialists. The results will help create stronger security measures, better ways to identify them, and better training initiatives to reduce the dangers of insider access to EHR systems. This study fills this knowledge gap by investigating insider threats in Kerala's healthcare ecosystem's EHR systems.

1.2 Purpose of the Study

This study aims to investigate and evaluate the kinds, prevalence, and effects of insider threats that threaten Kerala's EHR systems(Southern Part Of India). The study intends to offer a useful and context-specific mitigation approach to improve data security and operational integrity in healthcare organizations by identifying current vulnerabilities and assessing current solutions.

1.3 Research Context

An interesting argument for examining cybersecurity in healthcare is Kerala, which is renowned for its comparatively excellent healthcare standards and level of digital literacy. The state continues to have difficulties with information security governance, employee training, and technology infrastructure, even in spite of notable advancements in the implementation of EHRs. In this case, systemic problems, undertrained staff, or inadequately implemented access rules could all be insider dangers. This study examines these vulnerabilities using a survey-based methodology, focusing on administrators and healthcare practitioners.

1.4 Significance and Justification

The following factors make this study noteworthy

- In Indian cybersecurity studies, insider threats are not well-represented, especially in the healthcareindustry.
- The sociocultural and infrastructure specifics of Indian healthcare are not taken into account by the majority of current frameworks, which are Western-centric.
- Kerala provides an excellent environment for examining real-world insider risk situations due to its high rate of EHR implementation and digital healthcare activities.
- Hospital managers, cybersecurity legislators, and IT suppliers will find the results useful in creating effective, locally relevant remedies.
- The study will add to the small amount of scholarly work on insider dangers associated to EHRs in poor countries.

1.5 Research Objectives

Identify and Categorize Insider Threats – Examine the types, sources, roles, and access levels of insiders involved in EHR security breaches, classifying threats as malicious, negligent, or accidental.

Assess the Impact of Insider Threats – Analyze the consequences of breaches on EHR security, patient data privacy, and healthcare organizations, including financial, reputational, and legal implications.

Evaluate Existing Security Measures – Review current technologies, policies, and mitigation strategies to identify gaps and limitations in protecting EHR systems from insider threats.

Develop Effective Mitigation Strategies – Propose a comprehensive framework with actionable recommendations for preventing, detecting, and responding to insider threats in EHR systems.

1.6 Research Questions

Categorization of Insider Threats:

How can insider threats be classified based on roles, access levels, and intent within Kerala's healthcare sector?

Impact Analysis:

What are the clinical, operational, and reputational consequences of insider breaches in EHR systems?

Evaluation of Security Measures:

How effective are existing insider threat mitigation strategies in Kerala's healthcare institutions?

Mitigation Frameworks:

What integrated measures—technological, procedural, and behavioral—can effectively reduce insider threat risks?

1.7 Dissertation Structure Overview

With a particular focus on the healthcare industry in Kerala, India, this dissertation is organized into five chapters, each of which logically adds to the thorough investigation of insider threats in Electronic Health Records (EHR) systems. The research backdrop and context are described in **Chapter 1**, the Introduction. The need of looking into insider threats in EHR systems, especially in Indian healthcare settings, is explained, along with the research objectives and questions that will guide the study. It also gives an outline of the dissertation's structure and defines important terms.

A thorough literature review is provided in Chapter 2, which critically evaluates the body of knowledge about cybersecurity issues, EHR system research, and the growing significance of insider threat mitigation. In addition to highlighting gaps in the existing literature, this chapter outlines important theoretical frameworks and lays the groundwork for the rest of the study.

The research design is explained in Chapter 3, the Methodology chapter, along with the justification for employing a survey-based strategy to target Keralan healthcare professionals. The demographic sample, data collection methods, research tools, and ethical issues including informed permission and participant confidentiality are all described. Additionally covered in this chapter are the chosen methodology's validity and limits.

Chapter 4 integrates the Discussion, Findings and analysis. Healthcare workers' knowledge levels, perceived dangers, and current mitigation techniques are examined, together with the data gathered from survey responses and insider threat patterns. A better comprehension of the implications of these findings is provided by the discussion, which incorporates them with the

body of previous literature. The results are also interpreted in the chapter's theoretical fram The dissertation is concluded in Chapter 5, which also discusses the limitations of the study, provides academic and practical recommendations, and summarizes the main findings and their significance. Future research directions that could broaden the breadth of mitigation techniques and better examine insider threat dynamics in various healthcare contexts are also suggested.

2. LITERATURE REVIEW

2.1 INTRODUCTION

This chapter reviews the literature on insider threats in the security of electronic health records (EHRs), emphasizing the dangers, effects, and countermeasures. The study, "Unmasking Insider Threats in Electronic Health Records (EHR): A Comprehensive Analysis of Risks, Impacts, and Strategic Mitigation Measures for Enhanced Healthcare Data Security," looks into how insiders can compromise healthcare organizations and how to make EHR security stronger.

This chapter's main goal is to critically review the body of research on insider threats in EHR systems, including their nature and effects. It assesses security frameworks, mitigation techniques, and detection procedures to find knowledge gaps and areas that need more investigation. This review offers a basis for comprehending insider threats and creating efficient defences by combining recent research.

The chapter is structured as follows:

- Classifying insider risks as malevolent, careless, or unintentional, as well as discussing their significance to EHR security, is part of Understanding Insider risks in EHR Security.
- The effects that insider threats have on healthcare institutions examines the effects of healthcare insider breaches on finances, regulations, operations, and reputation.
- Reviewing current security measures and their limitations, this article highlights the advantages and disadvantages of behavioural monitoring, anomaly detection, and access limits.
- Suggested Mitigation Strategies: Examines policies, training programs, and sophisticated security systems to reduce insider risks.

The need of protecting EHR systems from both internal and external threats was underlined in the Introduction chapter, which is expanded upon in this literature review. Through a review of previous studies, this chapter highlights knowledge gaps that guide the next Research Methodology chapter, which will go into greater detail about investigative techniques for insider threat detection and prevention. This review's observations will help create a thorough security framework that is suited to the particular difficulties posed by insider threats in EHR settings.

2.2 UNDERSTANDING INSIDER THREATS IN EHR SECURITY

2.2.1 Insider Threat Taxonomies and Classification

A key component of an effective cybersecurity defence against insider threats in Electronic Health Records (EHRs) is the classification and categorization of the various hazards that insiders present. Three main types of insider threats can be distinguished: malicious insiders, negligent insiders, and inadvertent insiders. Malicious insiders will fully abuse their access for their own financial or personal benefit, while negligent insiders disregard security procedures, exposing data or creating vulnerabilities in the system. On the other hand, unintentional insiders unintentionally jeopardize security by doing things like carelessly handling sensitive data or leaking it.

A thorough examination of insider risks in cybersecurity may be found in the publication "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations" by Mohammed Nasser Al-Mhiqani . The authors offer a taxonomy that classifies insider threats according to elements including the degree of access, the motive of the insiders, and the techniques used by the malicious insiders. They discuss the advantages and disadvantages of the different machine learning methods used to identify these dangers. The accessible datasets used to train and assess detection algorithms are also examined in the paper, with issues such as data imbalance and the lack of real-world cases highlighted. The authors list the need for more reliable detection techniques and the integration of various data sources as two of the field's unresolved issues. In order to increase organizational security, they highlight the significance of tackling these issues and offer suggestions for improving insider threat detection research and development in the future(Al-Mhiqani *et al.*, 2020a).

To expand on this paradigm, Prabhu and Thompson suggest a four-category model that provides a thorough understanding of insider behaviours by concentrating on intentional, negligent, unintentional, and cunning behaviours(Prabhu and Thompson, 2020). A more thorough method builds on this by combining insider profiling, motivations, and access levels to give a strong grasp of the wide variety of insider threats(Singh and Sharma, 2022). In the meantime, Anwita presents a novel method for classifying insider threats according to organizational, technical, and human behavioral markers. By helping firms recognize and address various insider threat scenarios, these classifications help to focus threat detection and mitigation efforts(Anwita, 2024).

2.2.2 Unintentional Insider Threats and AI-Driven Taxonomy

Unintentional insider attacks provide serious cybersecurity dangers that are frequently overlooked, especially in healthcare institutions. Usually, these are brought on by authorized users who, through carelessness or human mistake, unintentionally jeopardize system security. For example, a healthcare worker can inadvertently communicate private patient data to the incorrect person or misconfigure a system. These seemingly insignificant mistakes can have serious repercussions for the availability, confidentiality, and integrity of medical data, resulting in damage to one's finances and reputation.

An exploratory investigation of previous data breaches in healthcare organizations from January 2015 to December 2020 was carried out by the research team using data from the US Department of Health and Human Services in order to determine the degree to which human factors contributed to data security events.
An analysis of 1,485 breach events that affected 141,252,797 medical records between January 2015 and December 2020 was conducted by the descriptive data breach information from the U.S. Department of Health and Human Services is analysed in this study using text mining and visualization tools. The study's objectives are to examine weaknesses in internal security systems, identify different insider and external threats, and create suitable data security solutions. The strategy offers a fresh way to comprehend the types of data breaches that occur in the healthcare industry. The research team. Out of that total, malevolent factors accounted for 26.7 percent of the compromised records, while inadvertent factors accounted for 73.1 percent. According to research, the most common causes of cyber breaches in HCOs include carelessness and negligence (382 instances), theft (222 incidents), and falling for a phishing scam (221 incidents)(Liu Hua Yeo, 2022).

The substantial cybersecurity risk posed by unintentional insider threats—actions by authorized users that unintentionally jeopardize data availability, confidentiality, or integrity—is addressed in the paper "Create the Taxonomy for Unintentional Insider Threat via Text Mining and Hierarchical Clustering Analysis" by Jolynn Baugher and Yanzhen Qu. The authors stress the importance of creating a uniform taxonomy to improve the efficiency of artificial intelligence (AI) systems in reducing these risks because they acknowledge the significant financial impact of such threats. By examining 1,850 human error instances from public data breach datasets, the study applies text mining and hierarchical clustering approaches to characterize unintended insider threat actions. The resulting taxonomy is divided into five main

categories: misconfigurations, lost media, improper data permissions, application failures, and communication errors. By giving cybersecurity experts a comprehensive grasp of the many types of unintended risks, this structured taxonomy makes it easier to create more effective AI-driven protection mechanisms and to establish focused mitigation methods(Baugher and Qu, 2024).

2.2.3 Behavioural Analysis and Detection of Insider Threats

Behavioural analysis is essential for identifying insider dangers, especially when it comes to inadvertent and negligent insider behaviours. While technical barriers like encryption and access controls are important, they sometimes overlook the more covert activities of insiders who might not have overt hostile intent but nevertheless represent a serious risk, according to Al-Mhiqani and Mimecast. EHR security can be seriously impacted by negligent actions including disclosing passwords incorrectly, failing to follow encryption guidelines, or losing critical data(Al-Mhiqani *et al.*, 2020b)&(mimecast, 2025).

Insider risks are further categorized by Al-Mhiqani into a number of behavioural factors, such as suspect device usage, altered work habits, and odd access patterns. Before it becomes a breach, these actions could be an indication of an approaching insider threat(Al-Mhiqani *et al.*, 2020). Analysing these behaviours, regardless of whether they are the result of organizational causes, technological errors, or personal concerns, offers a more comprehensive view of insider dangers(Anwita, 2024). By tracking possible threats early on, behavioural indicators can assist organizations in improving detection efficiency and lowering the probability of successful security breaches. In order to reduce human error, this emphasizes the necessity of ongoing employee activity monitoring and the development of a security-conscious organizational culture.

2.2.4 Insider Threats in Healthcare and the Need for a Specialized Taxonomy

Because of its reliance on linked digital technology, the healthcare industry confronts particular cybersecurity challenges. Electronic Health Records (EHRs) are particularly vulnerable to internal and external attacks due to their sensitive nature. Mahima Jaikanth and Vijay K. Madisetti's work "A Comparative Analysis of Cybersecurity Threat Taxonomies for Healthcare Organizations" explores the particular cybersecurity issues that healthcare organizations confront because of their reliance on interconnected digital technologies. Although established threat taxonomies like the Open Threat Taxonomy (OTT), NIST, and ENISA offer fundamental frameworks for comprehending IT dangers, the authors point out that they are not especially

designed to handle the complexity present in the healthcare industry. Inadequate mitigation techniques for risks such as illegal access to patient records, interruptions in medical facility services, and possible injury from compromised medical devices might arise from this imbalance. The study emphasizes the need for a customized taxonomy that aligns more closely with the specific threat landscape of healthcare organizations. By critically assessing existing frameworks, the authors aim to bridge the gap between general cybersecurity taxonomies and the specialized needs of the healthcare industry, thereby enhancing the sector's ability to protect patient data and maintain the integrity of critical healthcare systems(Jaikanth and Madisetti, 2024).

Understanding insider threats is crucial for EHR security, and this literature review highlights the necessity for a sophisticated strategy to identify and stop both intentional and inadvertent insider activity. An organization's ability to effectively handle insider threats is improved by the inclusion of a structured taxonomy, whether the focus is on behavioural analysis or developing AI-driven detection methods. Additionally, proactive monitoring and security rules, in addition to tailored taxonomies for specialized industries like healthcare, are essential for protecting sensitive data and guaranteeing system integrity.

Organizations must obviously modify their cybersecurity plans to reflect the ever-changing nature of insider threats. Through the implementation of a multifaceted strategy that incorporates behavioral analysis, technical defenses, and specialized threat taxonomies, organizations can enhance the protection of their EHR systems against insider threats, guaranteeing patient confidence and regulatory compliance.

2.3 The Impact of Insider Threats on Healthcare Institutions

For healthcare organizations, insider threats can have a significant impact on not only data security but also finances, regulatory compliance, and general operations. In order to prioritize effective mitigation efforts and ensure organizational resilience, it is imperative to comprehend the entire extent of these consequences(Neetesh Saxena, 2020).

2.3.1 Financial Consequences

Insider threats provide serious financial concerns because they can result in fraud, fines from the government, harm to one's reputation, and interruptions to operations. Human error, malevolent intent, and systemic flaws are the main causes of insider threats in Electronic Health Records (EHR) systems, which pose a significant financial burden for healthcare institutions.

This review summarizes the extent, causes, and countermeasures of these dangers by combining data from industry reports, case studies, and peer-reviewed research.

The average cost per breach in 2020 was $7.13 million for healthcare data breaches, with PHI-related breaches costing $150 per compromised record on average, while non-PHI breaches cost $146. 85% of breaches involve human error, with phishing compromising **421,938 records per incident** on average (Yeo and Banfield, 2022). Costs of insider threat remediation in the pharmaceutical and healthcare industries increased by 31% from 2018 to $10.81 million per year by 2020.
Containment time: The cost of incidents that were not resolved within 90 days was almost double ($13.71 million) as opposed to those that were managed more quickly ($7.12 million). In 2020, investigations alone cost $103,798 for each event, an 86% increase over 2018 being the secondary cost (Imprivata, 2020).

Source: Developed by author

Threat Type	Frequency	Cost per Incident	Key Characteristics
Negligence	55%	$7.2 million annually	Mishandling PHI, phishing susceptibility, and poor security practices(Yeo and Banfield, 2022).
Malicious Insiders	23%	$701,500 per event	Intentional data theft, sabotage, or espionage (e.g., selling PHI on black markets)(Macklin, 2025).
Credential Theft	22%	Not reported	Unauthorized access via stolen credentials, often enabling ransomware or data leaks(Imprivata, 2020).

Table2.1 : Summary of Financial Impact caused by Insider threat

Numerous studies have shown how insider threats to Electronic Health Records (EHR) systems can have an increasing financial impact. Insider threats are important in the financial services industry because they frequently include the abuse of privileged access, which can result in data loss, financial fraud, or harm to one's reputation.

According to a study by Whitelaw et al. (2024), even with robust exterior cybersecurity safeguards, UK financial institutions are vulnerable to insider threats. Insiders have trusted

access, the authors point out that although external cyber risks frequently garner more attention, insider threats—which come from within the company—can be just as harmful, if not more so. The study examines the reasons behind insider threats, which might include everything from resentment toward the company to financial gain, from a practitioner-focused perspective (Findlay Whitelaw; Jackie Riley; Nebrase Elmrabit, 2024).

The wider effects of insider threats on many businesses are further covered by Saxena, who highlight the monetary damages resulting from insider data breaches. These risks have an impact on healthcare's financial stability as well as operational efficiency, which can result in penalties and harm to the industry's reputation. Furthermore, fixing such violations comes at a high cost in the form of lost revenue, fines from the authorities, and legal actions(Neetesh Saxena,2020).

According to Subhani, insider threats have disastrous financial repercussions, including harm to a brand's reputation, a decline in customer trust, and legal repercussions. These financial consequences are exacerbated in the context of EHRs because to the sensitive sensitivity of patient data and the high expense of repairing compromised systems(Subhani *et al.*, 2021).

The healthcare industry is particularly susceptible to insider threats because of a number of features peculiar to the sector. Protected Health Information (PHI) can sell for $250 to $363 per record on the black market, which is far more than the value of credit card data, making high-value data a serious worry. PHI's extensive personal information accounts for this high value, which makes it perfect for identity theft and medical fraud(Liu Hua Yeo, 2022). There are hazards associated with complex IT systems as well. Decentralized EHR access points and reliance on outside vendors lead to a number of vulnerabilities, particularly through personal endpoints and medical equipment that are not secure. Last but not least, regulatory demands from HITECH and HIPAA impose harsh penalties for non-compliance, with fines of up to $1.5 million per infraction, raising the financial stakes for healthcare firms even more(Tampa Bay, 2025).

Insider threats in healthcare pose financial hazards, as demonstrated by two noteworthy case studies. Christopher Dobbins, a disgruntled former employee, disrupted vital PPE deliveries during the COVID-19 epidemic by sabotaging the company's shipping systems, causing major operating delays for Stradis Healthcare. This insider threat caused significant monetary losses as well as harm to the company's reputation. In a another case, an insider-perpetrated

ransomware attack in a Texas hospital stole patient data and disrupted facility operations, including HVAC systems. The breach highlighted the serious financial consequences of insider threats in healthcare settings, resulting in a $2.5 million cleanup cost and additional sanctions from the law(Macklin, 2025).

The overall financial impact of insider threats in EHR systems is significant, including both direct expenses like penalties and legal fees as well as indirect costs like patient discontent, lost trust, and long-term reputational damage. In the healthcare industry, reducing these risks and guaranteeing organizational resilience require effective detection, prevention, and mitigation techniques.

The financial costs of insider threats in the Indian healthcare industry are substantial and go beyond the price of immediately fixing breaches. Nearly 28% of healthcare data breaches in India are caused by insider-related occurrences, according to studies, with an average financial loss per incident of ₹4.2 crores(4.3 million Euro) due to operational disruptions, legal expenditures, and regulatory fines(Sreekandan, 2023). These expenses are further increased by the high value of Protected Health Information (PHI) on illegal markets, since exposed data may result in identity theft, insurance fraud, and expensive legal action(Sujeet Katiyar, 2024). Furthermore, indirect expenses like harm to one's reputation, a decline in patient confidence, and higher compliance costs due to new laws like the Digital Personal Data Protection Act make the financial burden on healthcare providers even worse(DSCI , 2025).

When combined with low cybersecurity investments, India's complicated healthcare IT archit ecture frequently results in longer breach discovery and containment timeframes, which raise s total costs(Patel, 2022).
Given Kerala's changing healthcare environment and the Indian healthcare context, specific i nsider threat prevention and mitigation techniques are desperately needed, as these financial r epercussions demonstrate.

2.3.2 Regulatory and Legal Ramifications

Regulations have a significant impact on Electronic Health Records (EHRs), affecting privacy, data security, and healthcare operations. The secondary use of EHR data is addressed by laws like GDPR, which ensure adherence to changing digital health rules(Shah and Khan, 2020). Strict regulatory enforcement is necessary to stop sensitive patient data from being misused and accessed by unauthorized parties. Similar to this, Banerjee contend that in order to combat

new cybersecurity threats, privacy regulations must change, highlighting the need for compliance measures such data encryption and employee training(Banerjee *et al.*, 2024).

Insider threats and encryption vulnerabilities are highlighted as major regulatory concerns in Janarthanan et al.'s (2024) discussion of the legal complexities surrounding the deployment of EHRs(Janarthanan *et al.*, 2024). (Park *et al.*, 2013) examines how cybersecurity laws affect networked healthcare systems, emphasizing the value of legal frameworks in reducing insider threats. In order to ensure ethical and secure data management, (Ismail Keshta, 2021)Keshta and Odeh (2021) emphasize the necessity of regulatory monitoring to protect patient data across digital healthcare platforms.

Financial penalties for breaking HIPAA and HITECH standards can be severe; fines can amount to up to $1.81 million per year. Because improper use of Electronic Health Records (EHR) or illegal access can lead to legal infractions, insider threats in healthcare organizations are a serious concern. Furthermore, third-party breaches make culpability even more difficult because these rules also apply to business associates who handle patient data. Mitigating these financial and legal risks requires rigorous adherence to compliance standards. Implementing frameworks like HITRUST (integrating HIPAA, GDPR) requires significant investment in encryption, access controls, and training.

Because class-action lawsuits and settlements frequently surpass remediation expenses, litigation risks increase the financial burden. For instance, after the hack, a hospital in Texas paid $2.5 million. Reporting public breaches on the HIPAA "Wall of Shame" damages patient confidence and may result in fewer partnerships and recommendations. Healthcare businesses need to put strong compliance frameworks in place to reduce these risks. These frameworks should include real-time monitoring, frequent audits, and strict vendor management. In order to lower the possibility of willful neglect penalties and related legal obligations, proactive steps like encrypting ePHI and implementing Business Associate Agreements (BAAs) are essential(Alder, 2023).

Source: Developed by author

Risk Factor	Impact
DPDPA violations	Penalties up to ₹250 crore (~$30 million) for serious data breaches; fines for non-compliance and delayed breach notification; enforcement by the Data Protection Board of India (DPDPA, 2023)
HIPAA violations	Fines up to **$1.81 million annually** and mandatory audits by HHS(HSS, 2022).
Third-party breaches	Vendor vulnerabilities (e.g., 2015 EHR vendor breach exposing 4M patients)(Hales, 2023).
Litigation	Class-action lawsuits and settlements (e.g., Texas Hospital's $2.5M breach remediation)(admin, 2024).

Table2.2: Legal Consequences and regulatory frame work impact summary

Privacy, security, and secondary usage are issues that are intended to be addressed by regulations and legal frameworks pertaining to Electronic Health Records (EHRs). GDPR-compliant frameworks that prioritize patient control and safe data sharing include the European Health Data Space (EHDS) and Ireland's Health Information Bill 2024. However, phishing and insider threats are just two of the ethical and legal issues that EHRs must deal with(EHD, 2025). These issues call for strong security measures and adherence to privacy laws. Furthermore, the need for data reuse in research and policymaking must be balanced with the right to privacy of individuals when using EHR data for secondary purposes. A major implementation difficulty for efficient EHR management is maintaining interoperability and compliance with regulations such as GDPR(ehealth,2025.).

A historic legislative framework in India, the Digital Personal Data Protection Act (DPDPA), 2023, aims to protect sensitive health information as well as other digital personal data. The Act, which was passed in order to strike a balance between people's right to privacy and the legitimate use of personal data, places strict requirements on healthcare providers to install

strong security measures including encryption and access controls, assure transparency, and acquire explicit patient approval(Anubhuti Sood, 2025).

Healthcare firms face serious financial risks if they do not appropriately protect patient data, as non-compliance can result in harsh penalties, with fines of up to ₹250 crore(DPDPA, 2023). The Act also has significant exclusions for medical emergencies, which are crucial in India's diversified and crowded healthcare system because they enable medical personnel to treat patients promptly without worrying about facing legal consequences(Anubhuti Sood, 2025). The DPDPA is a driving force behind the adoption of comprehensive data protection procedures by healthcare providers and a catalyst for fostering patient trust as India's healthcare industry rapidly digitizes. This helps to mitigate financial losses resulting from data breaches and insider threats. Healthcare businesses, particularly those in Kerala, must invest in customized cybersecurity strategies and compliance frameworks in order to protect sensitive health data and maintain operational resilience in light of the changing legal landscape.

