AKENTEN APPIAH-MENKA UNIVERSITY OF SKILLS TRAINING AND ENTREPRENEURIAL DEVELOPMENT -MAMPONG

PERSPECTIVE OF EMPLOYEES' COMPLIANCE WITH ELECTRONIC MEDICAL RECORDS PRIVACY POLICY IN ASHANTI REGION

BY

SIMMS OFOSU

2025

AKENTEN APPIAH-MENKA UNIVERSITY OF SKILLS TRAINING AND ENTREPRENEURIAL DEVELOPMENT

PERSPECTIVE OF EMPLOYEES' COMPLIANCE WITH ELECTRONIC MEDICAL RECORDS PRIVACY POLICY IN ASHANTI REGION

BY

SIMMS OFOSU

(8222030015)

A thesis submitted to the School of Graduate Studies, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, in partial fulfilment of the requirements for the award of a Master of Philosophy degree in Public Health at the Department of Public Health.

DECEMBER, 2025

DECLARATION

Candidate's Declaration

I hereby declare that this thesis is the result of my original work and that no part of it has been presented for another degree at this university or elsewhere.

Candidate's Name: SIMMS OFOSU

Signature …… Date ……

Supervisor's Declaration

We hereby declare that the preparation and presentation of the thesis were supervised in accordance with the guidelines on supervision of the thesis laid down by the Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development.

Principal Supervisor's Name: DR. ERNEST OSEI

Signature …… Date ……

Co-supervisor Supervisor's Name: REV DR. DENIS DEKUGMEN YAR

Signature …… Date ……

ABSTRACT

Electronic Medical Records (EMRs) are increasingly utilized in Ghana to improve healthcare delivery. However, compliance with privacy policies remains a critical concern, particularly in resource-constrained settings such as the Ashanti Region. Understanding perspective of employees' compliance with electronic medical records privacy policy is essential for strengthening patient data protection. To assess healthcare employees' perspective of employees' compliance with electronic medical records privacy policy in selected public hospitals in the Ashanti Region of Ghana. A cross-sectional survey was conducted among 269 healthcare professionals, proportionally sampled from Mampong, Agona, and Ejura Government Hospitals. Participants included medical officers, nurses, records officers, IT staff, and administrators. Data were collected using structured questionnaires and analyzed with descriptive statistics, Fisher's t-test for awareness, and weighted average index models for compliance and influencing factors. Mean awareness scores differed significantly between clinical and non-clinical staff ($t = 3.41$, $p = 0.001$). The Weighted Average Index indicated moderate overall compliance (0.56), with higher scores among staff who had received prior training (WAI = 0.63 vs. 0.48, $p < 0.05$). Logistic regression identified training exposure (AOR = 2.84, 95% CI: 1.62–4.96), leadership support (AOR = 1.91, 95% CI: 1.15–3.18), and system usability (AOR = 2.07, 95% CI: 1.22–3.51) as significant predictors of compliance. Challenges of EMR privacy policy included inadequate training (47.3%), limited resources (42.6%), outdated EMR systems (38.5%), and high workload (35.1%). Improving EMR privacy compliance in Ghana depends on focused staff training, clear and simple policies, adequate resources, and upgraded technology to protect patient data and strengthen institutional trust.

ACKNOWLEDGEMENT

For his tremendous advice, encouragement, and support during my research journey, I would like to sincerely thank my supervisor, Dr. Ernest Osei. His astute criticism and steady commitment have greatly influenced the direction of this work.

I also want to express my sincere gratitude to my wife, Evelyn Owusu Dentaah, for her unwavering love, tolerance, and comprehension. Her steadfast assistance and selflessness have given me courage and inspiration.

I want to express my sincere gratitude to my amazing children, Rocklyn Ofosu, Simms Twum Ofosu, and Evelyn Lois Eniyena Ofosu, for their inspiration, love, and patience. I feel so happy and purposeful when you are in my life. Above all, I thank God for His grace, wisdom, and the strength to complete this research successfully. Thank you all for your immense contributions to my academic journey.

DEDICATION

I dedicate this research work to my beloved wife, Evelyn Owusu Dentaah**,** whose unwavering love, support, and encouragement have been my greatest source of strength throughout this journey.

To my wonderful children, Rocklyn Ofosu, Simms Twum Ofosu, and Evelyn Lois Eniyena Ofosu**,** you are my greatest inspiration. Your love and patience have been a constant motivation for me to strive for excellence.

Above all, I dedicate this work to God Almighty**,** whose grace, wisdom, and strength have made this accomplishment possible.