2.3.3 Operational and Reputational Damage

Healthcare operations are at serious danger from EHR outages, especially when they are brought on by insider threats like ransomware attacks or system sabotage. Workflows in critical care may be stopped by these interruptions, postponing treatments and endangering patient safety. For example, healthcare providers are forced to use manual procedures during downtime, which raises the possibility of mistakes in clinical paperwork and medicine orders, thus jeopardizing patient care. Hospitals lose an average of $7,900 every minute due to unscheduled outages, which has a significant financial impact on both revenue and operational effectiveness(Hales, 2023).

The operational dangers of insider threats are further highlighted by supply chain sabotage, as seen in the 2020 Stradis Healthcare event. The COVID-19 outbreak caused major delays and operational paralysis when a former employee gained illegal access to the shipping system, momentarily stopping PPE shipments. Furthermore, insider threats against decentralized EHR systems have the potential to do expensive harm to IT infrastructure. Large-scale rebuilds are frequently necessary for compromised networks, which reduces operational effectiveness and raises recovery expenses significantly. In 2024 alone, for instance, healthcare firms spent an average of $2.57 million on recovery expenses after ransomware attacks. These events highlight the necessity of strong security protocols to stop such interruptions and safeguard organizational assets as well as medical care(Alder, 2023).

Healthcare organizations have a major challenge when it comes to operational and reputational harm caused by insider threats in electronic health record (EHR) systems. Data breaches have a detrimental effect on hospital performance and financial incentives associated with the deployment of EHRs in addition to compromising sensitive patient information. Healthcare operations are disrupted, patient treatment is delayed, and trust in digital health systems is damaged when insider threats take advantage of system flaws. These breaches put additional strain on an organization's operational capabilities and financial stability by requiring it to devote significant resources to recovery(Kwon and Johnson, 2025).

Additionally, insider attacks that take advantage of security flaws might cause operational instability and privacy violations, which calls for expensive mitigation measures and regulatory actions(Rahman *et al.*, 2024). An institution's reputation is severely impacted by insider-driven EHR breaches in addition to operational difficulties. Rele and Patil (2023) contend that violations damage patient confidence and subject medical institutions to monetary and legal risks. Patients may be discouraged from using digital health services due to the public's perception of degraded security, and the strain on healthcare professionals is increased by regulatory monitoring. To reduce these threats and maintain institutional credibility, it is essential to monitor insider activity and strengthen cybersecurity procedures(Rele and Patil, 2023).

Healthcare organizations may suffer severe operational, financial, legal, and reputational consequences as a result of insider threats. The severity of these effects highlights the pressing need for thorough and efficient methods of detecting and mitigating insider threats.

2.4 Current Security Measures and Their Limitations

To reduce insider risks to Electronic Health Records (EHR) systems, healthcare institutions have put in place a few security measures. Important actions consist of:

2.4.1 Behavioural Monitoring and User Activity Tracking

Tools that track user behaviour to find odd patterns that might point to malevolent or careless behaviour are essential for identifying insider threats in the healthcare industry. While studies show that these tools are useful, particularly for monitoring access to sensitive patient data, they also highlight the possibility of false positives, which need to be carefully calibrated to prevent interfering with legal activities(Diaz, 2022).

Behavioural analytics and real-time visibility are essential for reducing insider threats in electronic health record (EHR) systems. Anomalies that can point to malevolent or careless insider conduct can be quickly identified thanks to real-time user activity monitoring tools like Teramind. In order to further improve security, advanced behavioural analytics provide baselines of typical user activity and spot any differences that can indicate possible risks. But there are difficulties in putting these safeguards into practice, especially when it comes to striking a balance between security and employee privacy. While maintaining strong defences against insider threats, organizations must carefully set monitoring systems to ensure compliance with privacy requirements(Whitelaw *et al.*, 2024).

2.4.2 Anomaly Detection Systems

An essential tool for spotting insider threats in Electronic Health Records (EHR) systems are anomaly detection systems driven by machine learning algorithms. These systems function by setting baselines for typical user behaviour and identifying any variations that might point to malicious activity. To detect anomalies with high accuracy, minimize false positives, and improve the security of sensitive healthcare data, methods like Isolation Forest and Local Outlier Factor clustering are employed(Tabassum *et al.*, 2024).

However, anomaly detection systems still have problems even with their efficacy. They may find it difficult to adjust to novel, unidentified attack patterns, necessitating regular upgrades to be functional(Bin Sarhan and Altwaijry, 2023). Furthermore, the level of data granularity and the particular machine learning methods employed can affect these systems' accuracy(Le and Zincir-Heywood, 2019). User-session data, for example, has demonstrated high detection rates and quick response times. As healthcare environments change, these systems must adapt to new risks and learn from new data in order to continue being a strong defense against insider threats(Kotb *et al.*, 2025).

Security awareness programs and compliance culture improve the effectiveness of technical controls by addressing human vulnerabilities. Subjective methods like self-assessment questionnaires dominate cybersecurity behaviour assessment, but they often introduce biases that can affect the reliability of findings(Kannelønning and Katsikas, 2023). Hurst examines the application of supervised classification techniques, such as decision tree, random forest, and support vector machine algorithms, to actual data from a hospital in the United Kingdom, with a focus on insider-threat detection within healthcare infrastructures. By addressing the

inherent dangers associated with digitizing patient records, the study seeks to effectively detect misuse of EHR data(Hurst *et al.*, 2022).

S. Ramasami and P. Uma Maheswari's work "Securing Electronic Health Records from Insider Threats in Smart City Healthcare Cloud Using Machine Learning Approach" tackles the crucial problem of safeguarding Electronic Health Records (EHRs) in smart city healthcare systems. Since insider threats are frequently harder to spot than external attacks, the authors suggest a machine learning-based approach for detecting and mitigating them. Through the examination of user behaviour patterns and access logs, the system seeks to differentiate between harmful and authorized activity. This proactive strategy improves EHR security while guaranteeing the integrity and confidentiality of patient data. The results of the study help to strengthen security protocols in cloud environments for healthcare, emphasizing the value of incorporating cutting-edge technologies to protect private data(Ramasami and Maheswari, 2024).

2.4.3 Access Control and Encryption

A meta-review of 18 studies found a significant link between well-implemented security controls and reduced cyber risks. Evidence suggests that organizations with robust security measures experience fewer breaches and better risk outcomes. Cybersecurity frameworks, such as NIST and ISO 27001, are widely recognized for improving organizational resilience. However, their adoption often varies due to resource constraints and lack of standardization(Goel, 2019).

.

CTI (Cyber Threat Intelligence) has been shown to improve precautionary measures against breaches by providing actionable insights into emerging threats. Organizations that integrate CTI into their security operations demonstrate better preparedness and response capabilities(Saeed *et al.*, 2023).

The importance of robust security measures for Electronic Health Records (EHRs) to protect against insider threats and ensure data integrity. Key strategies include implementing Role-Based Access Control (RBAC) and the Principle of Least Privilege (PoLP) (Alarfaj and Rahman, 2024). RBAC ensures that users only access information necessary for their roles, reducing the risk of unauthorized data breaches. This approach is supported by studies highlighting the need for strict access controls to maintain EHR security. Additionally, encryption plays a critical role in safeguarding sensitive patient information by converting data

into unreadable formats unless accessed with the correct decryption keys(Nduma N. Basil, 2022).

Even if the security systems in place now provide useful protection, their shortcomings highlight the necessity for further development. To reduce insider threats, effective security frameworks should combine cutting-edge technologies with robust regulations and employee training.

2.5 Suggested Mitigation Strategies for Insider Threats

A comprehensive strategy that incorporates organizational, technological, and human-centred tactics is needed to mitigate insider threats in EHR systems. In order to identify and stop insider threats, effective mitigation measures include developing policies, training staff, and implementing advanced security tools.

2.5.1 Policies and Governance

The security, availability, and integrity of electronic health records (EHRs) are seriously threatened by insider threats in the healthcare industry. To reduce these risks, governance structures and policies must be strong.

In order to prevent insider threats, it is imperative that clear organizational policies be established. These guidelines ought to specify data access procedures, permissible use, and the penalties for breaking security safeguards. Research indicates that by encouraging accountability, well stated policies might lessen negligent insider threats(Nassir *et al.*, 2024). To guarantee that policies are properly implemented, robust governance mechanisms are required. Security awareness training, incident response planning, and routine risk assessments are all included in this. Organization-wide, leadership-driven awareness initiatives are more successful because they prioritize a culture of trust and security(HSS, 2022).

Issues like controlling third-party risks and striking a balance between security and employee privacy still exist in spite of these precautions. Implementing strong access controls, keeping an eye on systems, and making sure staff members receive ongoing training to handle changing threats are a few solutions(Triplett, 2024).

Healthcare businesses can improve insider threat mitigation and safeguard sensitive patient data by prioritizing strong policies and governance, which will ultimately improve the security and privacy of EHR systems.

2.5.2 Training and Awareness Programs

Programs for security education, training, and awareness (SETA) are crucial for reducing insider risks because they create a culture that is security-conscious. According to Hu, Hsu, and Zhou , structured training can help reduce human error, enhance policy compliance, and fortify organizational resilience against cyber threats. They also stress the importance of ongoing learning and flexible implementation techniques(Hu *et al.*, 2022).

A thorough literature evaluation on raising information security awareness among staff members in both public and private companies is presented by Khando in his studies. The significance of security education, training, and awareness (SETA) initiatives in reducing insider threats is emphasized by the study. It underlines important determinants of awareness, such as employee involvement, leadership support, and company culture. Lack of motivation, resistance to training, and the dynamic nature of cybersecurity threats are some of the issues the authors point out. Best practices including scenario-based learning, gamification, and continuous reinforcement techniques are also examined in the review. The study finds that in order to create a security-conscious workforce and lessen vulnerabilities to insider threats, a multi-layered strategy that combines technology controls and human-centric interventions is essential(Khando *et al.*, 2021).

Customized training formats increase efficacy and engagement. Examples include software-based simulations for intermediate learners, instructor-led workshops for beginners, and documentation for refreshers. However, there are still issues, such as resolving resource limitations in smaller firms and sustaining workforce attentiveness over time. Awareness is maintained by proactive steps like phishing simulations, yearly refreshers, and incorporating threat intelligence into training programs(Berezin, 2025).

2.5.3 Advanced Security Technologies.

Studies also explore the role of emerging technologies like IoT and AI in cybersecurity frameworks. While these technologies offer advanced threat detection capabilities, they also introduce new vulnerabilities that require updated security measures(Cremer *et al.*, 2022)

The integration of cutting-edge technical solutions, continuous staff education, and strong rules must all be balanced in a complete plan to reduce insider risks. In order to strengthen their security against insider threats, healthcare organizations should address both technical and psychological elements.

2.7 Conceptual frame work

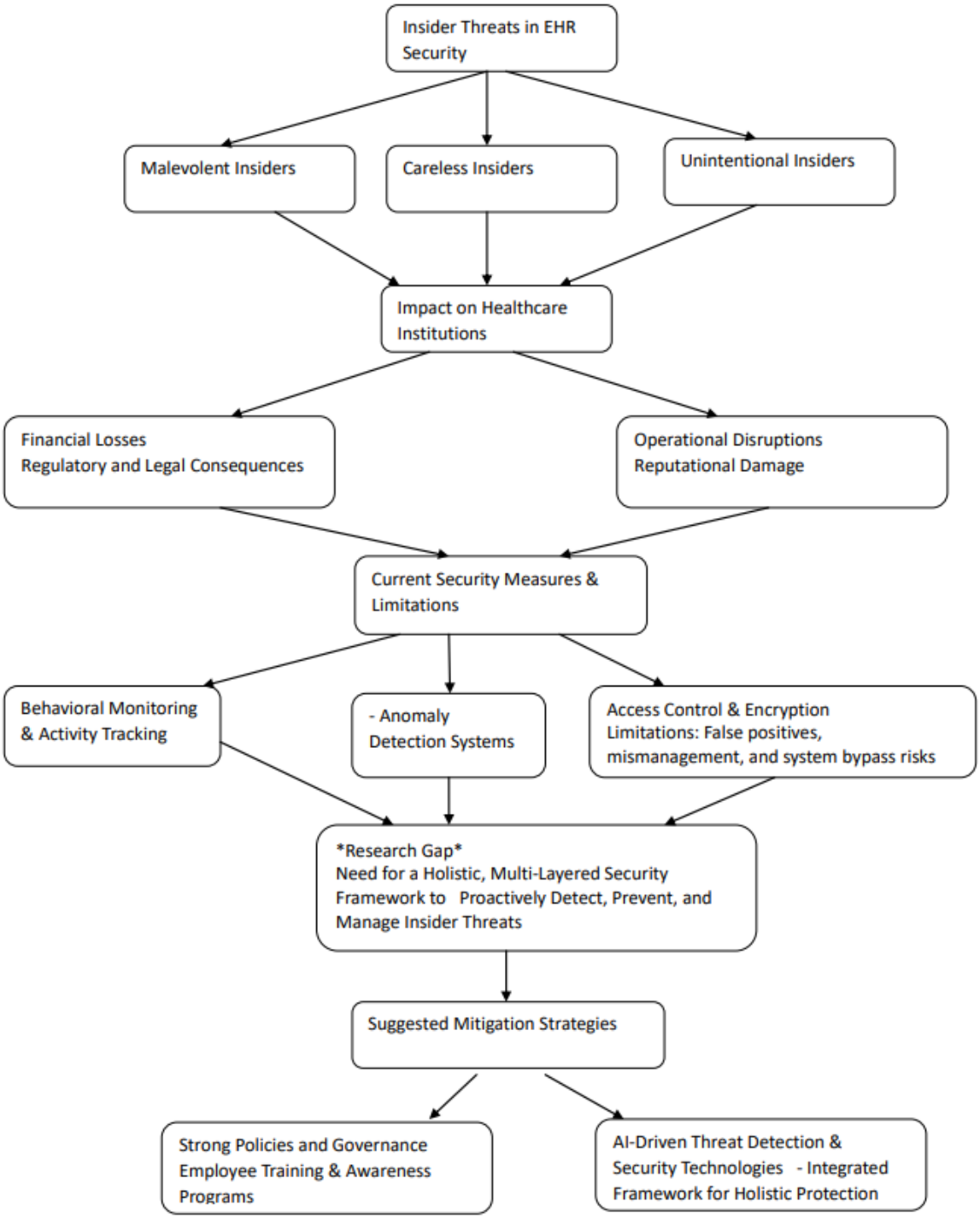


Figure 2.1: Conceptual Framework *Source: Developed by author*

This figure illustrates:

1. **Types of insider threats** (Malevolent, Careless, Unintentional).

   Threats are divided into three primary categories by the conceptual framework for insider threats in Electronic Health Records (EHR) security: malicious insiders, negligent insiders, and inadvertent insiders. Malevolent insiders purposefully use their access for sabotage or personal benefit, while negligent insiders jeopardize security because they are unaware of the risks. On the other hand, unintentional insiders unintentionally cause vulnerabilities, frequently by handling sensitive data improperly or becoming the target of phishing campaigns.

2. **Impact on healthcare organizations** (Financial, Legal, Operational, Reputational).

   Healthcare organizations face serious consequences from these risks, which impact their operational and financial stability. Regulatory fines, legal penalties, and possible challenges brought on by data breaches can result in financial losses. Furthermore, hospital operations can be disrupted by insider threats, which can result in system interruptions, patient care delays, and reputational harm, all of which can lower public confidence in the healthcare system.

3. **Existing security measures and their limitations**.

   Access control, anomaly detection, and behavioural monitoring are the main focuses of current security procedures. Although anomaly detection and behavioural monitoring are useful tools for spotting suspicious activity, they frequently produce false positives, making it difficult to distinguish between malicious and genuine activity. Although encryption and access control are important security measures, they have drawbacks, such as the possibility of system bypass and poor management. Despite these initiatives, current tactics are insufficient to successfully stop insider threats.

4. **ResearchGap**

   The absence of a comprehensive, multi-layered security solution to proactively detect, mitigate, and manage insider threats is one of the main research gaps noted in this framework. Insider dangers are not sufficiently addressed by many security solutions, which concentrate on external threats. To improve protection, a more all-encompassing approach is required.

5. **Mitigation strategies** (Policies, Training, AI-Driven Security).

The framework recommends the implementation of robust policies, governance, and personnel training programs to enhance security awareness and decrease irresponsibility in order to mitigate these risks. A proactive and flexible defence system against insider threats in EHR security can also be established by utilizing AI-driven threat detection and integrated security technologies to enhance real-time monitoring and reaction.

3. METHODOLOGY

3.1 Overview

This chapter outlines the research philosophy, approach, strategy, data gathering methods, and data analysis methodologies used in the study. By guaranteeing a methodical and exacting procedure for data collection and analysis, the chosen methodology is crucial for accomplishing the study's goals. It lays the groundwork for producing trustworthy and legitimate results that can improve the security of healthcare data and guide pertinent policy suggestions.

The chapter begins with a discussion on the adoption of a **pragmatic research philosophy**, highlighting its focus on practical solutions and adaptability, paired with an **inductive approach** that enables the development of theories based on the collected data. This methodological combination is particularly appropriate for investigating the multifaceted nature of insider threats in Electronic Health Records (EHR) systems. The research strategy is next described, emphasizing the study's quantitative character and providing evidence for the use of structured questionnaires. To enable comprehensive statistical analysis, the survey mostly uses closed-ended questions; open-ended questions are used to gather more in-depth qualitative information.

The data collection section outlines the target population, the sampling method, and the structure of the survey tool. Ethical considerations—such as informed consent, voluntary participation, and confidentiality—are also addressed to ensure participant rights are protected. Finally, the data analysis section describes the methods used to interpret both quantitative and qualitative data. Quantitative responses are assessed using descriptive statistics, frequency distributions, and regression analysis to identify patterns and relationships. Open-ended responses are analysed thematically to draw out key insights. Together, these methods aim to offer a thorough understanding of insider threats within EHR systems.

The figure below shows an over view of research process. The study on electronic health records (EHR) takes a pragmatic stance, emphasizing workable solutions with an adaptable methodology. It investigates patterns found in the data using an inductive approach. With a few qualitative components, the research design is primarily quantitative. The main method is the use of surveys, which combine some open-ended questions to elicit more in-depth information from medical experts with closed-ended ones for statistical analysis.

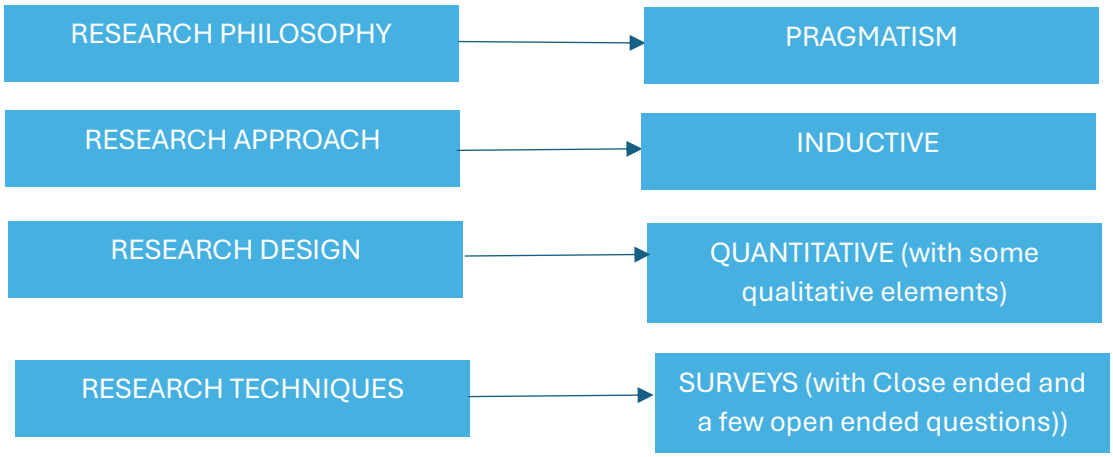


Figure 3.1: Overview of Research Process

The Saunders' Research Onion framework is used in this dissertation to guarantee a methodical, cohesive, and well-justified research process. This approach offers a methodical framework for organizing research methodology, assisting researchers in making consistent and rational choices about everything from data collecting and analytic strategies to philosophical stance. Saunders et al. (2019) created the Saunders' study Onion, a structured framework that helps researchers navigate the phases of study design. It is represented as an onion with six interconnected layers that progresses from general philosophical underpinnings to particular approaches, guaranteeing methodological clarity and clarity.

The six layers include:

1. **Research Philosophy** – The overarching worldview (e.g., pragmatism, positivism).
2. **Research Approach** – The logic of reasoning (inductive or deductive).
3. **Methodological Choice** – Selection of quantitative, qualitative, or mixed methods.
4. **Research Strategy** – The method for data collection (e.g., surveys, case studies).
5. **Time Horizon** – The timeframe of the research (cross-sectional or longitudinal).
6. **Techniques and Procedures** – Specific tools used for collecting and analysing data(Saunders *et al.*, 2009).

The layers of Saunders' Research Onion were implemented in this dissertation is as shown in the figure below.

Research Philosophy-Pragmatism

The study takes a pragmatic approach, emphasizing useful results and answers to pressing problems. Pragmatism is appropriate for evaluating insider threats from both a technological and a human standpoint since it encourages the use of both objective (quantitative) and subjective (qualitative) data.

Research Approach- Inductive

In order to extract patterns, themes, and insights from the data, an inductive technique was employed. For exploratory research with little theoretical underpinning, like comprehending new types of insider risks in EHR systems, this is appropriate.

Methodological Choice – Primarily Quantitative with Some Qualitative Elements

The study mostly uses a structured survey and a quantitative technique. Open-ended inquiries are used, nevertheless, in order to get qualitative data. This makes it possible to collect quantifiable data and have a better grasp of the viewpoints of medical professionals.

Research Strategy – Survey

Data from experts was gathered using a survey-based approach. This is a useful technique for compiling extensive information on insider danger perceptions, experiences, and mitigation tactics.

Time Horizon – Cross-Sectional

A cross-sectional design was employed, capturing data at a single point in time. This provides a snapshot of current practices and challenges related to EHR security.

Techniques and Procedures – Structured Questionnaire & Data Analysis

A systematic questionnaire that included both closed-ended questions for statistical analysis and a few open-ended questions for thematic analysis was used to gather data. In order to find important themes and insights, thematic analysis was used to examine qualitative replies, while regression analysis, frequency distributions, and descriptive statistics were used to analyze quantitative data.

The following section describes detailed insight to each layer of the onion.

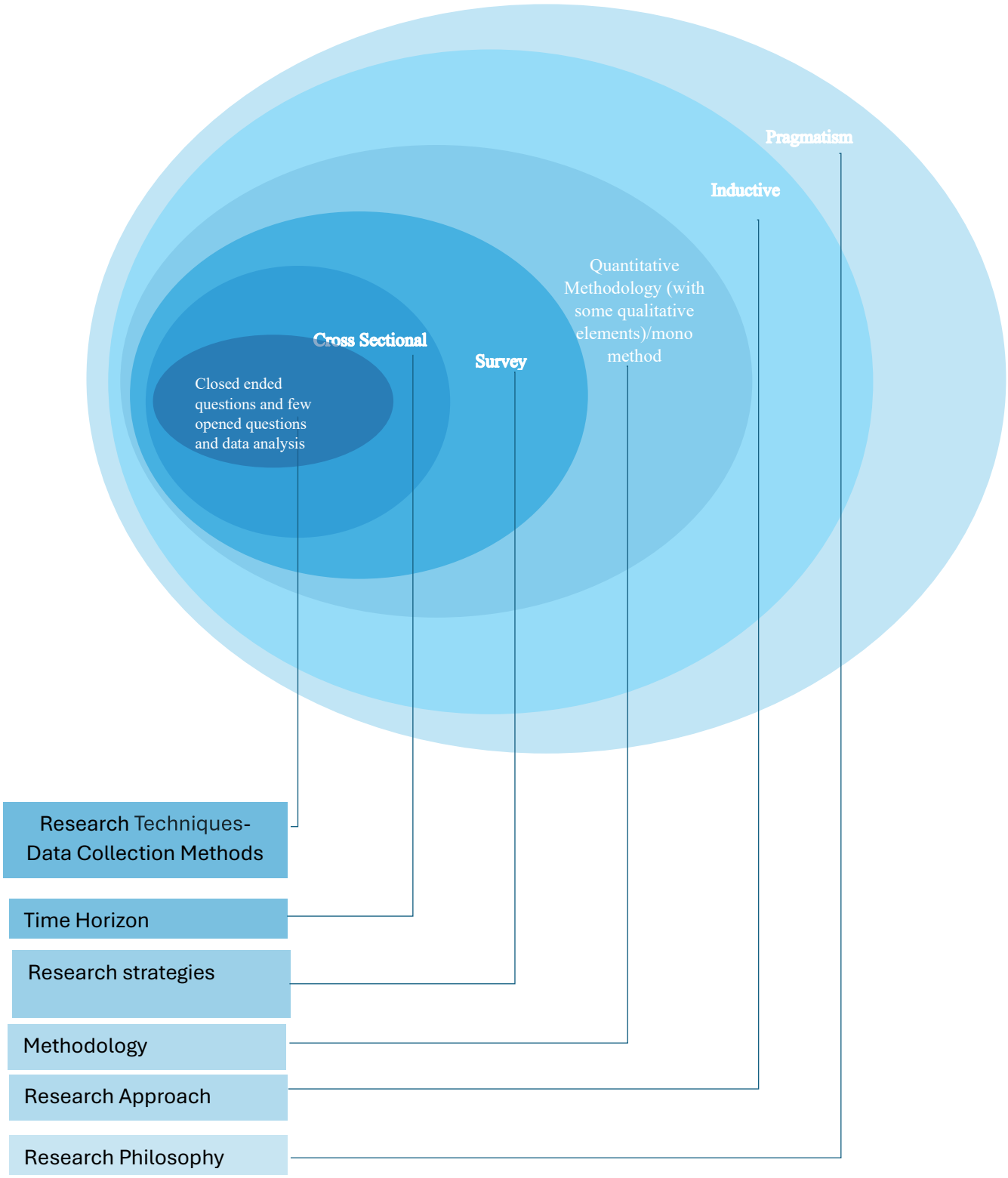


Figure 3.2 Saunder Research Onion

Source: Developed by author

3.2 Research Philosophy and Approach

The research philosophy selected for this study was pragmatism, which places an emphasis on useful results and real-world applications. Pragmatism respects both objective and subjective viewpoints and is not limited to a single system of thought. Instead of strictly following a certain approach, it concentrates on coming up with workable answers to real-world issues. This strategy fit in nicely with the study's goal of examining insider threats in Electronic Health Records (EHR) systems, a field that necessitates contextual knowledge and empirical analysis in order to create effective security measures.

The research philosophy chosen for this study, pragmatism, is justified due to its emphasis on practical results and methodological flexibility, which allow the best approaches to be used to solve challenging, real-world issues. In contrast to strict frameworks that only emphasize quantitative or qualitative methods, pragmatism values diversity and permits researchers to use both techniques to provide thorough and useful discoveries. This way of thinking prioritizes what actually works in practice, appreciating theories and approaches that can be modified and improved in accordance with how well they address the research topic. Given the complexity of insider threats in Electronic Health Records (EHR) systems, pragmatism encourages an integrative strategy that takes into account contextual variations as well as measurable patterns(King, 2022).

Additionally, the study's objective of generating results with practical significance and influence is in line with pragmatism. It promotes adaptability in both research design and data gathering, which is crucial when investigating complex and dynamic phenomena like insider threats. Through the integration of various viewpoints and information sources, pragmatism promotes a deeper comprehension of the problem, aiding in the creation of workable solutions and well-informed policy suggestions. In order to keep the research current and based in real healthcare settings, this flexibility also enables the researcher to react to new information that comes up during the study(Allemang *et al.*, 2022). This adaptability is essential in research that examines insider threats from both a technological and human perspective, as quantitative data could not fully convey the extent of the problem. The study can take a problem-centered and outcome-oriented approach by adopting a pragmatic mindset, with an emphasis on generating findings that are significant to researchers, practitioners, and policymakers alike(Kaushik and Walsh, 2019).

An inductive approach was employed in this study to allow patterns and theories to emerge from the data. Instead of starting with a predetermined premise, this approach encourages the investigation of insider dangers using practical feedback from medical experts. The inductive approach is especially well-suited to this study because there isn't much research in this particular field, which makes it possible to find new themes, behaviours, and mitigation techniques. Additionally, it supports discoveries that are based on factual data and applicable to real-world situations, which enhances the pragmatic philosophy. This method aids in the development of well-informed and efficient countermeasures by revealing the underlying causes, motives, and vulnerabilities linked to insider threats in EHR systems(Thomas, 2006).

3.3 Methodological Choice

A quantitative survey approach is the primary methodological choice for this study on insider risks in Electronic Health Records (EHR), with open-ended questions included to provide qualitative components. A wide range of healthcare personnel (such as doctors, nurses), administrators, IT specialists, and others who work with and oversee EHR systems will have their quantifiable data systematically gathered using this hybrid method. All key stakeholders involved in EHR security and data handling are guaranteed to provide insights thanks to this broad scope.

Focus on Quantitative Analysis

Quantitative surveys make it possible to get organized information about the types, impacts, and efficacy of security measures against insider threats in EHR systems. Statistical analysis of this data can reveal trends, correlations, and risk factors among various roles and organizations, offering objective evidence of insider threat difficulties and the effectiveness of mitigation. Administrators and IT specialists are included in the study to provide a comprehensive understanding of security procedures, governance, and technical protections in healthcare institutions. This is especially crucial because administrators are in charge of rules and compliance, while IT specialists are in charge of system security and access controls(Clifton, 2024).

A large percentage of healthcare data breaches are caused by insider threats, according to the HIPAA Journal (2023), underscoring the need for strong security procedures including staff members at all organizational levels. In order to evaluate the efficacy of these protocols and gauge compliance with them, quantitative data is essential(Alder, 2023c). Through the analysis of user access patterns and behaviours, machine learning and anomaly

detection techniques—which rely significantly on quantitative data—have been effectively applied to Electronic Health Record (EHR) datasets in order to uncover insider threats. These techniques highlight how crucial quantitative methods are to creating automated and scalable security solutions(Hurst *et al.*, 2022).

Additionally, quantitative surveys make cross-sectional studies easier, giving researchers a thorough picture of insider threat knowledge and mitigation strategies in a range of healthcare settings. Because insider threats in healthcare settings are so complex and varied, this is especially important.

Complementary Qualitative Elements

Open-ended questions enhance the quantitative data by delivering more in-depth information about particular insider threat instances, organizational reactions, and opinions of the efficacy of mitigation strategies, all of which contribute to a more complex understanding of the problem.

This method's quantitative assessment of prevalence and impact across various professional occupations strikes a good balance between breadth and depth, as does the qualitative investigation of contextual factors. The goal of the study is to properly examine insider threats in EHR systems, and this fits in nicely with that goal. Furthermore, by facilitating effective data gathering from time-pressed managers, IT staff, and healthcare experts while capturing a variety of viewpoints, this method overcomes practical limitations.

3.4 Research Strategy

A survey-based method was used to collect information from specialists and medical professionals. Since surveys are very good at gathering a lot of data from a wide range of people in a short amount of time, this approach was chosen. When it comes to insider threats to Electronic Health Records (EHR), a survey allows for the methodical gathering of comprehensive information about the opinions, experiences, and defensive strategies of those who work directly with or are affected by EHR systems.

By using a survey approach, data collecting may be standardized, guaranteeing that different respondents will provide the same kinds of information. When examining complicated topics like insider threats, where organizational procedures and subjective experiences might differ greatly, this is especially helpful. Through the use of structured questions, including multiple-

choice, Likert scales, and rating items, the survey collects quantitative data that can be statistically examined to find recurring patterns, trends, and connections.

The purpose of the study was to collect comprehensive data on insider threats in Electronic Health Records (EHR), with an emphasis on risk perceptions, event experiences, effects on healthcare organizations, security mechanisms in place, and mitigation techniques. In order to ensure a thorough demographic profile, multiple-choice questions enabled respondents to identify their employment roles, years of experience, and knowledge with EHR systems.

The effectiveness of current security procedures was evaluated, along with the frequency and perceived seriousness of insider threats, using Likert scale questions. For example, respondents used a scale ranging from "rarely" to "always" to indicate how frequently insider threats endanger the security of EHRs. Participants were asked to rank the implications of insider threats, including monetary loss, legal ramifications, and reputational harm, according on their relative importance.

In order to determine awareness and firsthand experiences with insider threat situations, dichotomous yes/no questions were used. For instance, the question "Have you ever encountered or heard of an insider threat incident in your organization?" was designed to measure the degree of exposure that healthcare professionals had. Questions on a rating scale, like "How effective are your organization's policies in addressing insider threats?" evaluated the frequency of training and the perceived efficacy of security measures. The ratings range from "Not effective at all" to "Very effective." This methodical methodology made it possible to gather solid, diverse data that would aid in a thorough examination of insider threats in EHR systems.

Additionally, by including open-ended survey questions, participants are able to share more details about their experiences and recommend other mitigation techniques, which gives the results more qualitative depth. Measurable facts and detailed viewpoints are combined in this method to enhance the overall study.

The survey's focus on professionals and experts from a range of healthcare roles—including doctors, nurses, IT specialists, and administrative staff—is crucial because it guarantees that the data represents a thorough comprehension of insider threats from a variety of perspectives within healthcare organizations. The research findings' validity and usefulness are improved by this diversity. By effectively obtaining comprehensive, pertinent, and useful data on insider

threat threats, their effects, and efficient security measures in healthcare settings, the survey-based research approach is often well-suited to accomplishing the study's goals.

3.5 Collection of Primary Data

Participants for this study were accessed primarily within the geographic region of Kerala, India, which focused on medical professionals and specialists working with Electronic Health Records (EHR) systems, a combination of professional networks, healthcare facilities, and social media platforms were used. A wide range of healthcare positions, including physicians, nurses, IT specialists, and administrative personnel, were able to get the survey thanks to partnerships with professional associations and healthcare organizations. Healthcare workers frequently use social media sites like Facebook and LinkedIn for communication and professional development, thus these channels were aggressively used to reach a wider and more varied audience.

A strong response rate was also ensured by sending follow-up reminders along with email invites to well-known opinion leaders and experts in the sector. Because of its accessibility, ease of use, and capacity to standardize data collecting using a variety of question forms, including multiple-choice, Likert scales, binary yes/no questions, rating scales, and open-ended responses, Google Forms was used to administer the survey.

The study did not involve vulnerable populations, so specific ethical concerns related to such groups were not relevant. The Griffith College Ethics Committee (GCEC) is responsible for reviewing research projects before they begin to evaluate ethical considerations and offer guidance, support, and approval to researchers. To comply with these requirements, a Research Ethics Approval Form was completed, which required postgraduate students and staff to reflect on the ethical aspects of their research proposals and include an information sheet as part of their ethics application.

Informed consent was a key principle in this study. Participants received comprehensive information about the study’s objectives, procedures, potential risks, and benefits prior to participation. They provided electronic informed consent before completing the survey. The consent forms were straightforward and easy to understand, clearly outlining the nature of the research, any possible risks, and emphasizing that participation was voluntary. Participants were also informed that they could withdraw from the study at any time without any negative consequences. To ensure confidentiality, all responses were anonymized, and data were securely stored with encryption. Participants were assured of confidentiality, with clear

explanations about any legal limits to confidentiality. No coercion or undue incentives were used to obtain consent.

The ethical approval process began with completing Griffith College's Ethics Approval Form, which was reviewed and discussed with the research supervisor. After proofreading and supervisor approval, the application was submitted to the GCEC. Data collection only commenced after receiving written approval from the committee. The GCEC meets roughly four times a year, or more frequently if necessary, to review research proposals promptly. Any recommended changes or ethical improvements suggested by the committee were incorporated into the research to ensure full compliance with ethical standards.

Sample Size Calculation

A 95% confidence level and a 5% margin of error were used to calculate the sample size, which was based on the estimated population of healthcare professionals in Kerala who work with Electronic Health Records (EHR)—roughly 4,950 to 14,940 people across public and private healthcare facilities. Approximately 370 respondents were found to be the minimum sample size needed to ensure statistical validity using the conventional sample size methodology.

Given an anticipated response rate of roughly 30%, which is in line with global averages for surveys of healthcare professionals, which typically fall between 45% and 53%, the survey was sent to a minimum of 1,283 prospective respondents. While taking partial submissions and non-responses into consideration, this distribution technique sought to reach the desired sample

The sampling frame included clinicians, nurses, administrative staff, and IT specialists working in Kerala's estimated 653 public healthcare facilities and approximately 337 private hospitals, where each site employs between 5 and 15 personnel interacting with EHR systems. This approach ensured representation across diverse roles and healthcare settings within the state's comprehensive eHealth ecosystem.

This sample size and distribution plan aligns with best practices in healthcare survey research and supports reliable, generalizable insights into insider threats and mitigation strategies in Kerala's EHR environment.

3.6 Data Analysis

Frequency distribution and the chi-square goodness-of-fit test were the two primary statistical methods used to analyse the quantitative data obtained from the insider-threat survey

in order to guarantee a comprehensive analysis of the responses. In order to (1) identify distinct patterns in the data and (2) determine whether the observed response distributions deviated from the expected distributions if each category were selected equally frequently, these methods were employed.

First, frequency-distribution analysis was used for each closed-ended question. A thorough picture of the distribution of responses across work positions, awareness levels, perceived impacts, security controls, and chosen mitigation strategies was provided by this summary of the frequency of selection of each option. By translating counts to percentages, we could rapidly determine the most prevalent trends, such as the sort of insider threat that is thought to occur most frequently, the extent to which multi-factor authentication is used, and the most severe obstacles to the successful implementation of policies.

In order to determine whether these observed patterns differed significantly from a uniform (equal-probability) distribution, important elements as mitigation preferences, impact rankings, and perceived policy success were subjected to the chi-square goodness-of-fit test (χ^2). Under the null hypothesis, which holds that all categories have an equal probability, the test compared observed frequencies with expected frequencies. In comparison to chance predictions, at least one group was either under-represented or preferred when the p-value was less than 0.05, which was considered statistically significant.

The choice of frequency distributions and χ^2 tests is justified by their ability to deliver both descriptive clarity and inferential rigour, thereby producing actionable insights into insider-threat dynamics within Electronic Health Records systems. All analyses were performed in **Minitab v22.2.2/Excel**, whose advanced statistical functions ensured accuracy and rapid visualisation.

3.7 Conclusion

This chapter has mapped out a clear, step-by-step plan for studying insider threats to Electronic Health Records. Anchored in a pragmatic worldview and structured with Saunders' Research Onion, the project pairs an inductive, survey-driven design with select open-ended questions. A cross-sectional questionnaire—distributed to healthcare staff across Kerala under strict ethical protocols and a statistically sound sampling frame—delivers data suitable for rigorous examination.

Applying frequency tables, chi-square tests, and thematic analysis allows numerical trends to be weighed against participant narratives, ensuring the results are both reliable and practically meaningful. In short, the philosophical stance, chosen methods, and analytic tools all converge on one aim: generating evidence that hospitals and policymakers can use to tighten EHR security. This methodological framework therefore underpins the credibility of the findings and recommendations in the next chapters.

4.Findings and Analysis

4.1 Overview:

The findings of this study offer important new information about the impact, awareness, and perceptions of insider threats to Electronic Health Record (EHR) systems in healthcare environments. Aspects such as the kinds and frequency of insider threats that healthcare workers face, the perceived dangers to the security of electronic health records, and the impact of these threats on operational, financial, legal, and reputational outcomes are all included in the report. The survey also looks at how well-functioning current corporate policies and security measures—like staff monitoring, encryption, anomaly detection, access limits, and training initiatives—are. Responses from different employment titles and types of institutions were compared using statistical tests, such as Chi-squared analysis. The results show the most successful mitigation techniques, including policy governance, staff training, and AI-driven security solutions, as well as the main obstacles. Furthermore, suggestions for strengthening insider threat defences are given by qualitative comments. In summary, the study provides a thorough understanding of insider threats to electronic health records and informs ways to increase patient trust in healthcare institutions and data security.

4.2 Demographics of Respondents

4.2.1 Job Role Distribution

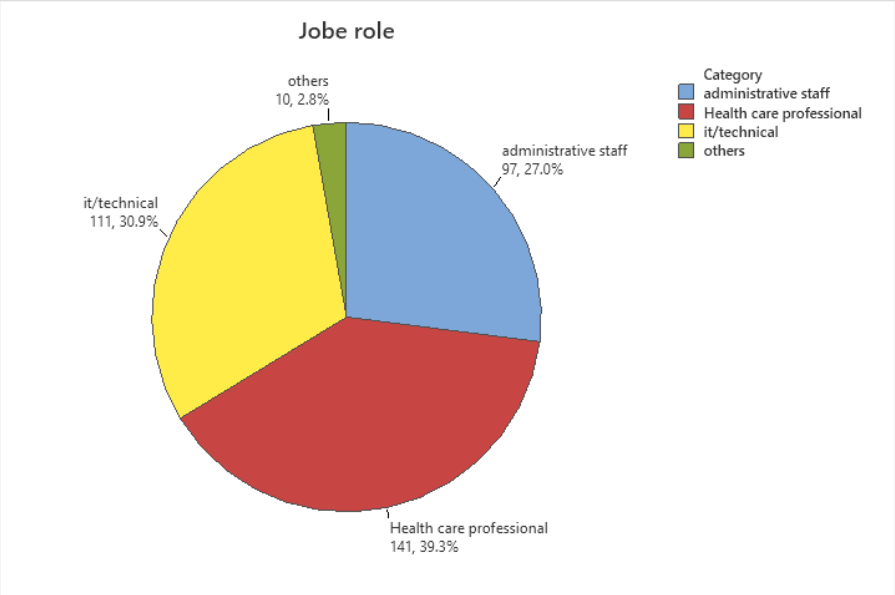


Figure 4.1: Distribution of Survey Participants by Job Role *Source: Developed by author*

This pie chart above shows how survey respondents were distributed based on their roles in the healthcare industry. Health care workers make up 39.3% (141 participants) of the total respondents, which is the greatest percentage. With 111 participants, IT/technical staff accounts for 30.9%, making them the second largest category. A small minority of 2.8% (10 participants) fall into the "others" category, which may include positions like contractors or outside vendors. Administrative staff make up 27.0% of the total (97 participants).Because of this varied representation, opinions on insider risks to EHR systems are represented from a variety of backgrounds, including technological, administrative, and clinical ones. The significant representation of IT/technology personnel and health care professionals emphasizes the value of both clinical and technical knowledge in resolving EHR security concerns.

4.2.2 Experience Level of Respondents

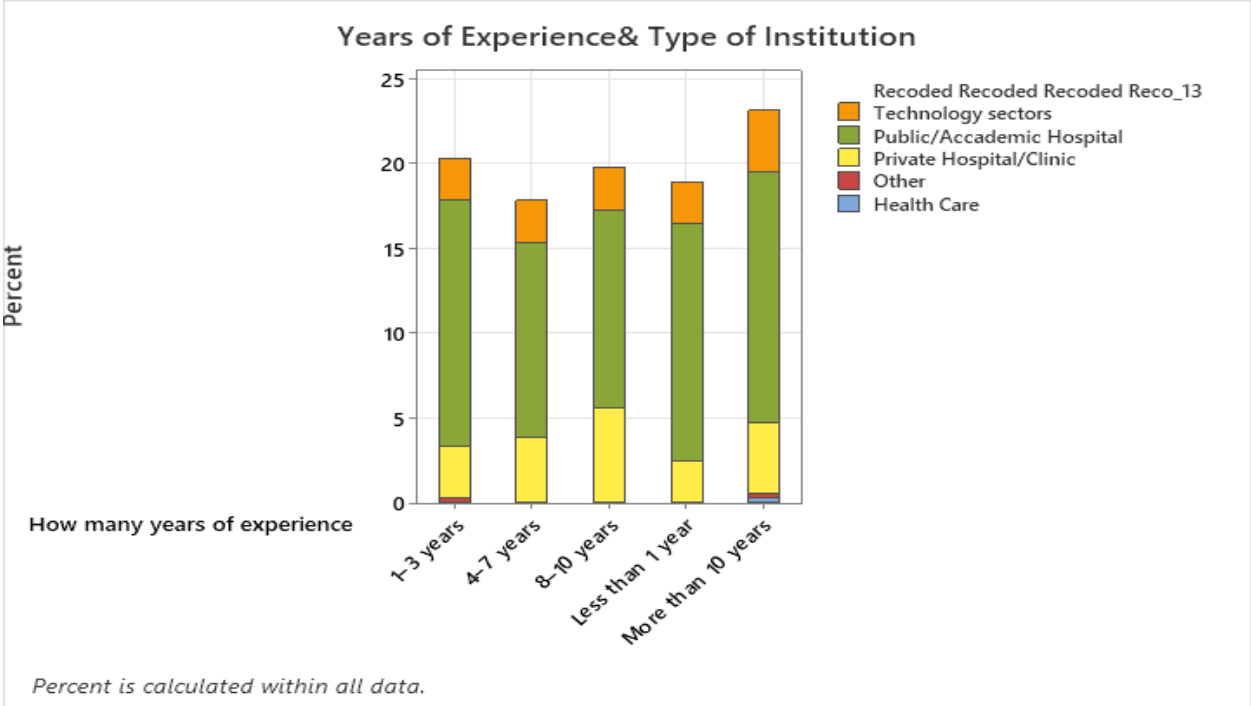


Figure 4.2 Frequency distribution of experience and type of institution *Source: Developed by author*

The distribution of survey respondents by years of experience and kind of institution is displayed in the stacked bar chart above. Across all experience levels, private clinics and hospitals (green) account for the highest percentage, followed by university and public hospitals (yellow). Smaller shares are represented by the technology, other, and healthcare industries. Strong representation of seasoned professionals is indicated by the fact that the "More than 10 years" category is the largest overall. This distribution captures a wide range of viewpoints on insider risks to EHR systems by reflecting a variety of expertise levels and institution types.

The participants' distribution according to years of experience in their current field is summarized in the table below. Out of the 359 responders, 83 participants, the largest group, 23.12%, have more than ten years of experience. Individuals with 1–3 years of experience make up 20.33% of the sample (73 participants), while those with 8–10 years make up 19.78% (71 participants). 18.94% (68 participants) and 17.83% (64 participants) of the participants have less than one year of experience, and those with four to seven years of experience, respectively. There is a fairly balanced distribution of early-career and more experienced professionals, with a mean of almost 6 years of experience (Mean = 6.04, SD = 4.38), and a median of 5.5 years.