TABLE OF CONTENT

CAPTER THREE

CHAPTER FOUR

LIST OF TABLES

LIST OF FIGURES

ETHICAL APPROVAL

Kwame Nkrumah University of Science and Technology, Kumasi

College of Health Sciences
SCHOOL OF MEDICINE AND DENTISTRY

COMMITTEE ON HUMAN RESEARCH, PUBLICATION AND ETHICS

13th December, 2024

Our Ref: CHRPE/AP/1303/24

Mr. Simms Ofosu
Akenten Appiah-Menka University of Skills
Training and Entrepreneurial Development
AAMUSTED-KUMASI.

Dear Sir,

LETTER OF APPROVAL

Protocol Title: ***"Perspective of Employee's Compliance with Electronic Medical Records Privacy Policy in Ashanti Region."***

Proposed Site: ***Mampong Government Hospital, Agona Government and Ejura Government Hospital.***

Sponsor: ***Self-Sponsored.***

Your submission to the Committee on Human Research, Publications, and Ethics on the above-named protocol refer.

The Committee reviewed the following documents:

- A notification letter of 27th August 2024 from the Regional Health Directorate, Kumasi (study site) indicating approval for the conduct of the study in the region.
- A Completed CHRPE Application Form.
- Participant Information Leaflet and Consent Form.
- Research Protocol.
- Questionnaire.

The Committee has considered the ethical merit of your submission and approved the protocol. The approval is for one year, renewable after that, from **13th December 2024 to 12th December 2025**. The Committee may, however, suspend or withdraw ethical approval at any time if your study is found to contravene the approved protocol.

Data gathered for the study should be used for the approved purposes only. Permission should be sought from the Committee if any amendment to the protocol or use, other than submitted, is made of your research data.

The Committee should be notified of the actual start date of the project and would expect a report on your study, annually or at the close of the project, whichever one comes first. It should also be informed of any publication arising from the study.

Thank you for your application.

Yours faithfully,

Rev. Prof. John Appiah-Poku.
Honorary Secretary
FOR: CHAIRMAN

Room 7, Block L, School of Medicine and Dentistry, KNUST, University Post Office, Kumasi, Ghana
Tel: +233 (0) 322 063 248 Mobile: +233 (0) 205 453 785 Email: chrpe.knust.kath@gmail.com / chrpe@knust.edu.gh

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Electronic medical records (EMRs) are digital versions of the paper-based medical records traditionally used by healthcare providers to document patient information. These records include a patient's medical history, diagnoses, treatment plans, medications ,lab results, and other critical health data (Keshta & Odeh, 2021).The widespread adoption and implementation of electronic medical records (EMRs) has significantly increased in recent years.(Janssen et al., 2021). This growth in EMR usage has been facilitated by the integration of technology into healthcare delivery systems. Technology catalyzes improving healthcare quality by enabling the adoption of comprehensive information systems that manage hospital operations across administrative, financial, and clinical domains (Janssen et al., 2021).

According to Senbekov et al. (2020), advancements in the Internet and information technology have facilitated the utilization of electronic patient records, allowing medical professionals to access patients' data, such as laboratory results and medical images. Many hospitals are increasingly advocating for electronic health records over traditional paper-based medical records, offering streamlined automated systems that support healthcare professionals in diagnosis and treatment. (Cerchione et al., 2023). Electronic medical records (EMRs) are designed to assist medical staff in their daily tasks through electronic data processing (Janett & Yeracaris, 2020). This shift is crucial because hospitals encounter numerous challenges associated with manually storing and disseminating patients' health records using methods such as pen and paper, as well as human memory (Kurniawati, 2017). Therefore, electronic medical records are replacing

manual methods of storing medical information. Typical EMRs encompass various subsystems such as appointment scheduling, admissions, discharge, transfers, dietary management, prescription ordering, treatment planning, routine clinical notes, laboratory data management, and other functionalities (Janssen et al., 2021).

In addition to transitioning health information into electronic formats, some institutions have progressed to implementing cloud-based electronic storage systems. These systems facilitate the transmission of patient information over electronic networks, enabling the collaborative sharing of electronic medical records via the Internet.(Janssen et al., 2021). In developing nations, the adoption of electronic information systems is still in its early stages (Janssen et al., 2021). It was noted that in South Africa, the utilization of EMRs was in its infancy. Sriram & Mohanasuundaram, (2020) reported efforts to promote the adoption and utilization of EMRs through the establishment of health management information systems (HMIS) policies, legal frameworks for health data reporting, policies for medical records, computerized district health management information systems, and the establishment of centralized health information centres.

Despite the limited deployment of EMRs in developing African countries, even by 2014 (Tsai et al., (2020) highlighted that nearly all general practitioners in Australia had implemented electronic medical records. Over the past decade, there has been an increase in the implementation of EMRs in healthcare settings across both developed and low- to middle-income countries.