Tally

How many years of experience	Count	Percent
1–3 years	73	20.33
4–7 years	64	17.83
8–10 years	71	19.78
Less than 1 year	68	18.94
More than 10 years	83	23.12
N=359		

Statistics

Variable	Mean	StDev	Median
Recoded How many years of exper	6.03621	4.37985	5.5

Table 4.1: Distribution of Survey Participants by Years of Experience *Source: Developed by author*

4.2.3 Familiarity and Frequency of Usage of EHR system

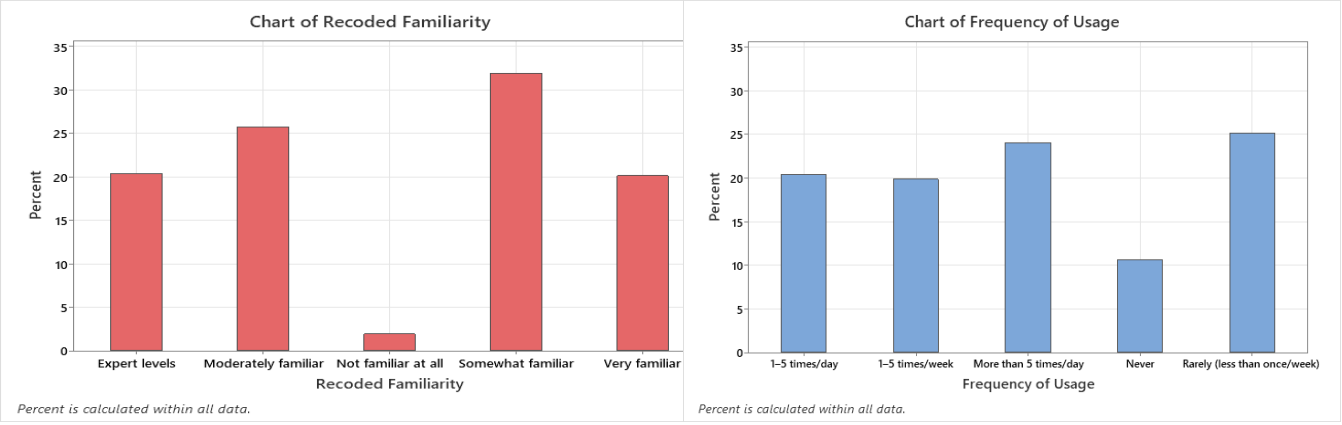


Figure 4.3: Record of Familiarity and frequency of Usage *Source: Developed by author*

According to the above figure, the majority of respondents are at least somewhat familiar with EHR systems; the most prevalent category was "Somewhat familiar," which was followed by "Moderately familiar." Very few respondents said they were completely unfamiliar. EHR systems are used by the largest groups either infrequently (less than once a week) or more than five times a day, while a smaller percentage use them daily or weekly, and only a small percentage never use them, according to the frequency of usage chart. This implies that although respondents have a generally high level of knowledge with EHR systems, their actual utilization patterns vary.

Rows: Familiarity Level Columns: Frequency of Usage	1–5 times/day	1–5 times/week	More than 5 times/day	Rarely
Expert level (designs, administers, or secures EHR systems)	12	15	26	20
Moderately familiar	28	18	17	29
Not familiar at all	2	1	0	4
Somewhat familiar	13	21	21	60
Very familiar	18	17	22	15

Table4.2: Familiarity Level and Frequency of Usage *Source: Developed by author*

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	37.371	12	0.000
Likelihood Ratio	38.539	12	0.000

Table 4.3 : Chi-Square Test *Source: Developed by author*

The distribution of respondents' varying degrees of familiarity with EHR systems and how frequently they use them is displayed in the tables above. For instance, the largest percentage of Expert level users (26) utilize EHR systems more than five times per day, whereas the smallest percentage (12) use them one to five times per day. The majority of respondents who are somewhat familiar (60) fall into the Rarely usage category, which denotes less regular use eventhough they are somewhat familiar. The findings of the Chi-Square test show a statistically significant correlation between the frequency of EHR usage and familiarity level (Pearson $\chi^2 = 37.371$, df = 12, $p < 0.001$). This indicates a substantial correlation between a respondent's familiarity with EHR systems and their frequency of use.

Interprectation: While users who are less familiar with EHR systems tend to use them infrequently, more experienced users—experts and extremely familiar—tend to utilize them more frequently. It is evident from this association that higher usage frequency is associated with greater familiarity.

4.3 Awareness of Insider Threats

The understanding and experiences of healthcare workers with regard to insider threats to the security of Electronic Health Records (EHRs) are examined in this section. It looks at respondents' assessments of the most prevalent threats—malicious, careless, or unintentional—as well as their awareness of the risks and experiences with insider threat occurrences. It also evaluates the frequency with which participants think insider threats endanger the security of EHRs, offering information about the perceived seriousness and frequency of these issues at healthcare institutions.

Source: Developed by author

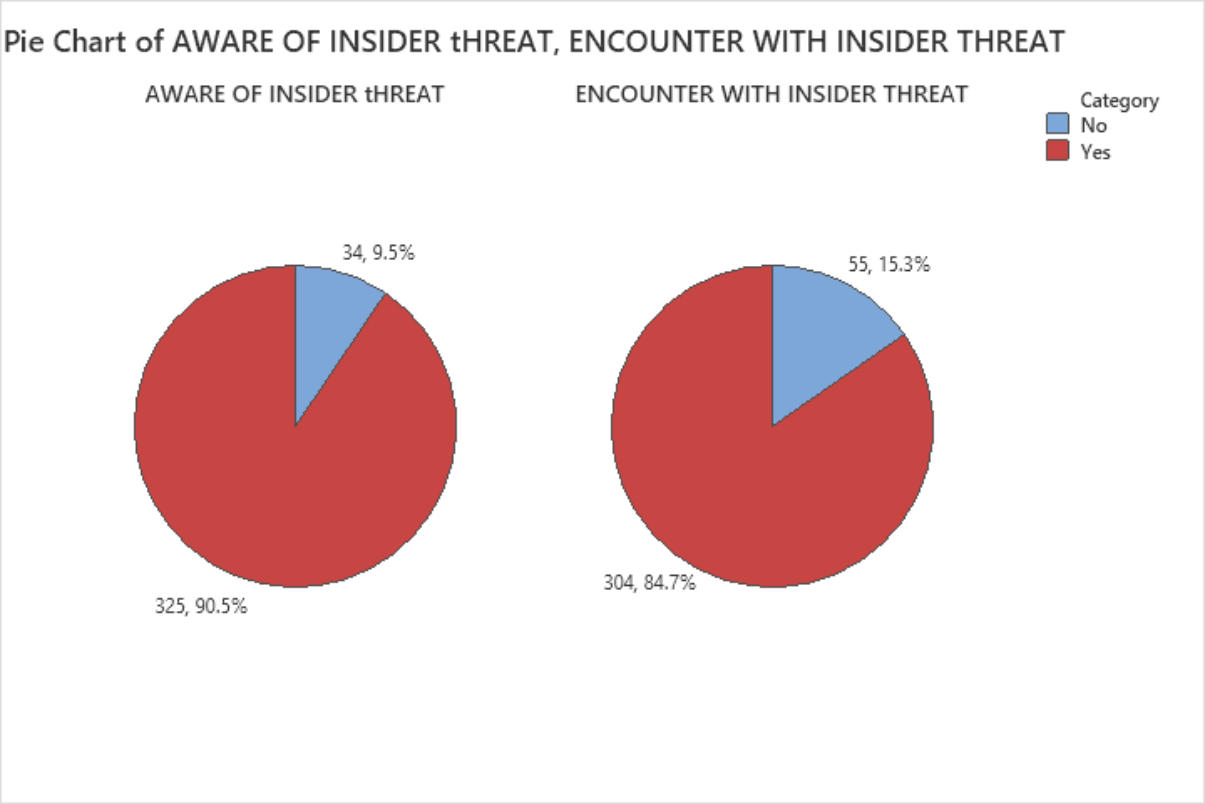


Figure 4.4: Awareness and Personal Encounter with Insider Threats among Respondents (N = 359)

The picture displays two pie charts that summarize survey results about insider threats to the security of electronic health records (EHRs). Only a tiny percentage of respondents (34, or 9.5%) are unaware of insider threats to EHR security, according to the Aware of Insider Threat pie chart. The majority of respondents (325, or 90.5%) are aware of these concerns.

According to the Encounter with Insider Threat pie chart, the majority of respondents (304, or 84.7%) have either heard of or experienced an insider threat occurrence within their ompany. A smaller sample has not experienced this, consisting of 55 individuals, or 15.3%. These figures show how common insider threats are in EHR systems and how the majority of survey respondents are aware of them as well as having either heard of or experienced such instances at work.

4.3.1 Insider Threats Types and its frequency of occurrence

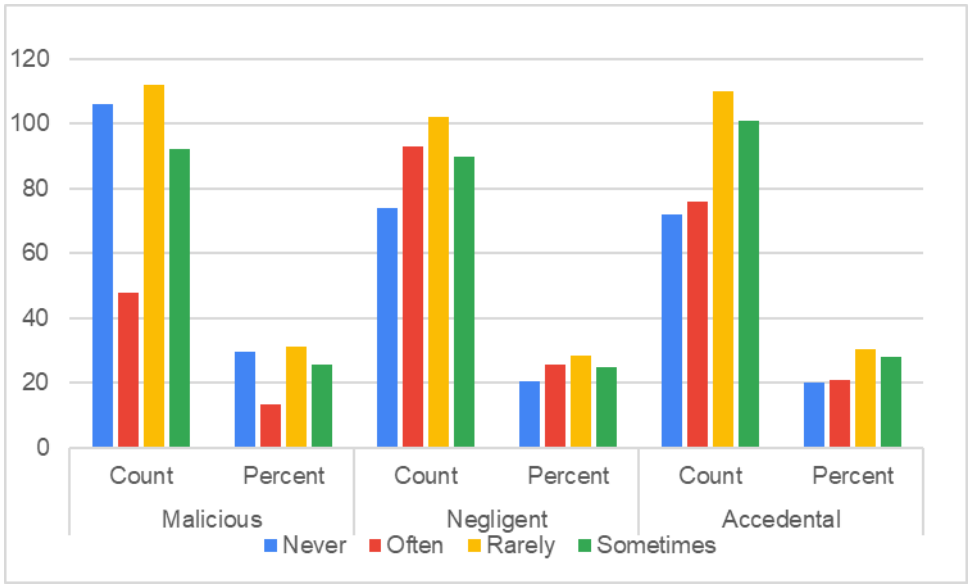


Figure 4.5: Frequency of Insider Threat Types by Category *Source: Developed by author*

The bar graph above contrasts the perceived frequency of three categories of insider threats—Malicious, Negligent, and Accidental—in organizations according to survey data. Malicious Threats (yellow bars) are scored as "Rarely" more often than "Sometimes" or "Often," with over 140 replies. Malicious insider threats are acknowledged, although they are not regarded as often, as indicated by the moderate proportion of respondents who chose "Never." Fewer respondents selected "Never," while the most common ratings for Negligent Threats (blue bars) are "Sometimes" (approximately 150 responses) and "Rarely" (about 140). This implies that careless threats are thought to occur more frequently than malevolent ones. Green bars for

accidental threats show a similar trend to those for negligent threats, with large numbers for "Sometimes" and "Rarely," but also a noteworthy quantity for "Often," suggesting that unintentional errors are a common worry. Insider threats that are careless or unintentional are seen as happening more regularly ("Sometimes" and "Often") than malicious ones, which are typically thought of as uncommon. This demonstrates how carelessness and inadvertent behavior are viewed as greater threats to EHR security than purposeful malevolent behavior.

4.3.2 Frequency of Threat Perception

Source: Developed by author

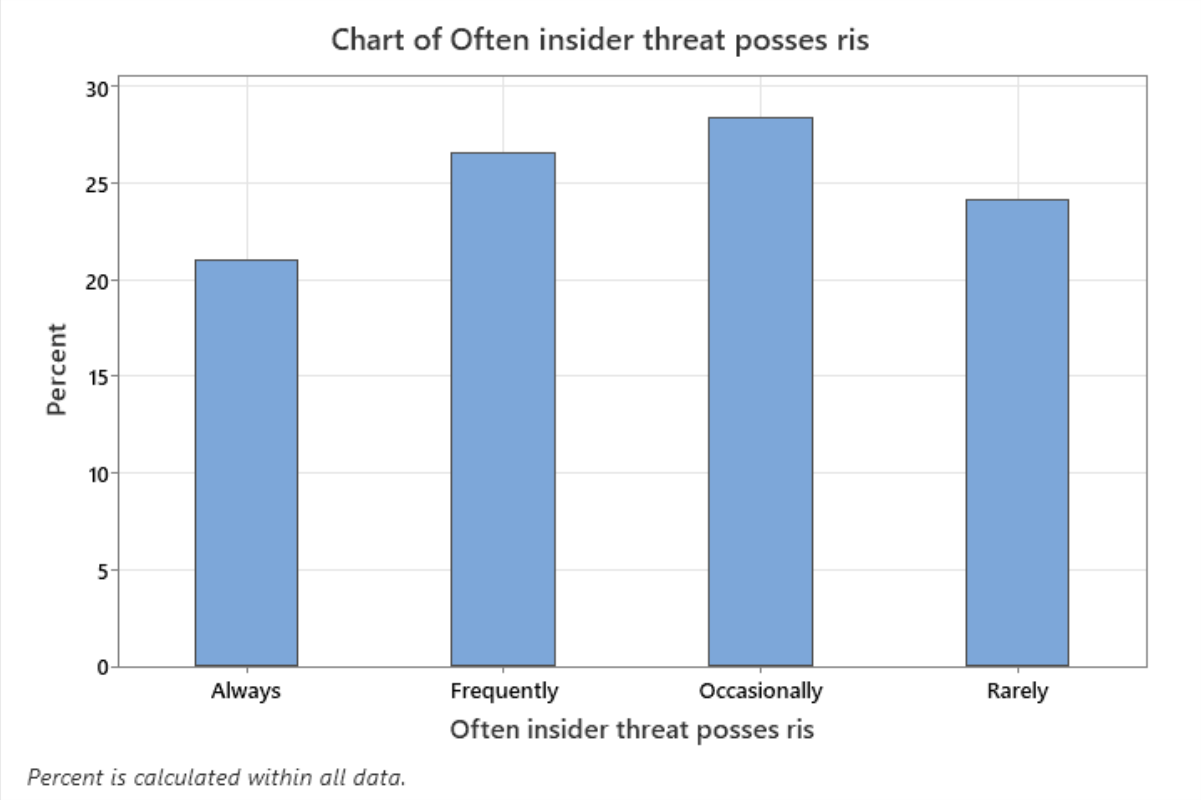


Figure 4.6: Respondents' Perception of Insider Threat Risk Frequency in EHR Systems

The frequency with which respondents think insider threats endanger the security of Electronic Health Records (EHRs) is depicted in the bar chart.The majority of participants consider insider threats to be a frequent worry, as seen by the most prevalent responses, Occasionally (around 29%) and Frequently (about 27%).Only a minority perceive insider threats as either infrequent or persistent, as evidenced by the less prevalent but still substantial responses of Rarely (24%) and Always (21%).

Statistics *Source: Developed by author*

Variable	Mean	StDev	Median
Frequency of Threat Perception	2.44444	1.07317	2

Table 4.4: Descriptive Statistics of Insider Threat Frequency Perception

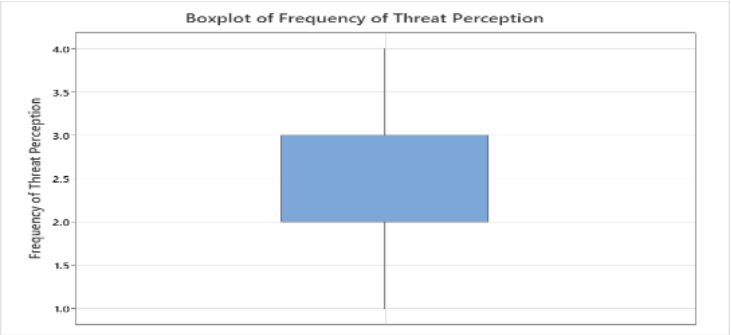


Figure 4.7: Box plot for the statistical information *Source: Developed by author*

According to the statistical summary, there is some variation in the replies, with a mean score of 2.44 and a median of 2 on a scale where lower numbers indicate more frequent perceptions of insider threat danger. The box plot also shows the statistical information. The implication is that respondents generally believe insider threats to EHR security to occur "Frequently" to "Occasionally." According to the interpretation, insider threats are a frequent worry for the majority of participants, highlighting the necessity of constant watchfulness and strong security protocols in healthcare institutions. There is a balanced but continuous awareness of the risk, since only a tiny percentage perceive these hazards as either infrequent or regular.

4.3.3 Thematic Analysis of Data Security Incidents in Healthcare Settings

Six main themes emerged from the thematic analysis of reactions to data security incidents: technological and systemic failures, human mistake, poor response, unauthorized access, lack of staff training, threats from outside vendors, and inadequate response. Lack of audit trails, inability to document data access, system outages, and inadequate identification of unusual access behavior were the most commonly mentioned problems. Unattended screens containing sensitive data, inaccurate patient record updates, and autofill errors in email correspondence were also frequent examples of human error. Insufficient training made employees more

susceptible to phishing attempts and ignorant of proper data handling procedures, which increased the dangers.

Unauthorized access—which is frequently made possible by inadequate role-based controls—including worker eavesdropping and the use of shared logins has become a serious concern. With numerous stories of test database copies and insider exploitation, external vendors also presented risks. A lot of incidents lacked appropriate follow-up or remedial measures. In order to prevent future breaches and guarantee adherence to data privacy laws, the results highlight the critical need for improved security infrastructure, thorough audit and monitoring systems, enforced access controls, required training programs, and well-defined incident response procedures.

Source: Developed by author

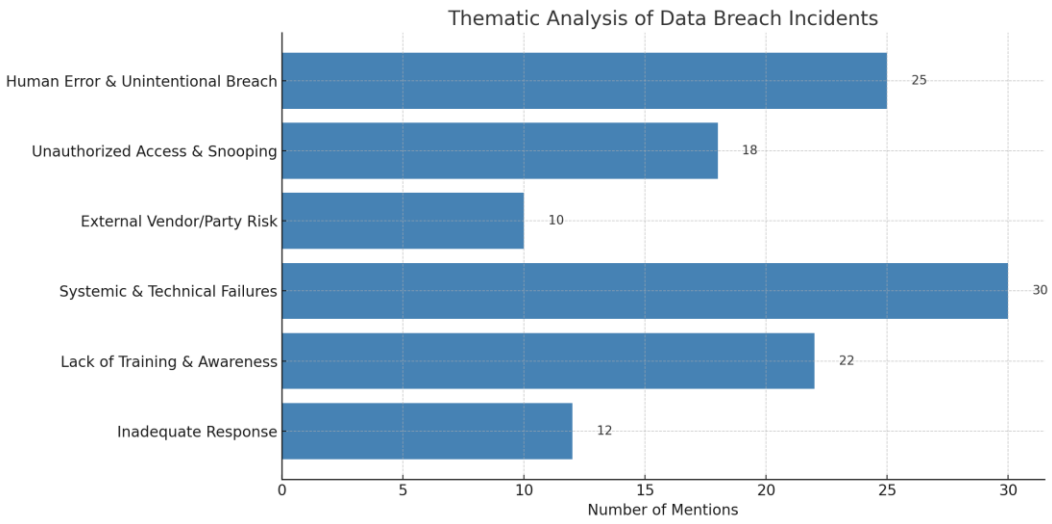


Figure 4.8: Frequency distribution of thematic analysis of data breach incidents

Systemic & Technical Failures: (e.g., EHR downtime, audit trail absence) were the most frequent.

Human Error & Unintentional Breach (e.g., wrong patient data entry) was also very common.

Lack of Training & Awareness (e.g., phishing, improper logout) significantly contributed to breaches.

Unauthorized Access & Snooping incidents showed ongoing concerns around internal misuse.

Inadequate Response (e.g., no action taken) and **External Vendor Risks** (e.g., test DB misuse) were notable but less frequent.

4.4 Impact of Insider Threats

The analysis will summarize perceptions of insider threats' key impacts-financial, legal, operational, and reputational-using frequency counts and rankings. It will assess concern levels about patient data security and evaluate effects on patient trust, clinical quality, and operational efficiency. The presence of insider threat policies will be examined to gauge organizational readiness. Cross-tabulations and visualizations will highlight differences and key insights, guiding effective mitigation strategies.

4.4.1 Impact Distribution

Source: Developed by author

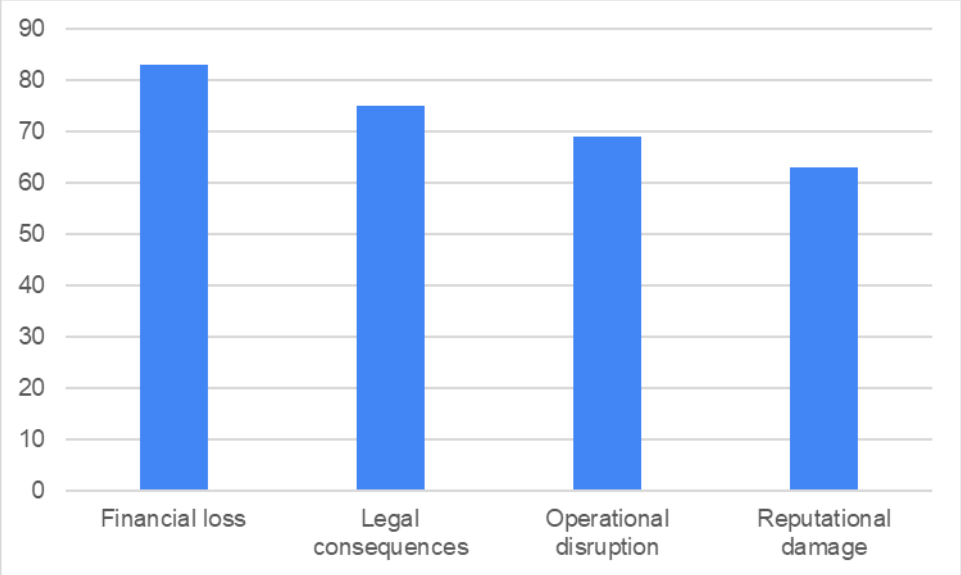


Figure 4.9: Percentage Impact of Insider threat

The bar graph shows the percentage impact of insider threats in four important areas: operational disruption, financial loss, legal consequences, and reputational damage.

Interpretation of the Bar Chart

Financial Loss: The impact in this area is the highest, at about 83%. This suggests that the most common way insider threats cause firms to suffer direct financial losses is through theft, fraud, or lost revenue.

Legal Consequences: About 75% of the damage is in the form of legal repercussions. Legal actions, regulatory fines, or compliance issues are frequently the result of insider threats, and

they can turn to be very much expensive and harmful. Operational Disruption: Approximately 69% of operations are disrupted. This illustrates how insider threats can reduce productivity and raise expenses by interfering with regular corporate activities, causing outages, or disrupting workflows.

Reputational Damage: Although still substantial, reputational harm accounts for the smallest share, at roughly 63%. Even though it comes in last out of the four, reputational damage can have long-term consequences including a decline in market share and customer trust.

Statistics *Source: Developed by author*

Variable	**Mean**	**StDev**	**Median**
financial Loss	3.91	1.13	4
Legal Consequences	3.63	0.98	4
Operational disruption	3.35	1.02	3
Reputational damage	3.10	1.16	3
Other	1	0	1

Table 4.5: Statistical summary of Impact of insider threat

With a mean score of 3.91 and a median of 4, the statistical summary emphasizes that people believe that financial loss is the most serious effect of insider threats. Given the actual costs that insider threats might result in, like as theft, fraud, or lost income, it is clear that the majority of respondents view financial harm as a significant outcome. With a median score of 4 and a mean score of 3.63, legal repercussions also score strongly, highlighting worries about potential legal action, regulatory fines, and compliance infractions brought on by insider occurrences. Relatively consistent replies from both categories indicate widespread consensus regarding their crucial relevance.

With mean values of 3.35 and 3.10, respectively, operational disruption and reputational harm are ranked somewhat lower, but still being noteworthy. These repercussions include disruptions to corporate operations and possible damage to an organization's reputation, which may be seen as less urgent than financial and legal issues but may have longer-term consequences. Divergent views on the severity of reputational damage are indicated by the greater variety in replies. All things considered, the data supports the idea that companies should prioritize preventing insider risks from causing financial and legal harm while simultaneously correcting operational and reputational weaknesses.

Tally *Source: Developed by author*

	financial Loss		Legal Consequences		Operational disruptions		Reputational Damage	
	Count	**Percent**	**Count**	**Percent**	**Count**	**Percent**	**Count**	**Percent**
Rank1	156	43.45	69	19.22	68	18.94	66	18.38
Rank2	77	21.45	150	41.6	67	18.66	65	18.11
Rank3	64	17.6	78	21.73	147	40.95	71	19.78
Rank4	62	17.27	62	17.27	77	21.21	158	44.01
N=358								

Table 4.6 : Ranked Perceptions of Consequences of Insider Threats in EHR Systems

Financial loss is definitely the most severe impact of insider threats, according to the ranking data shown in the table above, with 43.45% of respondents putting it as their top concern. This emphasizes how firms' bottom lines can be directly impacted by the immediate and palpable expenses they incur, such as theft, fraud, or asset loss. The significant ramifications of regulatory fines, litigation, and noncompliance that frequently accompany insider occurrences are reflected in the ranking of legal repercussions as the second most important factor by 41.6% of respondents. These findings demonstrate that when firms deal with insider threats, their top priorities are financial and legal issues.

Most respondents ranked reputational harm fourth (44.01%) and operational interruptions third (40.95%), indicating that these two effects are typically viewed as less significant. Even while these topics might not be thought of as the most pressing, they yet pose significant difficulties. Business continuity and productivity can be impacted by operational disruptions, and while reputational harm is listed lowest, it can have a lasting impact on consumer trust and brand value. The necessity of a well-rounded insider threat management strategy that balances operational and reputational risks with financial and legal protections is highlighted by these observations taken together.

4.4.2 Concern About Insider Threats to Patient Data Security

Source: Developed by author

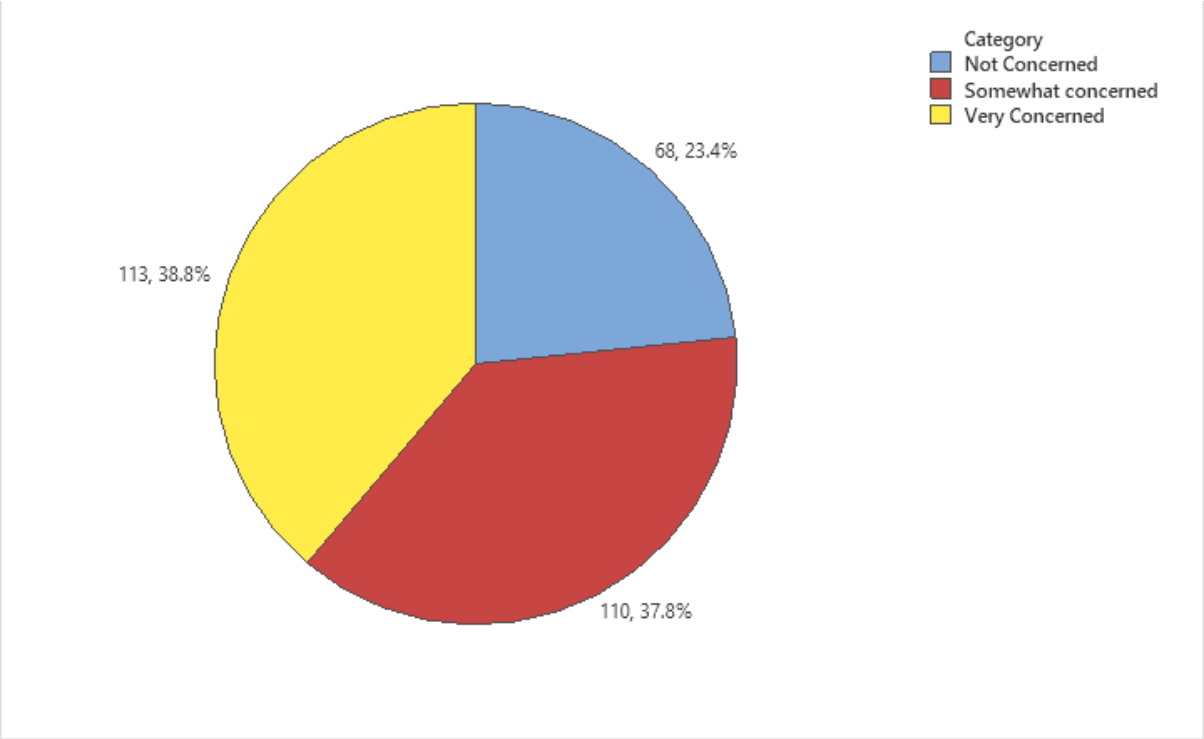


Figure 4.10: Concern Level of Insider threats to patient data security

Source: Developed by author

Responses	Count	Percentage
Very Concerned	113	38.83
Somewhat concerned	110	37.80
Not Concerned	68	23.36

Table 4.7: Frequency of Concern level (N=359)

Regarding participant concerns about insider threats to patient data security, a descriptive analysis was performed. With "Very concerned" being the most often chosen response (113 mentions), the data indicates that a sizable majority of respondents indicated high levels of anxiety. The phrase "Somewhat concerned" was then stated 110 times, suggesting that most participants admit the significance of insider threats, albeit to differing degrees. Conversely, a mere 68 respondents expressed "Not concerned," indicating a comparatively low level of complacency among the sample. A lesser percentage of respondents (60) chose "Not applicable," which may indicate that they are not directly responsible for or aware of data security.

These findings suggest that the risk insider threats represent to patient data security is widely acknowledged by stakeholders and healthcare professionals. A possible need for more robust internal controls, staff training, and risk monitoring systems is reflected in the high degree of worry. Awareness campaigns and data protection rules appear to be having an effect, based on the very small number of unconcerned responses. Institutions may need to address this gap by role-specific training or targeted communication, as the existence of "Not applicable" responses indicates a lack of role-based relevance or understanding.

Rows: Job role Columns: concern level

Source: Developed by author

	very concerned	**Somewhat Concerned**	**not concerned**
Health care professional	64	46	31
	57.66%	43.45%	39.89%
it/technical	48	31	32
	45.39%	34.20%	31.40%
administrative	29	30	38
	39.67%	29.89%	27.44%
Others	5	3	0
	3.27%	2.46%	2.26%
All	146	110	101

Table 4.8: Distribution of Concern level about insider threat by job level

Chi-Square Test

Source: Developed by author

	Chi-Square	**DF**	**P-Value**
Pearson	13.513	6	0.036
Likelihood Ratio	15.646	6	0.016

Table 4.9: Chi-Square test Concern level Vs Job role

There is a statistically significant correlation between work role and the degree of concern regarding insider threats to patient data security, according to the results of the Chi-Square test (Pearson $\chi^2 = 13.513$, $p = 0.036$; Likelihood Ratio $\chi^2 = 15.646$, $p = 0.016$). We can infer that people's levels of concern change significantly depending on their employment role because

both p-values are below the traditional cutoff of 0.05. Concern levels varied statistically significantly by employment type, according to chi-square analysis (p = 0.036). This implies that various security awareness training are required, with an emphasis on technical staff regarding system-level vulnerabilities and response processes, and a focus on clinical staff about real-life circumstances.

It would appear from this that the risk of insider threats is not uniformly perceived by administrative staff, IT/technical staff, healthcare professionals, and others. According to these results, healthcare organizations require customized security and awareness training programs that take into account the unique viewpoints and worries of every work group.

4.4.3 Belief in Financial Impact

Source: Developed by author

BELIF IN FINANCIAL IMPACT	Count	Percent
No	**147**	**40.95**
Yes	**212**	**59.05**
N=359		

Table 4.10: Belief in Financial Impact Due to Insider Threats

The majority of the 359 respondents (212, or 59.1%) think that insider threats can cost healthcare organizations a lot of money, although 147 (40.9%) disagree as summarised in table above. This shows that over half of the people you surveyed are aware of the direct financial hazards that dishonest or careless insiders pose. The large percentage of respondents who said "No" (more than 40%) points to a lack of awareness of the hidden costs that frequently follow insider occurrences, including investigation, remediation, regulatory fines, and reputational harm. All of these findings point to the necessity of more transparent communication of the actual financial risks associated with insider threats as well as cost-effective investments in staff training, detection equipment, and preventative procedures.

4.4.4 Perceived Impact on Patient Trust

Source: Developed by author

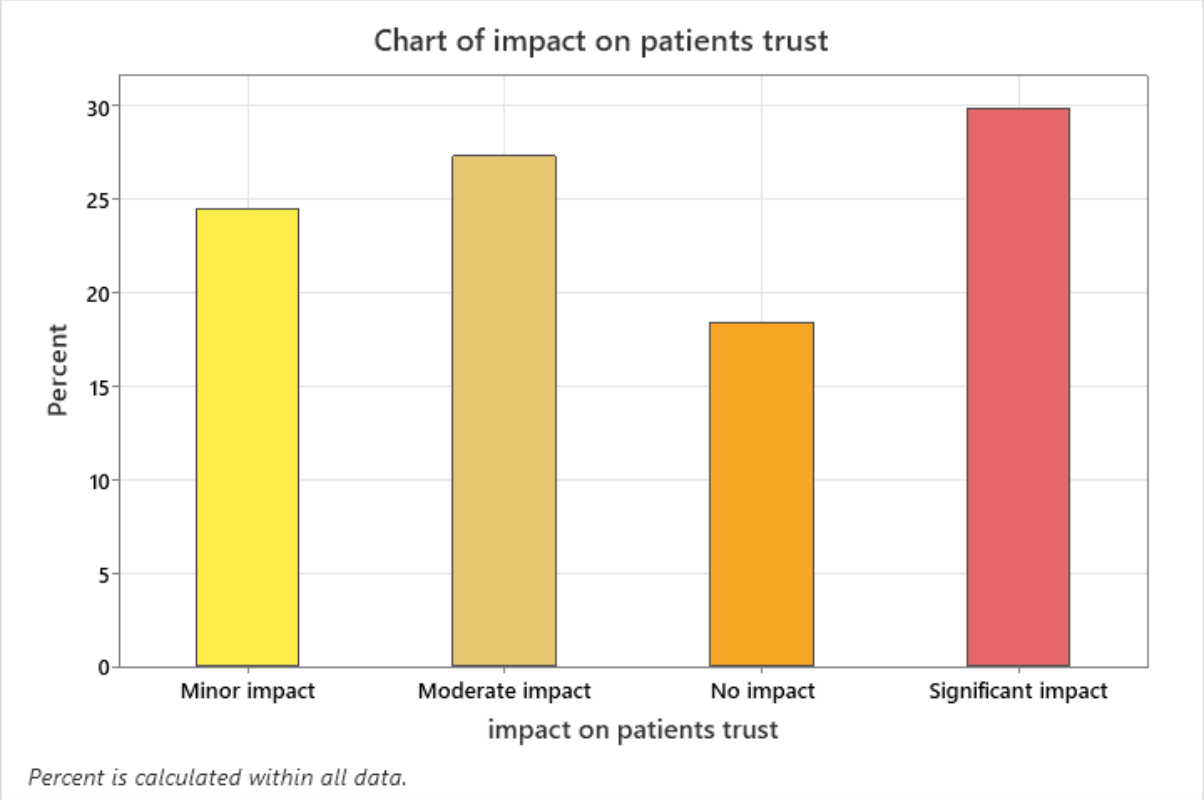


Figure 4.11: Impact Levels on Patient Trust: Distribution by Percentage

Source: Developed by author

impact on patients trust	**Count**	**Percent**
Minor impact	88	24.51
Moderate impact	98	27.30
No impact	66	18.38
Significant impact	107	29.81
N=359		

Table 4.11: Patient_trust_impact_distribution

Most respondents believe that insider threats have at least some detrimental effect on patients' faith in healthcare organizations, according to the statistics shown in table above. In particular, 107 individuals (29.8%) think the impact is large, while 98 participants (27.3%) think it is moderate. When taken as a whole, this indicates that more than half (57.1%) of those surveyed

acknowledge that insider threats significantly undermine trust. Conversely, 88 (24.5%) respondents believe the impact is minimal, while 66 respondents (18.4%) see no impact at all. These results demonstrate the growing concern about how transparency, patient participation, and overall service quality may be impacted by data breaches or internal wrongdoing undermining public trust in healthcare institutions. The bar chart helps to visualise the data which is shown above.

4.4.5 Impact on Clinical Quality

Source: Developed by author

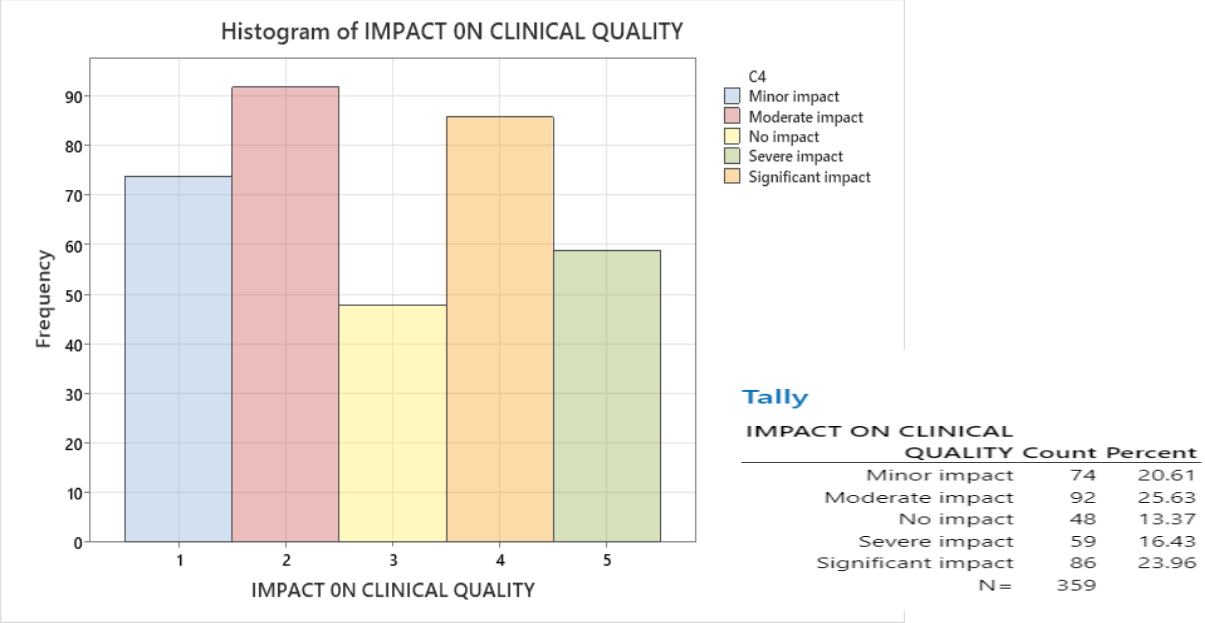


Figure 4.12: Distribution of Impact Levels on Clinical Quality

The majority of respondents think insider threats have at least a moderate effect on clinical quality, according to the histogram. The most common responses were "moderate impact" and "severe impact," but fewer respondents said "no impact." According to this, just a tiny percentage of respondents believed that insider threats had little to no impact on clinical quality. The tally shows that among 6 responses, each category of impact-Minor, Moderate, No, Severe, and Significant-received exactly one count, each representing 16.67% of the total. This indicates an even distribution of opinions, with no single impact level dominating. The responses reflect diverse views on the effect of insider threats, suggesting varied experiences or perceptions within this small sample.

Chi-Square Test *Source: Developed by author*

	Chi-Square	DF	P-Value
Pearson	14.371	8	0.073
Likelihood Ratio	14.853	8	0.062

Table 4.12 : Chi-Square test Jobe role Vs Perceived impact on insider threat.

The results of the Chi-Square test indicate that, with eight degrees of freedom and a p-value of 0.073, the Pearson Chi-Square value is 14.371. According to this finding, there is no statistically significant correlation, at the traditional 0.05 level, between job role and the perceived impact of insider threats. The p-value, however, is near the cutoff, suggesting a possible trend that merits more investigation. Similar results are obtained with the Likelihood Ratio test, which supports this finding with a p-value of 0.062 and a value of 14.853. These findings were not definitive, but they do imply that a more distinct pattern would show up if the sample size were increased or if the category classifications were made simpler.

4.4.6 Impact on Operational Efficiency

A total of 359 respondents provided feedback on the impact of insider threats on healthcare operational efficiency. The majority—32.87%—perceived a significant impact, followed by 24.23% who reported a moderate impact, and 15.88% who indicated a severe impact. In contrast, only 12.53% saw no impact, and 14.48% reported a minor impact. These results show that over 72% of respondents believe insider threats have a moderate to severe effect on operational efficiency, highlighting a strong perceived vulnerability within healthcare operations.

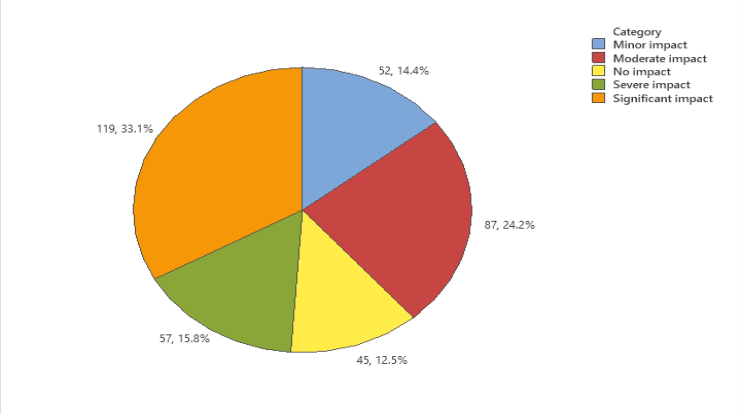


Figure 4.13: Distribution of Impact Levels on Clinical Quality *Source: Developed by author*

4.5. Organizational Security Measures for Insider Threat Mitigation

In order to mitigate insider threats in healthcare settings, this section examines the current organizational rules, technical measures, and staff practices. The kinds of electronic health record (EHR) security measures in place, the frequency of security training, access control mechanisms, the use of monitoring technologies, the existence of explicit insider threat policies, and the perceived efficacy of such policies were all questions posed to the respondents. The results shed light on how healthcare institutions are actively tackling insider threats and highlight any implementation gaps or irregularities. The study also looks at relationships between views of the efficacy of policies, training frequency, and policy presence.

4.5.1 Presence of Insider Threat Policies *Source: Developed by author*

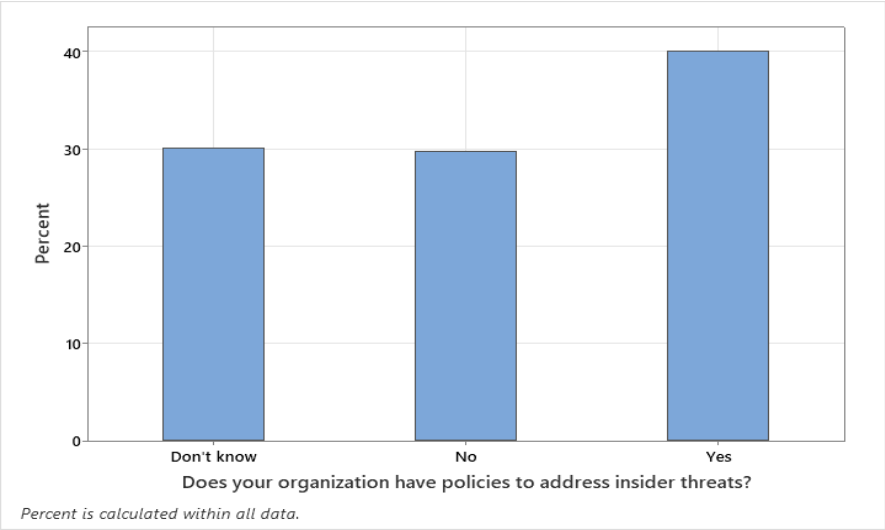


Figure 4.14: Organizational Policies to Address Insider Threats: Response Distribution

Source: Developed by author

	Count	Percent
Don't know	**108**	**30.08**
No	**107**	**29.81**
Yes	**144**	**40.11**
N=359		

Table 4.13: Policy_awareness_responses

Question "Does your organization have policies to address insider threats?" answers are displayed in a bar chart. With almost 40% of respondents selecting "Yes," the largest group said that their organizations have such rules in place. Nonetheless, about 30% of respondents stated "No," and another 30% said "Don't know," indicating that a sizable percentage of businesses either don't have insider threat policies or their staff members aren't aware of them. The aforementioned underscores the necessity of improved policy implementation and communication to guarantee that all employees are aware of insider threat management.

4.5.2 Implemented Security Measures for EHR Protection

Source: Developed by author

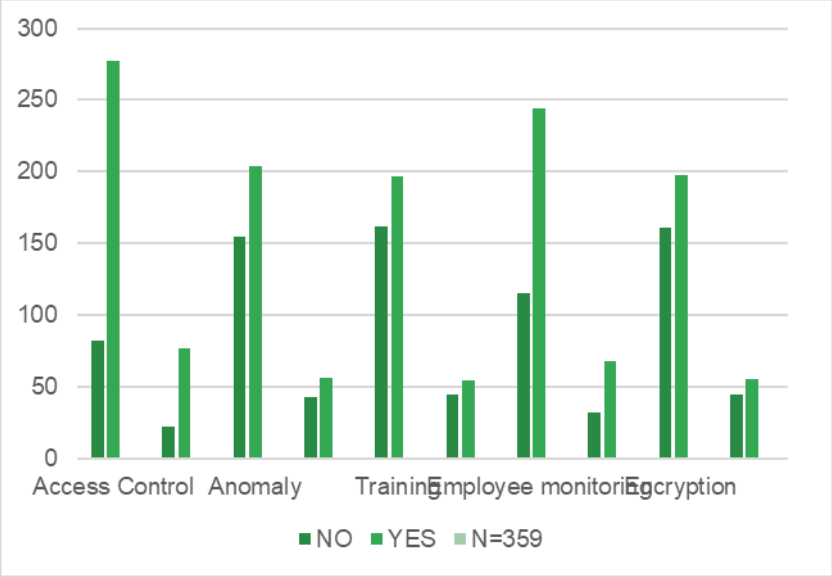


Figure 4.15: Frequency Distribution of Implemented security measures for EHR system

	Access Control		Anomaly		Training		Employee monitoring		Encryption	
	Count	Percent	Count	Percent	Count	Percent	Count	Percent	Count	Percent
NO	82	22.84	155	43.18	162	45.13	115	32.03	161	44.85
YES	277	77.16	204	56.82	197	54.87	244	67.97	198	55.15
N=359										

Table 4.14: Implementation of Security Controls in EHR Systems *Source: Developed by author*

The tally results from Section 5 reveal how frequently different security measures are implemented across healthcare organizations to protect Electronic Health Records (EHRs). Among the 359 respondents, Access Control was the most widely reported measure, with 77.16% confirming its use. This was followed by Employee Monitoring (67.97%) and Anomaly Detection (56.82%), indicating that technical controls for monitoring and detecting abnormal behavior are moderately adopted. Meanwhile, Encryption was used by 55.15% of respondents, and Training—a crucial component for human factor security—was reported by only 54.87%, suggesting that nearly half of the organizations may not provide formal security training to their staff. The table is visualised in a clustered bar chart as shown above.