Electronic medical records (EMRs) are underutilized in sub-Saharan Africa, according to Bervell & Al-Samarraie, (2019) Despite the increasing number of information technology initiatives, some developing countries have begun implementing EMRs.

However, Bervell & Al-Samarraie, (2019) noted that many of these projects are still in their early stages. In Ghana, several studies have documented the adoption of EMRs. Niang et al., (2023) describe the implementation of a real-time registration and verbal autopsy system using MGV-NET, an open-source health information system.

Additionally, Caliskan, (2016) found that the Komfo Anokye Teaching Hospital in Ghana utilizes EMRs for functions such as patient registration, search for patient previous data, and triage.

According to Aithal & Madhushree, (2019) Information and Communication Technology (ICT) refers to the broad range of technologies and tools used to handle telecommunications, media, and information processing. ICT encompasses all digital technologies that enable the collection, storage, processing, transmission, and sharing of information.

According to Janssen et al.,(2021), the integration of information and communication technology (ICT) into healthcare is essential for enhancing patient safety and reducing healthcare costs. They emphasize the critical role of ICT in improving healthcare delivery. The security of electronic medical records (EMRs) is a crucial concern, focusing on three main principles: confidentiality, integrity, and availability.(Janssen et al., 2021). Confidentiality ensures that information is disclosed only to authorized users, integrity ensures that information is created and modified by authorized personnel, and availability ensures that authorized users can access information when necessary. EMRs must incorporate robust security measures to safeguard the confidentiality of medical

information, ensure the accuracy and validity of patient data to protect patient rights and implement measures to preserve the privacy of patient records (Janssen et al., 2021).

Electronic medical records (EMRs), despite their capability to provide comprehensive healthcare data and detailed patient information, face significant challenges related to security and privacy (Keshta & Odeh,2021). Health information privacy (HIP) is a critical issue for both patients and healthcare professionals alike. Patients are particularly concerned about the potential secondary use of their health information for purposes such as research. Meanwhile, healthcare workers are focused on implementing effective measures to restrict access to medical records (Keshta & Odeh, 2021). Recent years have seen a significant rise in threats to healthcare information security(Sari et al., 2022).According to the Health Information and Management Systems Society (HIMSS) Report (2018), approximately 75.7% of hospitals surveyed reported experiencing major security incidents. The HIMSS Report (2018) categorizes the types of security incidents affecting electronic medical records, including online scams or phishing (37.6%), unintentional but negligent insiders (20.8%), hackers (20.1%), malicious insiders (5.4%), social engineering or vishing (4.7%), and other forms. In the Ghanaian health sector, there is a notable absence of policy guidelines regarding electronic data exchanges and the security of patient-identifiable information, which contributes to unclear ownership and security issues(Shah & Khan, 2020).

Security and privacy concerns represent the foremost obstacle to the widespread adoption of electronic health records (EHRs). These issues pose significant challenges in managing EHRs, particularly given the perspectives of both patients and healthcare professionals. Several security and privacy policies have been established to facilitate the

effective implementation of EHR systems. Consequently, there is a critical need to examine the adherence of healthcare facilities in Ghana to these security measures aimed at safeguarding records from potential breaches (Shah & Khan, 2020).

1.2 Problem Statement

The recent implementation of electronic medical records (EMRs) in Ghana's hospitals, whether private or public, symbolizes a critical step toward modernizing healthcare delivery and has improved the accessibility, storage, and management of patient data. However, ensuring compliance with EMR privacy policies among healthcare employees remains a pressing challenge with implications for patient confidentiality, data security, and institutional trust and credibility in healthcare and also several reports of breach of unauthorized access, which could lead to an increased risk of data breaches, legal repercussions, financial losses, and a deterioration in the quality of care. Although the national framework, such as Ghana's Data Protection Act 2012, provides strategies, regional differences in infrastructure, socio-cultural norms, and staff willingness generate irreplaceable obstacles to compliance that are poorly understood. Prevailing research on EMR compliance in Ghana primarily focuses on teaching hospitals in Accra and Kumasi, overlooking the municipal and district hospitals that comprise a mixture of rural and urban healthcare facilities, varying resource availability, and deeply rooted communal values that may conflict with individual privacy norms. Furthermore, the technological infrastructure in many hospitals in the Ashanti region includes outdated systems and limited cybersecurity measures, thereby exacerbating the risk of data breaches. This study seeks to examine the perspectives of healthcare employees on their compliance with EMR Privacy Policies in the Ashanti Region, in order to identify ways to strengthen adherence and improve the protection of patient information.