4.5.3 Perceived Effectiveness of Security Policies

Source: Developed by author

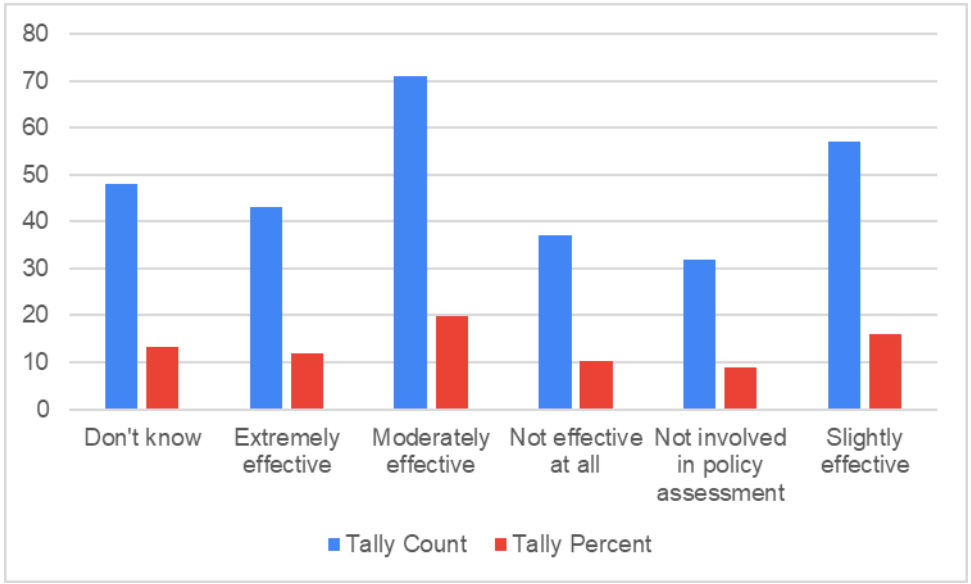


Figure 4.16: **Perceived Effectiveness of Policy Assessment Measures**

Source: Developed by author

Effectiveness of policies	Count	Percent
Don't know	48	13.37
Extremely effective	43	11.98
Moderately effective	71	19.78
Not effective at all	37	10.31
Not involved in policy assessment	32	8.91
Slightly effective	57	15.88

Table 4.15: Statistics of Effectiveness of Policies

The results of the survey on Q3: "How effective are these policies?" show a range of opinions about the efficacy of insider threat policies among medical professionals as summarised in the table. "Moderately effective" and "Very effective," which were selected by 19.78% of participants, were the most commonly selected categories out of 359 responses. According to this, about 40% of respondents think that the policies of their company are either fairly or somewhat effective.

However, significant numbers of respondents indicated hesitancy or lack of confidence: 10.31% said the measures were "not effective at all," and 13.37% said they "don't know." 15.88% also said they were only "slightly effective," and 8.91% said they were "not involved in policy assessment." Collectively, these answers show that although a core group believes that current policies are beneficial, a sizable portion either doubt their efficacy or are unaware of and uninvolved in them—potential gaps that could impair organizational security performance. The bar chart fives the visual illustration of the frequency didtribution.

4.5.4 Frequency of Security Training

Source: Developed by author

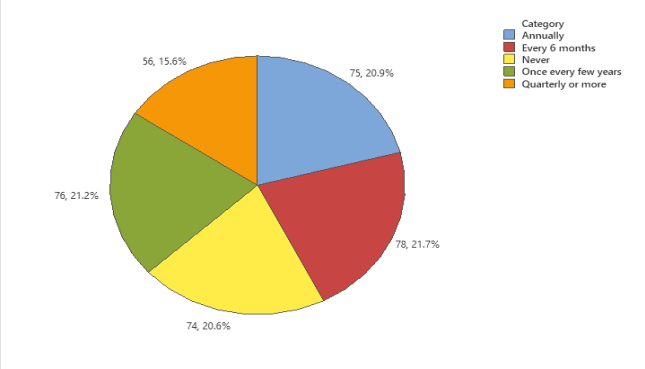


Figure 4.17: Frequency Distribution of security training precevied

The pie chart illustrates how frequently organizations conduct a specific activity related to insider threats, such as training or policy reviews. The responses are distributed quite evenly across the different categories: 21.7% of organizations conduct this activity every 6 months, 21.2% do so once every few years, 20.9% conduct it annually, and 20.6% do it quarterly or more often. Notably, 15.6% of organizations never conduct this activity. This even distribution suggests that there is no standard frequency across organizations, with practices varying widely. However, it is encouraging that the majority engage in this activity at least once a year, although the 15.6% who never do so highlights a gap that could be addressed to improve insider threat management.

4.5.5 Access Control Mechanisms in Use

This table below displays the degree of adoption of different security measures, with 1 being "implemented" and 0 denoting "not implemented." With high mean values (between 0.94 and 0.95), and medians of 1, biometric authentication, automated logouts, and restricted access to sensitive data are commonly utilized in many enterprises. On the other hand, time/location-based limits, role-based access, and multifactor authentication have low medians of 0 and mean values (0.09–0.15), indicating that these controls are rarely used. The widely used measures' low standard deviations show regular use, whereas the less popular controls' somewhat greater variability suggests patchy or irregular application. While more sophisticated access controls are less prevalent, biometric authentication, automated logouts, and limiting access to sensitive data seem to be priorities for most firms.

Source: Developed by author

Variable	Mean	StDev	Median
Biometric authentication	0.94429	0.229682	1
Role based access	0.091922	0.289319	0
multifactor authentication	0.128134	0.334705	0
Time/Location based restriction	0.247632	0.35523	0
Automatic logouts	0.941504	0.235006	1
limited access to sensitive data	0.95429	0.219682	1

Table 4.16: Summary Statistics of Security Control Implementation

The chart compares the average implementation (mean) and variability (standard deviation) of different security controls in organizations. The bars represent the mean values, showing how

commonly each control is used, while the line represents the standard deviation, indicating the consistency of their implementation.

Source: Developed by author

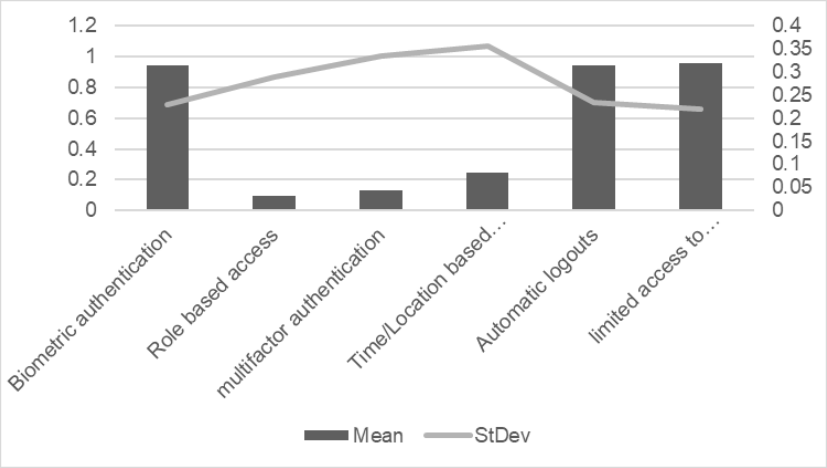


Figure 4.18: Mean and Standard Deviation of Security Techniques for EHR Protection

4.5.6 Monitoring Tools for Suspicious Activity

Source: Developed by author

Are monitoring tools used to detect suspicious activity	Count	Percent
No	**96**	**26.74**
Not sure	**98**	**27.30**
Yes (e.g., user activity logs, anomaly detection)	**165**	**45.96**
N=359		

Table 4.17: Monitoring Tools Usage Frequency for Suspicious Activity

The majority of respondents (45.96%) said that in order to identify suspicious activities, their firms do utilize monitoring technologies such anomaly detection systems or user activity logs.

In order to detect possible insider threats, this indicates that almost half of the firms are actively putting technical safeguards into place. The fact that roughly 27.3% of respondents were unsure if such tools were available suggests that there may be a communication or awareness gap concerning cybersecurity procedures in their organizations.

The fact that 26.74% of respondents said they did not employ monitoring technologies is noteworthy since it could put these firms at higher risk of insider activities going unnoticed. Even when security technologies are available, employees might not be sufficiently taught or informed about them, as seen by the significant percentage of "Not sure" answers. In order to guarantee that monitoring systems are applied and comprehended at all levels of healthcare organizations, this emphasizes the significance of openness, education, and security culture.

4.6 Mitigation Strategies

Finding the best and most advised methods to reduce insider risks in healthcare environments is the main goal of Section 6. The first multiple-choice question asks about the respondents' opinions of the best mitigation techniques, which include AI-driven security, employee training, and policies and governance. The most widely supported strategies were identified by analyzing the responses using frequency counts and percentages. Because the second question is open-ended, participants are free to offer more mitigating techniques. A thematic analysis of these qualitative comments can reveal recurrent recommendations or original concepts. When combined, these evaluations offer a thorough understanding of present perspectives on mitigation strategies and potential areas for enterprises to improve their insider threat defenses.

4.6.1 Perceived Effectiveness of Mitigation Strategies Against Insider Threats

Source: Developed by author

	Policies		Employee training		AI driven security	
	Count	Percent	Count	Percent	Count	Percent
NO	94	26.18	65	18.11	197	54.87
YES	265	73.82	294	81.89	162	45.13
N=359						

Table 4.18: Adoption Frequency of Security Policies, Employee Training, and AI-Driven Security Measures

Source: Developed by author

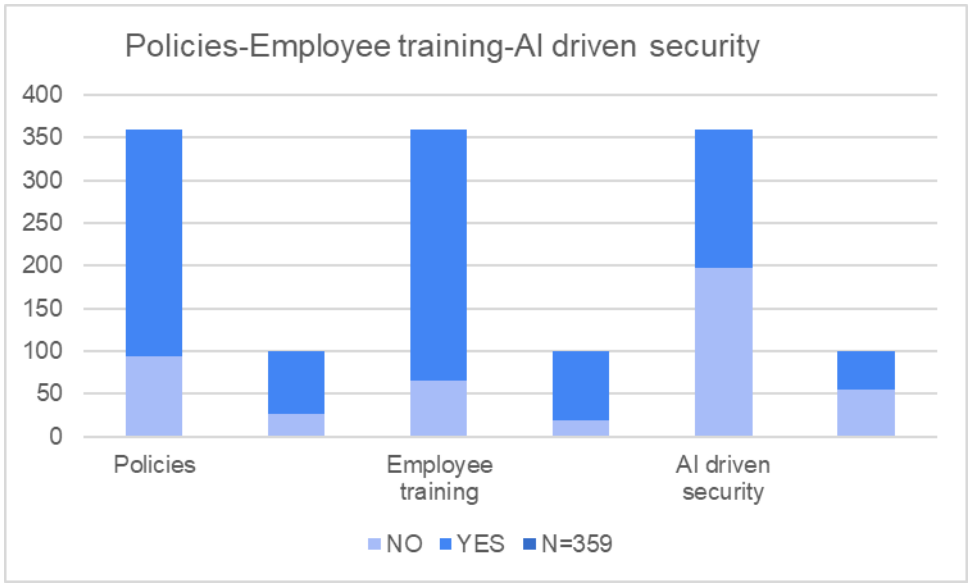


Figure 4.19: Frequency of Implementation: Security Policies, Employee Training, and AI-Driven Security Measures

The stacked bar chart illustrates the frequency distribution of the respondents. Employee training was chosen by 81.89% of respondents as the most preferred solution when asked about effective mitigation techniques against insider threats. As a frontline defense, this shows a high level of trust in educating and alerting personnel. 73.82% of respondents selected policies and governance, indicating the perceived significance of formal regulations and supervision in controlling internal risks. It's interesting to note that the majority of participants (54.87%) did not perceive AI-driven security as a viable technique, with only 45.13% choosing it. Respondents in this study expressed little faith in AI-based anomaly detection systems, despite the literature's emphasis on its significance (Tabassum et al., 2024). This could be a sign of a lack of technical expertise, confidence, or knowledge in medical facilities. Similarly, training is still uncommon in many businesses, despite suggestions for frequent and scenario-based SETA programs (Hu et al., 2022), suggesting a mismatch between best practices and actual implementation.

This implies that many healthcare professionals may still have more faith in human-driven methods like policy enforcement and training, even though AI is a developing subject in cybersecurity.

4.6.2 Additional Strategies

Several important topics that are essential to controlling and reducing insider risks in businesses are shown by the thematic analysis of open ended question. Training & Awareness is the most often highlighted theme, emphasizing the value of continuous staff training, scenario-based learning, phishing simulations, and rigorous onboarding procedures to minimize human mistake. Role-based permissions and access controls are also heavily featured, with an emphasis on putting Role-Based Access Control (RBAC) into practice, upholding the least privilege principle, and limiting data access based on work duties. In order to improve access security, authentication and authorization security emphasizes the use of biometric login systems, two-step verification, and multi-factor authentication (MFA). Monitoring and Behavior Analytics are closely related and include real-time tracking, user behavior analysis, artificial intelligence (AI) anomaly detection, and keeping thorough audit trails to spot questionable activities.

Implementing rapid response plans, creating safe routes for reporting insider threats, and providing incentives to promote proactive reporting are all examples of incident response and reporting protocols, which is another crucial topic. Encrypting sensitive data while it's in transit and at rest, using data loss prevention (DLP) techniques, and protecting private or health records are all part of data protection and encryption. Organizations also place a high priority on regular audits and system maintenance, which includes patching infrastructure to close security gaps, regular software updates, and methodical evaluations of system vulnerabilities.

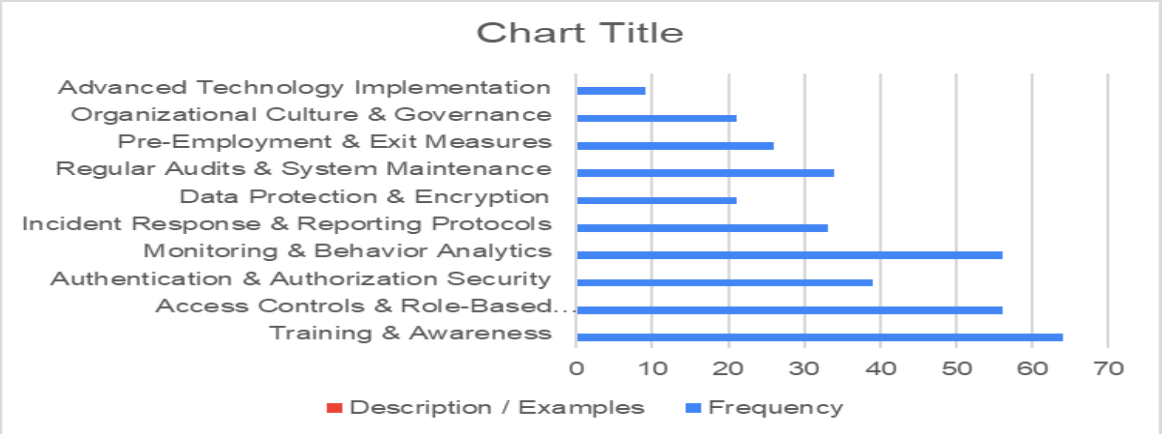
Comprehensive background checks, exit interviews, pre-exit monitoring, and offboarding audits are examples of pre-employment and exit measures that guarantee safe employee transfers and reduce post-exit hazards. Enforcing policies, encouraging leadership responsibility, and instilling a privacy-first mentality across the whole organization are all made possible by a robust organizational culture and governance. In order to improve the overall security architecture, Advanced Technology Implementation—which is less commonly discussed—involves utilizing state-of-the-art tools like blockchain for immutable logs, AI/ML algorithms for threat detection, and just-in-time access controls.

Key Theme	Frequency	Description / Examples
Training & Awareness	64	Emphasis on ongoing staff training, phishing simulations, scenario-based sessions, onboarding awareness.
Access Controls & Role-Based Permissions	56	Implementing RBAC, least privilege access, data visibility restrictions by job role or department.
Authentication & Authorization Security	39	Use of MFA, two-step verification, biometric authentication for secure login.
Monitoring & Behavior Analytics	56	Real-time tracking, AI-driven anomaly detection, User Behavior Analytics, audit trails.
Incident Response & Reporting Protocols	33	Rapid response plans, insider threat reporting channels, incentives for reporting threats.
Data Protection & Encryption	21	Encrypting data at rest/in transit, using DLP tools, securing sensitive health records.
Regular Audits & System Maintenance	34	Security audits, server maintenance, software patching, and system updates.
Pre-Employment & Exit Measures	26	Background checks, pre-exit monitoring, exit interviews, offboarding audits.
Organizational Culture & Governance	21	Promoting accountability, leadership enforcement of policies, privacy-first mindset.
Advanced Technology Implementation	9	Blockchain-based audit logs, just-in-time access, AI/ML threat detection, immutable logs.

The data of the thematic analysis is summariesed in the table below.

Table 4.19: Frequency Distribution of Key Security Themes and Their Descriptions

Figure 4.20: Frequency of Key Security Themes in EHR Protection Strategies



This horizontal bar chart shows how frequently different security issues are highlighted in methods for protecting Electronic Health Records (EHRs). The most often mentioned themes in the chart are "Training & Awareness," "Access Controls & Role-Based Permissions," and "Monitoring & Behavior Analytics," highlighting the significance of continuous staff training, stringent access control, and real-time monitoring in protecting sensitive health data. A thorough, multi-layered approach to EHR security is demonstrated by advanced technologies, corporate culture, and incident response procedures, all of which are less commonly discussed but are nonetheless important.

4.7 Discussions

The findings of this study align closely with existing literature on insider threats in EHR systems. For example, consistent with Liu Hua Yeo (2022) and Al-Mhiqani et al. (2020), our data indicate that negligent and unintentional insider threats are perceived as more frequent than malicious ones, reinforcing the notion that human error remains the dominant risk in healthcare data security. The results of this study, which were supported by a varied and knowledgeable sample of respondents, provide a convincing picture of insider threats in the context of electronic health records (EHRs). With a cross-sectional grasp of healthcare workflows, system usage, and vulnerabilities, the representation of clinical (39.3%), technical (30.9%), and administrative (27%) staff highlights a thorough understanding of the complex nature of insider threats. The inclusion of people from hospitals and private clinics, most of whom have more than ten years of experience, lends credibility to these findings by providing viewpoints from seasoned experts who have probably seen how EHR systems have changed and how security concerns have increased in tandem.

According to the data, experience and EHR usage are directly correlated, with more seasoned respondents using EHR systems more frequently. This bolsters previous research that highlights how exposure to digital systems frequently improves familiarity and, ironically, increases the likelihood of both error and exploitation (van der Horst *et al.*, 2022). Crucially, since 90.5% of respondents said they were familiar with insider threats and 84.7% had experienced them, this familiarity has not resulted in complacency but rather in a greater awareness of them. According to earlier research, human-centric hazards are more common than simply technological weaknesses, and these numbers demonstrate a sophisticated awareness of cybersecurity concerns in the healthcare industry (Jalali and Kaiser, 2018).

It is significant that careless and unintentional actions are thought to be more common sources of insider threats than malevolent intent. It implies that the majority of incidents result from poor decision-making, inadequate training, or system abuse rather than malice. This is consistent with research by (R *et al.*, 2025), who pointed out that justified noncompliance, rather than malicious intent, is frequently the cause of information system policy infractions. Such knowledge is essential for directing prevention tactics, which must place a high priority on accountability, education, and system design that minimizes the effects of human error.

The interaction of human mistake and technology flaws was a common element in stories about data breaches. Lack of an audit trail, for example, makes businesses ignorant to access trends, and inadequate access restrictions make it easier for unauthorized data to be exposed. The systemic flaws that exacerbate human error and enable careless or inadvertent behaviour to grow into serious breaches are highlighted by these studies. Furthermore, as healthcare ecosystems become more interconnected, third-party risks like vendor misuse are becoming more prevalent, necessitating stricter vendor control and contractual security duties.

Insider threats were viewed as having a considerable influence, especially in terms of financial loss (83%) and legal ramifications (75%). According to the Ponemon Institute (2021), these worries are consistent with the larger industry experience, which has seen data breaches lead to significant recovery costs, legal action, and regulatory damages. Even though operational disruption and reputational harm were less of a worry (69% and 63%, respectively), they are nonetheless crucial to the overall risk profile. 57.1% of respondents agreed that insider threats have a negative impact on patient confidence, which is a crucial issue in the healthcare industry where secrecy is fundamental. This suggests that a tarnished reputation can erode patient trust.

Interestingly, perceptions of impact on clinical quality were more divided. The lack of a statistically significant difference across groups ($p = 0.073$) may suggest either a variance in actual experiences or a disconnect between data security incidents and their immediate clinical outcomes. This divergence underscores the need for more granular research to understand how insider threats translate into compromised care delivery. In contrast, the stronger consensus around the impact on operational efficiency (72%) demonstrates that, even if patient outcomes remain unaffected, insider threats can severely disrupt workflows, delay processes, and reduce productivity.

The absence of broad policy implementation and understanding was one of the most alarming findings. Most respondents were either ignorant of or denied the existence of insider threat

policies in their firms, while 40% of them acknowledged that they did. This disparity indicates either a genuine lack of institutional governance or inadequate communication. Only forty percent of those with policies thought they were moderately or extremely effective. The way policies are created, disseminated, and implemented needs to be critically reevaluated.

Although security procedures are widely used in some areas, such as staff monitoring (67.97%) and access control (77.16%), there were alarming gaps in encryption (55.15%) and training (54.87%). These numbers show where technical protections can be strengthened. Specifically, the underutilization of training is concerning, especially in light of the fact that 15.6% of firms do not provide any security training at all. The most common source of insider threats was found to be human error, therefore inconsistent training is a basic overlook. Given the ever-changing threat landscape, regular, scenario-based, and adaptive training need to be required.

The restricted use of sophisticated access control methods, such as location-aware systems and Role-Based Access Control (RBAC), is indicative of yet another significant weakness. In order to ensure that users only access the data required for their tasks and to enforce the concept of least privilege, such technologies are crucial. Similar to this, 46% of people utilize monitoring tools, but over half either don't or aren't sure, which may indicate that user activity is not fully visible. Proactive security is based on visibility. In the absence of efficient monitoring, insider threats might go unnoticed until serious harm has been done.

The respondents' suggested mitigation techniques clearly favor human-centric methods. Of those surveyed, the majority preferred governance regulations (73.82%) and employee training (81.89%), but only 45.13% trusted AI-powered technologies. Fear of false positives, algorithmic transparency, or unfamiliarity may be the causes of this cautious approach to AI. It does, however, also present an opportunity. Machine learning and artificial intelligence (AI) have a great deal of promise for spotting unusual user behaviour that could point to careless or malevolent insider activity. Companies ought to think about hybrid models in which automated detection technologies are supplemented by human monitoring.

The quantitative data was enhanced by qualitative responses, which provided useful information. Proposals for enhanced encryption, multifactor authentication (MFA), audit trail integrity, and robust incident response procedures are in line with industry best practices. It's very crucial to prioritize company culture, especially with regard to leadership responsibility and a privacy-first mentality. Effective policy adherence and vigilance require a security-aware culture that is nurtured by top-down commitment.

Furthermore, a small number of respondents recommended cutting-edge mitigating solutions like blockchain and AI/ML. Blockchain's transparency and immutability can improve auditability, while artificial intelligence can spot minute behavioral anomalies. Although careful integration and stakeholder education are necessary for these technologies, their inclusion in the conversation shows a growing understanding of the changing threat picture and the demand for creative solutions.

In conclusion, the information presents a thorough picture of EHR insider threats as a complex problem that is primarily caused by human behavior and made worse by organizational flaws and technical vulnerabilities. There is still a gap between knowledge and application, despite the high level of awareness. Healthcare companies must place a high priority on strong governance, frequent training, and efficient application of both technology-driven and human-centric solutions in order to close this gap. The effects on clinical outcomes and the efficiency of new technology in reducing insider threats should be further investigated in future studies. In contemporary healthcare, protecting patient data's availability, confidentiality, and integrity is not only technically required, but also morally and legally required.

5.Conclusion and Recommendations

This study aimed to investigate insider threats in Electronic Health Records (EHR) within the context of Kerala's healthcare sector through a structured questionnaire survey.

A total of 397 replies were gathered, and 359 legitimate responses remained in the final dataset following the data cleaning procedure, which involved eliminating entries that were either incomplete or invalid. Although this represents a slight decrease of about 3% from the initial sample, the validity and reliability of the results were unaffected.

5.1 Summary of Main Findings and Their Implications

- All healthcare roles agree that insider risks to EHR security are common, with careless and inadvertent activities being seen as more common than malevolent ones.

- The majority of respondents showed strong awareness of insider dangers, having either heard about or experienced similar situations.

- The necessity for role-specific mitigation techniques is underscored by the high level of concern around insider threats, particularly among clinical and IT personnel.

- The worst effects are thought to be financial and legal, then operational disruptions and reputational harm.

- Despite their increasing importance, AI technologies are regarded with some suspicion, while training and governance policies are the most popular mitigation solutions.

- According to the survey, there are gaps in implementation as many healthcare organizations either offer training infrequently or lack explicit insider threat policies.

- Advanced role-based and location-based systems are not fully employed, despite the prevalence of access controls like biometrics and automated logout.

5.2 Summary of Key Differences from Literature

- While literature stresses increasing reliance on AI-based monitoring and anomaly detection, survey responses indicate greater trust in human-centric methods such as training and policy.
- Healthcare-specific taxonomies and frameworks remain underdeveloped in practice, aligning with Jaikanth & Madisetti's (2024) critique of general models.
- Despite evidence from the literature about high operational and reputational damage, a significant portion of respondents underappreciated these aspects, indicating a possible disconnect between perceived and actual consequences.
- Literature identifies third-party vendors as significant risks, yet these were mentioned less frequently in the open-ended responses—suggesting under-recognition in real-world settings.

5.3 Practical Recommendations

Improve training initiatives: All positions should get ongoing, scenario-based, and required security training, with an emphasis on minimizing human error.

Strengthen governance and policy communication: It is important to establish, disseminate, and integrate explicit insider threat policies into routine procedures.

Implement advanced access control measures in place: Location-based access control, RBAC, and the least privilege principle should be given top priority.

Invest in AI-based behavioral analytics to anticipate insider threat activity by combining intelligent monitoring with human oversight.

Regular audits and incident response exercises: To foster a culture of responsibility and preparedness, including audit trail evaluations and anonymous reporting systems.

5.4 Academic Recommendations

- Further creation of insider threat taxonomies that are sector-specific and adapted for use in healthcare settings.
- investigation of hybrid detection systems that integrate sociotechnical knowledge with machine learning.
- Comparative research evaluating the relative merits of technology-led mitigation measures and policy in various healthcare settings.

5.5 Limitations of the Research

- The study involves extensive use of self-reported data, which could be impacted by recall mistake or bias.
- The sample size is varied, but it does not accurately reflect all institutional or geographic forms of healthcare.
- The cross-sectional design restricts causal inference because it records perception at a single moment in time.
- Though not all-inclusive, open-ended replies were rich, and further qualitative research could delve deeper into insider incident narratives.

5.6 Contributions of the Research

- Gives a comprehensive overview of insider threats from the viewpoints of technology, medicine, and administration.
- Combines the results of thematic literature with survey data based on perception, advancing our practical knowledge of EHR security.
- Provides practical information on the degree of acceptance and deployment of insider threat prevention techniques in the healthcare industry today.

5.7 Suggestions for Further Research

- Perform long-term research to evaluate how new technologies affect insider threat perceptions and reactions.
- Examine regional or cross-cultural differences in danger profiles, awareness, and policy implementation.
- Examine how patients feel about insider incident disclosure and data trust.
- Create and evaluate unique behavioral models and taxonomies for use in small and medium-sized healthcare facilities.

5.8 Final Reflections

After finishing this dissertation, I now have a better knowledge of how technology, legislation, and human behavior interact to protect patient data. It emphasized not just the advanced nature of technology instruments but also the vital function of awareness, administration, and training. This study is a timely reminder that, despite the ongoing digitization of healthcare, human interaction is still the weakest link and the best safeguard against EHR security threats.

REFERENCES

admin, craxis. (2024) *The Hidden Dangers of Insider Threats in Healthcare Data Security*. *DataPatrol*. Available at: https://datapatrol.com/the-hidden-dangers-of-insider-threats-in-healthcare-data-security/ (Accessed: 9 February 2025).

Alarfaj, K.A. and Rahman, M.M.H. (2024) (13) 'The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix'. *Applied Sciences*, 14(13), p. 5785. DOI: 10.3390/app14135785.

Alder, S. (2023a) *Editorial: Insider Threats to Healthcare Records*. *The HIPAA Journal*. Available at: https://www.hipaajournal.com/insider-threats-to-healthcare-records/ (Accessed: 17 March 2025).

Alder, S. (2023b) *Editorial: Insider Threats to Healthcare Records*. *The HIPAA Journal*. Available at: https://www.hipaajournal.com/insider-threats-to-healthcare-records/ (Accessed: 17 March 2025).

Alder, S. (2023c) *Editorial: Insider Threats to Healthcare Records*. *The HIPAA Journal*. Available at: https://www.hipaajournal.com/insider-threats-to-healthcare-records/ (Accessed: 23 April 2025).

Allemang, B., Sitter, K. and Dimitropoulos, G. (2022) 'Pragmatism as a Paradigm for Patient-oriented Research'. *Health Expectations : An International Journal of Public Participation in Health Care and Health Policy*, 25(1), pp. 38–47. DOI: 10.1111/hex.13384.

Al-Mhiqani, M.N. *et al.* (2020a) (15) 'A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations'. *Applied Sciences*, 10(15), p. 5208. DOI: 10.3390/app10155208.

Al-Mhiqani, M.N. *et al.* (2020b) (15) 'A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations'. *Applied Sciences*, 10(15), p. 5208. DOI: 10.3390/app10155208.

Anubhuti Sood. (2025a) *Impact and Challenges of the DPDP Act on Healthcare Organizations*. *SRL*. Available at: https://spiceroutelegal.com/data-protection/the-digital-personal-data-protection-act-impact-on-and-challenges-to-healthcare-organisations/ (Accessed: 27 May 2025).

Anwita. (2024) *Understanding Insider Threats: Types, Indicators, and Mitigation*. Available at: https://sprinto.com/blog/insider-threats/ (Accessed: 9 February 2025).

Banerjee, S. *et al.* (2024) 'EHR Security and Privacy Aspects: A Systematic Review'. In Puthal, D.Mohanty, S.and Choi, B.-Y. (eds.) *Internet of Things. Advances in Information and Communication Technology*. Cham: Springer Nature Switzerland, pp. 243–260. DOI: 10.1007/978-3-031-45878-1_17.

Baugher, J. and Qu, Y. (2024) (2) 'Create the Taxonomy for Unintentional Insider Threat via Text Mining and Hierarchical Clustering Analysis'. *European Journal of Electrical Engineering and Computer Science*, 8(2), pp. 36–49. DOI: 10.24018/ejece.2024.8.2.608.

Berezin, J. (2025) *Security Awareness Training for Healthcare Staff: 2025 Edition*. *CYOP*. Available at: https://cyopsecurity.com/insights/cybersecurity-awareness-training-for-healthcare-staff-2025-edition/ (Accessed: 21 March 2025).

Bhartiya, S. and Mehrotra, D. (2013) 'Threats and Challenges to Security of Electronic Health Records'. In Singh, K. and Awasthi, A.K. (eds.) *Quality, Reliability, Security and Robustness in Heterogeneous Networks*. Berlin, Heidelberg: Springer, pp. 543–559. DOI: 10.1007/978-3-642-37949-9_48.

Bin Sarhan, B. and Altwaijry, N. (2023) (1) 'Insider Threat Detection Using Machine Learning Approach'. *Applied Sciences*, 13(1), p. 259. DOI: 10.3390/app13010259.

Clifton, A. (2024) ‘Strategies for Insider Threat Mitigation and Detection’.

Cremer, F. *et al.* (2022) ‘Cyber Risk and Cybersecurity: A Systematic Review of Data Availability’. *The Geneva Papers on Risk and Insurance. Issues and Practice*, 47(3), pp. 698–736. DOI: 10.1057/s41288-022-00266-6.

Diaz, N. (2022) *HHS Warns of Insider Threats to Healthcare Organizations*. Available at: https://www.beckershospitalreview.com/cybersecurity/hhs-warns-of-insider-threats-to-healthcare-organizations.html (Accessed: 18 March 2025).

DPDPA. (2023) *Impact and Challenges of the DPDP Act on Healthcare Organizations*. *SRL*. Available at: https://spiceroutelegal.com/data-protection/the-digital-personal-data-protection-act-impact-on-and-challenges-to-healthcare-organisations/ (Accessed: 27 May 2025).

EHD. (2025) *European Health Data Space Regulation (EHDS) - European Commission*. Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en (Accessed: 17 March 2025).

Ellen Kim MD, MPH. (2019) *The Evolving Use of Electronic Health Records (EHR) for Research - ScienceDirect*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1053429619300426 (Accessed: 17 February 2025).

Findlay Whitelaw; Jackie Riley; Nebrase Elmrabit. (2024) *A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services | IEEE Journals & Magazine | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/10458945 (Accessed: 15 March 2025).

Goel, P.M. (2019) ‘A Literature Review of Cyber Security’. 6(2).

Hales, M. (2023) *EHR Cybersecurity Risks*. *The HIPAA E-Tool*. Available at: https://thehipaaetool.com/ehr-cybersecurity-risks/ (Accessed: 17 March 2025).

van der Horst, D.E.M. *et al.* (2022) ‘Optimizing the Use of Patients’ Individual Outcome Information – Development and Usability Tests of a Chronic Kidney Disease Dashboard’. *International Journal of Medical Informatics*, 166, p. 104838. DOI: 10.1016/j.ijmedinf.2022.104838.

HSS. (2022) ‘202204211300_Insider Threats in Healthcare_TLPWHITE’.

Hu, S., Hsu ,Carol. and and Zhou, Z. (2022) ‘Security Education, Training, and Awareness Programs: Literature Review’. *Journal of Computer Information Systems*, 62(4), pp. 752–764. DOI: 10.1080/08874417.2021.1913671.

Hurst, W. *et al.* (2022) ‘Securing Electronic Health Records against Insider-Threats: A Supervised Machine Learning Approach’. *Smart Health*, 26, pp. 100354–100354. DOI: 10.1016/j.smhl.2022.100354.

Imprivata. (2020) *The Cost of Insider Threats in the Healthcare Industry and How to Reduce Them | Imprivata UK*. Available at: https://www.imprivata.com/blog/the-cost-of-insider-threats-in-healthcare-and-how-to-reduce-them (Accessed: 17 March 2025).

India-Cyber-Threat-Report-2025.Pdf. Available at: https://www.quickheal.co.in/documents/threat-report/india-cyber-threat-report-2025.pdf (Accessed: 27 May 2025b).

Ismail Keshta. (2021) *Security and Privacy of Electronic Health Records: Concerns and Challenges - ScienceDirect*. Available at: https://www.sciencedirect.com/science/article/pii/S1110866520301365 (Accessed: 17 March 2025).

Jaikanth, M. and Madisetti, V.K. (2024) (5) 'A Comparative Analysis of Cybersecurity Threat Taxonomies for Healthcare Organizations'. *Journal of Software Engineering and Applications*, 17(5), pp. 359–377. DOI: 10.4236/jsea.2024.175020.

Jalali, M.S. and Kaiser, J.P. (2018) 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective'. *Journal of Medical Internet Research*, 20(5), p. e10059. DOI: 10.2196/10059.

Janarthanan, V. *et al.* (2024) 'Legal and Ethical Issues Associated With Challenges in the Implementation of the Electronic Medical Record System and Its Current Laws in India'. *Cureus*. DOI: 10.7759/cureus.56518.

Kannelønning, K. and Katsikas, S.K. (2023) 'A Systematic Literature Review of How Cybersecurity-Related Behavior Has Been Assessed'. *Information & Computer Security*, 31(4), pp. 463–477. DOI: 10.1108/ICS-08-2022-0139.

Kaushik, V. and Walsh, C.A. (2019) (9) 'Pragmatism as a Research Paradigm and Its Implications for Social Work Research'. *Social Sciences*, 8(9), p. 255. DOI: 10.3390/socsci8090255.

Khando, K. *et al.* (2021) 'Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review'. *Computers & Security*, 106, p. 102267. DOI: 10.1016/j.cose.2021.102267.

King, R. (2022) (10) 'The Utility of Pragmatism in Educational Research'. *Creative Education*, 13(10), pp. 3153–3161. DOI: 10.4236/ce.2022.1310199.

Kotb, H.M. *et al.* (2025) 'A Novel Deep Synthesis-Based Insider Intrusion Detection (DS-IID) Model for Malicious Insiders and AI-Generated Threats'. *Scientific Reports*, 15(1), p. 207. DOI: 10.1038/s41598-024-84673-w.

Kwon, J. and Johnson, M.E. (2025) 'Unraveling the Impact of Data Breaches: Evidence From the US Healthcare Sector'. *Production and Operations Management*, p. 10591478241305351. DOI: 10.1177/10591478241305351.

Le, D.C. and Zincir-Heywood, A.N. (2019) 'Machine Learning Based Insider Threat Modelling and Detection'.

Liu Hua Yeo. (2022) *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis - PMC*. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/ (Accessed: 17 February 2025).

Macklin, K. (2025) *Insider Threat Indicators: Keeping Your Health Records Safe*. *ChartRequest*. Available at: https://chartrequest.com/insider-threat-indicators/ (Accessed: 17 March 2025).

mimecast. (2025) *11 Real-Life Insider Threat Examples | Cyber Threats*. *Mimecast*. Available at: https://www.mimecast.com/blog/insider-threat-examples/ (Accessed: 9 February 2025).

Mishra, U.S., Yadav ,Suryakant. and and Joe, W. (2024) 'The Ayushman Bharat Digital Mission of India: An Assessment'. *Health Systems & Reform*, 10(2), p. 2392290. DOI: 10.1080/23288604.2024.2392290.

Muiris-Oconnor-Navigating-Heath-Data-Regulation.Pdf. Available at: https://www.ehealthireland.ie/media/tpojivgd/muiris-oconnor-navigating-heath-data-regulation.pdf (Accessed: 17 March 2025c).

Nassir, N.F.M. *et al.* (2024) 'REVEALING THE MULTI-PERSPECTIVE FACTORS BEHIND INSIDER THREATS IN CYBERSECURITY'. 17.

Nduma N. Basil. (2022) *Health Records Database and Inherent Security Concerns: A Review of the Literature | Cureus*. Available at: https://www.cureus.com/articles/117118-health-records-database-and-inherent-security-concerns-a-review-of-the-literature#!/ (Accessed: 18 March 2025).

Neetesh Saxena. (2020) *Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses*. Available at: https://www.mdpi.com/2079-9292/9/9/1460 (Accessed: 16 March 2025).

Nifakos, S. *et al.* (2021) (15) 'Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review'. *Sensors*, 21(15), p. 5119. DOI: 10.3390/s21155119.

Organization, W.H. (2017) *Global Diffusion of EHealth: Making Universal Health Coverage Achievable: Report of the Third Global Survey on EHealth*. World Health Organization.

Park, S.-A. *et al.* (2013) 'Evaluation of Feature Extraction Methods for EEG-Based Brain-Computer Interfaces in Terms of Robustness to Slight Changes in Electrode Locations: Medical & Biological Engineering & Computing'. *Medical & Biological Engineering & Computing*, 51(5), pp. 571–579. DOI: 10.1007/s11517-012-1026-1.

Patel, R. (2022) 'CYBERSECURITY RISKS IN THE HEALTHCARE INDUSTRY'. *Indian Journal of Scientific Research*, 12(2), p. 45. DOI: 10.32606/IJSR.V12.I2.00007.

Prabhu, S. and Thompson, N. (2020) 'A Unified Classification Model of Insider Threats to Information Security'. *ACIS 2020 Proceedings*. Available at: https://aisel.aisnet.org/acis2020/40.

R, M. *et al.* (2025) (5135149) DOI: 10.2139/ssrn.5135149.

Rahman, MD.Z.U. *et al.* (2024) 'Proof of Trust and Expertise (PoTE): A Novel Consensus Mechanism for Enhanced Security and Scalability in Electronic Health Record Management'. *IEEE Access*, 12, pp. 115905–115925. DOI: 10.1109/ACCESS.2024.3424685.

Ramasami, S. and Maheswari, P.U. (2024) 'Securing Electronic Health Records from Insider Threats in Smart City Healthcare Cloud Using Machine Learning Approach'. In *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). pp. 643–648. DOI: 10.1109/ICICV62344.2024.00107.

Rele, M. and Patil, D. (2023) 'Securing Patient Confidentiality in EHR Systems: Exploring Robust Privacy and Security Measures'. In *2023 27th International Computer Science and Engineering Conference (ICSEC)*. 2023 27th International Computer Science and Engineering Conference (ICSEC). pp. 1–6. DOI: 10.1109/ICSEC59635.2023.10329773.

Saeed, S. *et al.* (2023) (16) 'A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience'. *Sensors*, 23(16), p. 7273. DOI: 10.3390/s23167273.

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods for Business Students*. Pearson Education.

Shah, S.M. and Khan, R.A. (2020) 'Secondary Use of Electronic Health Record: Opportunities and Challenges'. *IEEE Access*, 8, pp. 136947–136965. DOI: 10.1109/ACCESS.2020.3011099.

Singh, A.P. and Sharma, A. (2022) (arXiv:2212.05347) DOI: 10.48550/arXiv.2212.05347.

Sreekandan, N.S. (2023) 'Data Breach Analysis in Indian Healthcare Facilities: A Comprehensive Study (1st Edition)'. *International Research Journal of Modernization in Engineering Technology and Science*, 5(1), pp. 1–15.

Subhani, A., Khan, I.A. and Zubair, A. (2021) (4) 'Review of Insider and Insider Threat Detection in the Organizations'. *Journal of Advanced Research in Social Sciences and Humanities*, 6(4), pp. 167–174. DOI: 10.26500/jarssh.v6i4.174.

sujeet katiyar. (2024) *Top 10 Data Breaches in India's Healthcare Sector: A Wake-Up Call for Data Security | LinkedIn*. Available at: https://www.linkedin.com/pulse/top-10-data-breaches-indias-healthcare-sector-wake-up-sujeet-katiyar-t3jpf/ (Accessed: 27 May 2025).

Tabassum, M. *et al.* (2024) 'Anomaly-Based Threat Detection in Smart Health Using Machine Learning'. *BMC Medical Informatics and Decision Making*, 24, p. 347. DOI: 10.1186/s12911-024-02760-4.

Tampa Bay. (2025) *HIPAA – HITECH Non-Compliance*. *Tampa Bay Compliance*. Available at: https://tampabaycompliance.com/resources/hipaa-hitech-non-compliance/ (Accessed: 17 March 2025).

Thomas. (2006) *A General Inductive Approach for Analyzing Qualitative Evaluation Data - David R. Thomas, 2006*. Available at: https://journals.sagepub.com/doi/abs/10.1177/1098214005283748 (Accessed: 19 April 2025).

Triplett, W.J. (2024) 'Exploring and Mitigating Cybersecurity Challenges in Electronic Health Records'. *Cybersecurity and Innovative Technology Journal*, 2(1), pp. 41–52. DOI: 10.53889/citj.v2i1.344.

Whitelaw, F., Riley, J. and Elmrabit, N. (2024) 'A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services'. *IEEE Access*, 12, pp. 34752–34768. DOI: 10.1109/ACCESS.2024.3373265.

Yeo, L.H. and Banfield, J. (2022) 'Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis'. *Perspectives in Health Information Management*, 19(Spring), p. 1i.

APPENDIX A: SURVEY QUESTIONS IN GOOGLE FORM

Questions Responses 397 Settings

Unmasking Insider Threats in Electronic Health Records (EHR): A Comprehensive Analysis of Risks, Impacts, and Strategic Mitigation Measures for Enhanced Healthcare Data Security

My name is **Salini Chemmengattuvalappil Mohandas**, and I am currently pursuing an **MSc in Medical Device Technology and Business at Griffith College, Dublin, Ireland.**

As part of my dissertation, I am conducting a study titled:
"Unmasking Insider Threats in Electronic Health Records (EHR): A Comprehensive Analysis of Risks, Impacts, and Strategic Mitigation Measures for Enhanced Healthcare Data Security."

This research aims to examine the **challenges posed by insider threats** to EHR systems, assess their **impact on healthcare data security**, and identify **effective strategies** to mitigate these risks.

Your input is incredibly valuable and will provide critical insights into how organizations are addressing these threats. Participation is **voluntary**, and the survey is designed to take no more than **10 to 15 minutes**.

Thank you for your **time, support, and contribution** to this important area of research.

For more information, please contact : salini.chemmengattuvalappilmohandas@student.griffith.ie

Email Address

Short answer text

Before you begin, please read the following and indicate your cosent.* *

- [ ] I have read and understood the purpose, procedures, and potential risks associated with this research st...
- [ ] I consent to participate in this study voluntarily and understand that my responses will be kept confidenti...

Section 2 of 6

Section2: Background

Description (optional)

1. What is your current job role? *

- ○ Physician
- ○ Nurse
- ○ Administrative Staff
- ○ IT Staff
- ○ Clinical Support Staff
- ○ Contractor/External Vendor
- ○ Other Healthcare Support
- ○ Other...

2. How many years of experience do you have in your current field? *

If you would like to provide more detailed information, please specify your exact years of experience in the option other

- ○ Less than 1 year
- ○ 1–3 years
- ○ 4–7 years
- ○ 8–10 years
- ○ More than 10 years
- ○ Other...

3. What type of healthcare institution do you work in? *

- ○ Public Hospital
- ○ Private Hospital/Clinic
- ○ Research Facility
- ○ Government Healthcare Agency

4. How familiar are you with Electronic Health Record (EHR) systems? *

- ○ Not familiar at all
- ○ Somewhat familiar
- ○ Moderately familiar
- ○ Very familiar
- ○ Expert level (designs, administers, or secures EHR systems)

5. How frequently do you access Electronic Health Records (EHRs) in your role? *

- ○ More than 5 times/day
- ○ 1–5 times/day
- ○ 1–5 times/week
- ○ Rarely (less than once/week)
- ○ Never

Section 3 of 6

Section3: Awareness of Insider Threat

Description (optional)

1. Are you aware of the risks associated with insider threats to EHR security? *

- ○ Yes
- ○ No

2. Have you ever encountered or heard of an insider threat incident in your organization? *

- ○ Yes
- ○ No

3. Which type of insider threat do you believe is most common in your organization? *

	Often	Sometimes	Rarely	Never
Malicious threat (e...	○	○	○	○
Negligent threat (e...	○	○	○	○
Accidental threat (...	○	○	○	○

3a. If you selected "Often" or "Sometimes" for any of the above, please describe the incidents and any actions taken; ----------

Short answer text

4. How often do you think insider threats pose a risk to EHR security? *

- ○ Rarely
- ○ Occasionally
- ○ Frequently
- ○ Always

After section 3 Continue to next section

Section 4 of 6

Section 4: Impact of Insider Threat

Description (optional)

1. What do you think is the most significant impact of insider threats on healthcare organizations? (Select all that apply) *

- [ ] Financial loss
- [ ] Legal consequences
- [ ] Operational disruptions
- [ ] Reputational damage
- [ ] Other...

1a. Rank your selected impacts in order of significance *

(1 = most significant; only rank the ones you selected above)

	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
financial loss	○	○	○	○	○
Legal consequ...	○	○	○	○	○
Operational dis...	○	○	○	○	○
Reputational d...	○	○	○	○	○

2. How concerned are you about insider threats affecting patient data security? *

- ○ Not concerned
- ○ Somewhat concerned
- ○ Very concerned
- ○ Not applicable

3. Do you believe that insider threats can cause major financial losses for healthcare organizations? *

- ○ Yes
- ○ No

4. In your opinion, how do insider threats affect patient trust in healthcare institutions?

- ○ No impact
- ○ Minor impact

4. In your opinion, how do insider threats affect patient trust in healthcare institutions?

- ○ No impact
- ○ Minor impact
- ○ Moderate impact
- ○ Significant impact

5. How do insider threats impact patient care in terms of clinical quality? *

- ○ No impact
- ○ Minor impact
- ○ Moderate impact
- ○ Significant impact
- ○ Severe impact

6. How do insider threats impact operational efficiency in healthcare organizations?

- ○ No impact
- ○ Minor impact
- ○ Moderate impact
- ○ Significant impact
- ○ Severe impact

After section 4 Continue to next section

Section 5 of 6

Section5: Security Measures

Description (optional)

1. **Does your organization have policies to address insider threats?** *

- ○ Yes
- ○ No
- ○ Don't know
- ○ Other...

2. What security measures does your organization currently use to protect EHRs? (Select all that apply) *

- ☐ Access control
- ☐ Anomaly detection
- ☐ Employee monitoring
- ☐ Encryption
- ☐ Training

3. **How effective are these policies?** *

- ○ Not effective at all
- ○ Slightly effective
- ○ Moderately effective
- ○ Very effective
- ○ Extremely effective
- ○ Don't know
- ○ Not involved in policy assessment

4. How often do you receive security training?

- ○ Never
- ○ Once every few years
- ○ Annually
- ○ Every 6 months
- ○ Quarterly or more

5. Which access controls are in place? (Select all that apply) *

- ☐ Role-based access
- ☐ Multi-factor authentication (MFA)
- ☐ Time/location-based restrictions
- ☐ Automatic logouts
- ☐ Limited access to sensitive data
- ☐ Biometric authentication

6. **Are monitoring tools used to detect suspicious activity?**

- Yes (e.g., user activity logs, anomaly detection)
- No
- Not sure
- Add option or add "Other"

Required

ter section 5 Continue to next section

Section 6 of 6

Section 6: Mitigation Strategies

Description (optional)

1. What mitigation strategies do you think would be most effective against insider threats? Select all if apply *

- [ ] Policies & governance
- [ ] Employee training
- [ ] AI-driven security

2. What additional strategies should your organization implement?(Open-ended) *

Short answer text

APPENDIX B: ETHICS FORM

Innopharma education

GRIFFITH COLLEGE

Ethics Application & Declaration Form

DISSERTATION TITLE: UNMASKING INSIDER THREATS IN ELECTRONIC HEALTH RECORDS (EHR): A COMPREHENSIVE ANALYSIS OF RISKS, IMPACTS, AND STRATEGIC MITIGATION MEASURES FOR ENHANCED HEALTHCARE DATA SECURITY

RESEARCHER'S NAME: SALINI CHEMMENGATTUVALAPPIL MOHANDAS

PROGRAMME OF STUDY:MSC IN MEDICAL DEVICE TECHNOLOGY AND BUSINESS

SUPERVISOR'S NAME: MINA GHAHREMANZAMANEH

DECLARATION:
The information in this application form is accurate to the best of my knowledge. I undertake to abide by the principles outlined by Innopharma/Griffith College ethics policy in my research dissertation. I confirm that I have completed a full ethics assessment for my research dissertation as per the college guidelines. I will not begin my primary research until such approval from my supervisor and/or ethics Committee has been obtained.
I pledge to carry out my research according to the Innopharma/Griffith College academic integrity standards. Any results presented in my dissertation will be from my own, original research, I will reference and/or acknowledge any material or sources used in its preparation and I will not plagiarise the work of anyone else.

For Student:
STUDENT SIGNATURE: 

DATE:24/03/2025

The research contained within this research dissertation proposal has been approved.

For Supervisor:
Ethics Committee Approval Required: Yes ☐ No ■

SUPERVISOR SIGNATURE:

DATE: 28/03/2025

For Ethics Committee (if required):

Ethics Committee Approval Given: Yes ☐ No ☐

ETHICS COMMITTEE MEMBER SIGNATURE:

DATE:

NOTE: Supervisors are responsible for ensuring their students fill in this form correctly and that all ethical areas have been considered.

SECTION 1: DESCRIPTION OF RESEARCH STUDY

1.1 Purpose and objectives of research *[300 words maximum/ use literature review findings to guide]*

Through better patient care coordination, improved medical research, and simplified data management, electronic health records, or EHRs, have revolutionized the healthcare industry. Digital records enable real-time data access, which lowers medical errors and enhances decision-making. EHR integration in pharmaceuticals and biotechnology has also improved healthcare efficiency. But there are also serious security issues brought forth by digitization, especially insider threats.

EHR systems are particularly vulnerable to insider threats, or security lapses that start inside a healthcare institution. Because they originate from trusted persons with authorized access, insider breaches are more difficult to identify and prevent than external cyberattacks. These dangers include careless inadvertent breaches as well as malevolent actions like data theft and sabotage. Despite the severe effects of insider threats, such as breaches of patient privacy, monetary losses, and noncompliance, the majority of existing security measures concentrate on exterior threats, leaving a large research void.

To address these gaps:

Identify and Categorize Insider Threats – Examine the types, sources, roles, and access levels of insiders involved in EHR security breaches, classifying threats as malicious, negligent, or accidental.

Assess the Impact of Insider Threats – Analyze the consequences of breaches on EHR security, patient data privacy, and healthcare organizations, including financial, reputational, and legal implications.

Evaluate Existing Security Measures – Review current technologies, policies, and mitigation strategies to identify gaps and limitations in protecting EHR systems from insider threats.

Develop Effective Mitigation Strategies – Propose a comprehensive framework with actionable recommendations for preventing, detecting, and responding to insider threats in EHR systems.

This study intends to strengthen EHR security, lower insider threats, and better safeguard sensitive patient data by providing practical insights to healthcare businesses, legislators, and cybersecurity experts.

1.2 Research methodology:

Philosophical approach

This study evaluates EHR security using a pragmatic, survey-based methodology, with an emphasis on insider threats. With the help of surveys, administrators, IT security specialists, and healthcare professionals can effectively obtain information about the prevalence, impact, and mitigation techniques of threats.

Primary Data Collection Strategy

This study will utilize **online surveys** as the primary method for gathering data on insider threats to Electronic Health Records (EHRs). Surveys offer a **structured, scalable, and anonymous** approach, allowing key stakeholders—healthcare professionals, IT security specialists, and hospital administrators—to share their insights effectively.

Survey Design

The survey will incorporate both **closed-ended and open-ended questions** to facilitate **quantitative analysis** while capturing **qualitative insights**. Key focus areas include:

- **Demographics** (job role, experience, department)
- **Types of Insider Threats** (malicious, negligent, accidental)
- **Impact on EHR Security** (privacy risks, financial and legal consequences)
- **Existing Security Measures** (current policies, access controls, monitoring tools)

- **Mitigation Strategies** (recommendations for improving security)

Participant Selection & Sample Size

A **purposive and stratified sampling** approach will ensure a diverse representation across different hospital settings and professional roles. The target sample size is **100–200 participants**, with a minimum of **50 respondents per stakeholder group** to support meaningful comparisons.

We get sample size through formula as follows

Optimal sample size: ~350–400 for robust statistical reliability.

Minimum viable sample: 100–200, with at least **50 participants per stakeholder group** for meaningful subgroup comparisons.

Data Collection Process

The survey will be distributed via:

- **Online platforms** (Google Forms, SurveyMonkey, institutional email lists)
- **Healthcare institutions** (internal communications, professional networks)
- **Cybersecurity forums** (IT security communities, healthcare associations)

To **enhance response rates**, weekly reminders will be sent for a period of **four weeks**.

Pilot Testing

A **small-scale pilot study** will be conducted to evaluate survey clarity, structure, and usability. Participant feedback will be used to refine the survey before full implementation, ensuring reliability and accuracy.

By adopting a **structured, anonymous, and scalable approach**, this methodology minimizes response bias while enabling comprehensive insights into EHR security risks and mitigation strategies.

SECTION 2: POSSIBLE ETHICAL ISSUES

Answer 'yes' or 'no' to the following questions.

SUBJECT MATTER

Does the research proposal involve:

Research into specific company activities that would be deemed sensitive or confidential	No
Research into politically and/or racially/ethnically and/or commercially sensitive areas	No
Sensitive, personal, professional or corporate issues	No

RESEARCH PROCEDURES

Does the research proposal involve:

Research that might damage the reputation of companies or participants	No
Research that may negatively affect the reputation of Griffith College/Innopharma	No
Use of personal records without consent	No
Use of company data without consent	No
The offer of any inducements to participate	No
Audio or visual recording without consent	No
Using a language other than English	No

PARTICIPANTS

Does the research proposal involve:

People who are not competent and/or fluent in English	No
Does your research group include any of the following vulnerable groups	No

(Adults with psychological impairments; Adults with learning difficulties; Adults under the protection/control /influence of others (e.g. in care/prison); Relatives of ill people (e.g. parents of sick children); Hospital or GP participants recruited in a medical facility; persons under the age of 18)

If you have answered NO to ALL questions, please go straight to Section 4.

If you have answered YES to ANY question in SECTION 2, you must fill in SECTION 3.

SECTION 3: STEPS TAKEN TO AVOID ETHICAL ISSUES

[Only fill in this section if you answered YES to ANY of the questions in Section 3. For example, if you answered yes to including participants who are not fluent in English, you might put forward a plan that offers your survey in two languages to take this into account. Another example could be a study where the researcher wants to include information about the care received by children with a long-term condition but it would not be ethical to approach the children directly but it might be acceptable to instead ask parents questions about their child's care. If these plans are acceptable to your supervisor, you may not need to apply for ethical approval from the Ethics Committee].

3.1. If your ethics relates to ***Subject Matter***, outline your action plan to work around any sensitive issues.
3.2. If your ethics relates to ***Research Procedures***, outline your action plan to deal with possible ethical issues in your research procedures.
3.3. If your ethics relates to ***Participants***, outline how you will protect vulnerable persons or those that do not have English as their first language.

SECTION 4: ABOUT YOUR PARTICIPANTS

4.1. Outline your participant profile and why you have chosen them for this study *[Do not provide names except where it is deemed impossible to conceal identity].*

This study focuses on three key groups involved in Electronic Health Records (EHR) security to capture diverse perspectives on insider threats:

1. Healthcare Professionals (Doctors, Nurses, Administrative Staff)

Role: Regular EHR users responsible for handling patient information.

Reason for Inclusion: Provide insights into human errors and unintentional security risks.

2. IT Security Specialists (Cybersecurity Experts, System Administrators) Role: Manage security systems and monitor threats.

   Reason for Inclusion: Offer a technical viewpoint on vulnerabilities and defense strategies.

3. Hospital Administrators (Policy Makers, Compliance Officers)

   Role: Ensure regulatory compliance and enforce security policies.

   Reason for Inclusion: Provide perspectives on organizational security frameworks and enforcement challenges.

4.2 How do you plan to gain access to/contact/approach your participant(s).

To reach out to participants, I will employ the following methods:

1. Online Platforms: Distribute surveys through platforms such as Google Forms and SurveyMonkey via institutional email lists and professional networks.
2. Healthcare Institutions: Collaborate with hospitals and clinics to circulate surveys through internal communication channels like emails and newsletters.
3. Professional Networks: Engage with healthcare associations, cybersecurity forums, and LinkedIn groups to connect with IT specialists, hospital administrators, and healthcare professionals.
4. LinkedIn Outreach: Connect with relevant professionals on LinkedIn, send personalized messages explaining the study's purpose, and share the survey link.
5. Personalized Invitations: Send tailored emails to selected participants explaining the study's objectives and potential benefits.
6. Reminder Emails: Issue weekly reminders over four weeks to encourage participation.

These strategies will ensure a broad and diverse range of participants, increasing survey response rates.

SECTION 5: INFORMATION, CONSENT AND CONFIDENTIALITY

5.1 **Participant Information Letter (PIL) for participants: Attached in the appendix**

[You must submit an information letter for participants with this application, as part of your appendices document. For online surveys, it is sufficient to include a paragraph summarising and explaining the purpose of the research at the beginning of the survey. In all other research e.g. interviews, phonecalls, a PIL should be provided to each participant before they are asked for their consent to take part. A template PIL is available in Moodle].

Please confirm below that your information letter covers:

Description of the research topic and method	Yes
Details of what participation will involve	Yes
Rights to anonymity	Yes
Confidentiality	Yes
Rights to withdraw from the research	Yes
The contact details of the researcher and supervisor (if necessary)	Yes

5.2 **Informed Consent Form (ICF) for participants**

[Informed consent is required for most research. For online surveys, it is sufficient to get the participant to tick two boxes at the beginning of the survey – one to state they understand the research and one to give consent. In all other research e.g. interviews, phonecalls, a signed consent form is required. If the data is gathered online e.g. zoom, a signed consent form can be scanned and sent to the researcher. A template ICF is available in Moodle. The signed ICFs, along with the surveys, audio files or interview notes etc. must be stored in the primary data folder on moodle and can be accessed by Innopharma staff for the purposes of verifying the authenticity of the research carried out and the data collected].

Please indicate below if your research requires a signed consent form by selecting the relevant option only:No

Yes: my research requires signed consent and I have attached an ICF in the appendices of my application.
No: my research study involves an online survey only and/or does not require signed consent

---

SECTION 6: STORAGE OF DATA

[Please ensure that you are abiding by GDPR and the national Data protection laws https://www.hrb.ie/funding/gdprguidance-for-researchers/gdpr-and-health-research/).

*The student is responsible for storage of data and this will be handed over to the college in an electronic format as part of the thesis submission i.e. primary data and completed ICFs where applicable will be added to the primary data folder on moodle. The rationale is to keep data **as long as it is still useful** and there is an intention to use it further **for research** so if this is not the case then this can be stipulated here and a shorter retention period given.]*

6.1. How will you store the research data and for how long? How will you manage data protection issues?

The research data will be securely stored in a password-protected, encrypted digital format. This storage method ensures that only authorized personnel have access to the data, with multiple layers of security, including firewalls and two-factor authentication. All devices used to access the data will be password-protected, and access will be monitored to ensure accountability. The data will be stored for no more than six months to comply with data retention policies. After this period, all data will be securely deleted to protect participant confidentiality.

SECTION 7: NON-DISCLOSURE AGREEMENT & STUDENT CONSENT

7.1 **Non-Disclosure Agreement (NDA)**
Will the final dissertation contain any information pertaining to any source what would warrant the use of a Non-Disclosure Agreement (NDA) e.g. industry-based research?

No

7.2 **Student consent**
If a Non-Disclosure Agreement (NDA) is not required, does the Student consent to allow their completed dissertation to be held/published by Innopharma/Griffith College?

Yes

SECTION 8: RECORDING AND RETENTION OF DISSERTATION VIVA

8.1 **Viva Recording**
The Dissertation viva will be recorded. This recording may be used to facilitate assessment by Innopharma staff, a third reader if necessary and/or if requested by the external examiner for the Programme. The recording will be held in line with current GDPR guidelines and will not be made publicly available.

SECTION 9: DOCUMENT CHECKLIST

NOTE: Applicants must attach the following documents in electronic format to the appendix.

Which documents are added to the appendix? Please tick N/A if not applicable:

9.1 Participant Information Letter (PIL) for participant	N/A
9.2 Informed Consent Form (ICF) for participant	N/A
9.3 Questions/survey for interviewees/focus groups etc *(can be in draft form)*	Yes
9.4 Any other documents e.g. Non-Disclosure Agreement	N/A

I confirm that this application is complete and all required documents are included in the appendix.

For Student:
STUDENT SIGNATURE:

DATE:24/03/2025

SECTION 10: APPENDIX

Survey Questions: Insider Threats to HER Systems

Purpose:
This study aims to investigate insider threats to Electronic Health Records (EHRs) and explore security measures and mitigation strategies in healthcare settings.
Procedures:
Participants will complete an anonymous online survey with both closed and open-ended questions on insider threats, HER security, and improvement recommendations.
Risks:
There are no significant risks, but discussing security threats may cause discomfort. Responses are anonymous and confidential.
By ticking the box, you confirm your understanding and consent to participate.

I have read and understood the purpose, procedures, and potential risks associated with this research study.

○ Ye s ○ N o

I consent to participate in this study voluntarily and understand that my responses will be kept confidential and used solely for research purposes.

○ Ye s ○ N o

1. **What is your current job role?**
    - Physician ○
    - Nurse ○
    - Administrative Staff ○
    - IT Staff ○
    - Clinical Support Staff ○
    - Other (please specify): _____

2. **How many years of experience do you have in your current field?**
    - Less than 1 year ○
    - 1–3 years ○
    - 4–7 years ○
    - 8–10 years ○
    - More than 10 years

3. **What type of healthcare institution do you work in?**
    - Public hospital ○
    - Private hospital/clinic ○
    - Research facility ○

Governm

ent healthcare

agency ○

Telemedi

cine provider ○

Other

(please

specify):

_____

4. **How familiar are you with Electronic Health Record (HER) systems?**
   - ○ Not familiar at all ○ Somewhat familiar ○ Moderately familiar ○ Very familiar ○ Expert level
5. **How frequently do you access Electronic Health Records (EHRs) in your role?**
   - ○ Multiple times a day ○ Once a day ○ A few times a week ○ Rarely ○ Never

---

Awareness of Insider Threat

6. **Are you aware of the risks associated with insider threats to HER security?**

- Yes ○

  No

7. **Have you ever encountered or heard of an insider threat incident in your organization?**

   - Yes ○

     No

8. **Which type of insider threat do you believe is most common in your organization?**

   - **Malicious threat (e.g., data theft, sabotage):**

     - Yes
     - No
     - Not sure ○ **Negligent threat (e.g., careless data handling):**

     - Yes
     - No
     - Not sure ○ **Accidental threat (e.g., unintentional errors):**

     - Yes
     - No
     - Not sure

If yes to any ; describe----------

9. **How often do you think insider threats pose a risk to HER security?**

   - Rarely ○

     Occasion

     ally ○

     Frequentl

     y ○ Always

10. **What do you think is the most significant impact of insider threats on healthcare organizations?**

- Financial loss
- Legal consequences
- Operational disruptions
- Reputational damage

11. **How concerned are you about insider threats affecting patient data security?**

- Not concerned
- Somewhat concerned
- Very concerned

12. **Do you believe that insider threats can cause major financial losses for healthcare organizations?**

- Yes
- No

13. **In your opinion, how do insider threats affect patient trust in healthcare institutions?**

- Negligible
- Moderate
- Significant

14. **How do insider threats impact patient care or operations?**

- No impact
- Minor impact
- Moderate impact
- Significant impact
- Severe impact

Security Measures & Policies

15. **Does your organization have policies to address insider threats?**

- Yes
- No
- Not sure

If yes describe…….

16. **What security measures does your organization currently use to protect EHRs? (Select all that apply)**

- Access control
- Anomaly detection
- Employee monitoring
- Encryption
- Training
- Other (Please specify): _____

17. **How effective are these policies?**

- Not effective at all
- Slightly effective
- Moderately effective
- Very effective
- Extremely effective

18. How often training you got?

- Rarely
- Periodically
- Very often

19. **Which access controls are in place? (Select all that apply)**

- Role-based access
- Multi-factor authentication (MFA)
- Time/location-based restrictions
- Automatic logouts
- Limited access to sensitive data

20. **Are monitoring tools used to detect suspicious activity?**

- Yes (e.g., user activity logs, anomaly detection)
- No
- Not sure

21.What mitigation strategies do you think would be most effective against insider threats?

- Policies & governance
- Employee training
- AI-driven security
- All of the above

21. What additional strategies should your organization implement?(Open-ended)

TEMPLATE - Participant Information Letter

Please pay attention to:

- The **content** of the letter particularly the importance of using plain English.
- The **appearance** of the letter particularly the font and font size used.
- The National Adult Literacy Agency provide useful advice to ensure the letter is suitable for your target audience and is available at www.simplyput.ie.

[TITLE OF THE STUDY]: **Unmasking Insider Threats in Electronic Health Records (EHR): A Comprehensive Analysis of Risks, Impacts, and Strategic Mitigation Measures for Enhanced Healthcare Data Security**

I would like to invite you to take part in a research study. Before you decide you need to understand why the research is being done and what it would involve for you. Please take time to read the following information carefully. Ask questions if anything you read is not clear or if you would like more information. Take time to decide whether or not to take part.

WHO I AM AND WHAT THIS STUDY IS ABOUT

My name is Salini Chemmengattuvalappil Mohandas, and I am currently pursuing a master's degree in Medical Device Technology and Business at Griffith College. This research is being conducted as part of my academic studies and will contribute to the completion of my qualification.

We are conducting this study to analyze insider threats in Electronic Health Records (EHR) systems, examining the associated risks, impacts, and strategic mitigation measures to enhance healthcare data security. The study aims to provide a comprehensive assessment of potential vulnerabilities within EHR systems and explore effective strategies for strengthening data protection.

This research is an academic endeavor and does not assume any particular outcomes in advance. It seeks to provide an objective analysis of insider threats and contribute valuable insights into improving security frameworks in healthcare data management.

WHAT WOULD TAKING PART INVOLVE?

If you agree to take part, you will be asked to complete a survey on insider threats in Electronic Health Records (EHR) systems. Participation is voluntary, and you may withdraw at any time.

The study aims to minimize any impact on your daily life, requiring approximately **[5 to 10 minutes]** of your time.

Your insights will help improve healthcare data security. If you have any questions, feel free to ask.

WHY HAVE YOU BEEN INVITED TO TAKE PART?

You have been asked to participate in this study due to your [role/expertise/professional experience] in data security, Electronic Health Records (EHR) systems, or healthcare. Your observations are helpful in comprehending insider threats, their effects, and possible countermeasures.

The selection of participants was based on their engagement or pertinent knowledge of healthcare data administration, guaranteeing an educated viewpoint on the subject of the study.
The suggestions you make to strengthen EHR security will be influenced by your input.

DO YOU HAVE TO TAKE PART?

Please note:

- Participation in this study is entirely voluntary.
- Choosing not to participate will have no adverse consequences.
- You may decline to answer any question or withdraw from the study at any time without explanation.
- If you wish to withdraw, please contact **[SALINI CHEMMENGATTUVALAPPIL MOHANDAS]** at **[salucmohandas@gmail.com]**.

Your decision will be fully respected, and any data collected before withdrawal will be securely deleted if requested.

WHAT ARE THE POSSIBLE RISKS AND BENEFITS OF TAKING PART?

Benefits: By taking part, you will help advance knowledge about insider threats in Electronic Health Records (EHR) systems. The information acquired could aid in the creation of more robust data security plans, which would benefit patient privacy and healthcare institutions.

Risks:

Confidentiality: There is a slight chance of identifying even though all data will be anonymised. All comments will be safely kept, and no personal information will be disclosed, in order to lessen this.

Psychological Discomfort: Certain subjects, including insider threats or security breaches, may be delicate. You can skip any question or stop participating at any moment if it makes you uncomfortable.

Support resources will be provided in case of distress, and you can get in touch with if you have any questions.

WILL TAKING PART BE CONFIDENTIAL?

Yes, your involvement will remain private. Only research will be conducted using the anonymized and safely kept survey results.

The boundaries of confidentiality may be violated if answers reveal a significant danger of abuse, harm, self-harm, suicidal thoughts, or illegal conduct.

When using company data, the appropriate authorization will be acquired. Do not hesitate to ask any questions.

HOW WILL INFORMATION YOU PROVIDE BE STORED AND PROTECTED?

Data from the survey will be safely kept in [name a place, such as a password-protected file on a secure server, where only the researcher will have access.

Following the conclusion of the study, the data will be kept for six months before being safely removed.

The information you have submitted can be accessed at any time in accordance with freedom of information laws.

WHAT WILL HAPPEN TO THE RESULTS OF THE STUDY?

I will submit this research to Griffith College as a part of my master's dissertation. All dissertation research projects and their contents will be available in the college library, and if relevant, they might even be featured in an online repository or e-journal.

Beyond submission for academic evaluation, there are currently no plans for publication, conference presentations, or instructional use.

WHO SHOULD YOU CONTACT FOR FURTHER INFORMATION?

RESEARCHER: SALINI CHEMMENGATTUVALAPPIL MOHANDAS

CONTACT: salucmohandas@gmail.com/+353(899852864)

THANK YOU