1.3 Objectives of the Study

The main objective of these studies is to examine the healthcare Employees' Perceptions and Factors Influencing Compliance with EMR Privacy Policies in the Ashanti Region of Ghana

Specifically, the study sought to:

1. Assess the awareness of employees of the EMR privacy policy in the Ashanti Region of Ghana.
2. Determine the perceived level of compliance with the EMR privacy policy in the Ashanti Region of Ghana.
3. Examine the perceptions of employees of factors affecting compliance with the EMR privacy policy in the Ashanti Region of Ghana.
4. Evaluate the challenges faced by employees in using the EMR privacy policy in the Ashanti Region of Ghana.

1.4 Research Questions

1. What is the level of awareness of the EMR privacy policy in the Ashanti Region of Ghana?
2. What is the perceived level of compliance with the EMR privacy policy in the Ashanti Region of Ghana?
3. What are the perceptions of employees of factors affecting compliance with the EMR privacy policy in the Ashanti Region of Ghana?
4. What challenges do employees face in using the EMR privacy policies in the Ashanti Region of Ghana?

1.5 Justification of the study

The digital transformation in healthcare, hallmarking a global adoption of electronic medical records, is expected to ensure efficient care delivery and patient well-being in the future and provide seamless data interchange. The major investment in EHR implementation worldwide derives from the advantages that a centralized storage of accessible patient information provides within health systems. But this digital shift bears a very serious concomitant problem, and that is how to safeguard the highly sensitive data related to the patients' privacy and security. Data breaches occur most likely in health care settings, with global findings indicating that the health sector is the prime target for cyber-attacks or accidental disclosures leading to heavy penalties, damage to the reputations of the hospital concerned, and most importantly, lost patient trust. For instance, global trends indicate that human error and insider threats account for a significant percentage of healthcare data breaches, underscoring the indispensable role of employee compliance.

Ghana has been accelerating the discussion on digital health internally with the possible e-health strategy of the Ministry of Health and the Ghana Health Service integrating increasing EHR systems within a wide range of facilities. This important modernization effort, aimed at improving operational flow and healthcare delivery, has turned the Ashanti Region into quite a hub for healthcare services in Ghana since it contains various public and private facilities, including the major teaching hospitals and regional hospitals. As EHR systems become more widespread within this healthcare landscape, the degree of vulnerability of patient information is critically dependent on the healthcare personnel's adherence to applicable privacy policies. Ghana's Data Protection Act, 2012

(Act 843), fashions the legal framework for data privacy, but this becomes effective in the healthcare context upon actual implementation with full cooperation of employees.

This study becomes pertinent given that while one or more policies may exist on paper, actual compliance in practice is often multifaceted, influenced by employee knowledge, attitudes and barriers or facilitators within the work environment perceived to affect implementation. Unlike some of those Western nations, which have advanced enforcement mechanisms and an ingrained culture of data privacy, the healthcare facilities in the Ashanti Region would probably face much more than the advanced enforcement mechanisms and entrenched culture of data privacy in developed countries, such as the varying degrees of digital literacy among staff, resource constraints for comprehensive training and the different terrain in which they operate. Understanding how employees perceive awareness of policies, the importance of privacy and the factors that affect their compliance with them is necessary for identifying the gap and designing targeted interventions. The study will ultimately become a key diagnostic tool. By assessing employee adherence to EHR privacy policies in the Ashanti region, this assessment will allow for the provision of evidence-based recommendations that fit directly into local healthcare administration. The results will assist in crafting better awareness programs, strengthen existing privacy policies, and enhance data protection mechanisms to reduce breach risks; thereby increasing patient trust in the digital health system, such that the benefits of EHRs can be harnessed without compromising the very right to privacy of patient data in one of the most populated regions of Ghana.

1.6 Significance of the study

The study served as a reference for healthcare institutions and their management; the Ashanti Region healthcare facilities stand to gain utmost and immediate effects from this research. By understanding how employees view compliance with EMR privacy, administrators can now rethink and improve current privacy policies and strategies for implementation in hospitals. The findings will enable them to:

1. Tailor Training Programs: Instead of general privacy-attentive sessions, institutions can develop specific training that directly addresses specific misconceptions as identified in the study. It thus makes training more effectual and cost-saving while leading to tangible improvements in compliance.
2. Improved Policy Communication and Enforcement: Research will provide insight into the channels and the most preferred means of policy dissemination among employees. Further, it will inform on developing rigorous internal audit mechanisms and the disciplinary measures to be applied in case of violations as a way of developing a culture of accountability.
3. Lower Risks: Identifying compliance weaknesses beforehand and addressing them can have a tremendous impact on reducing the possibility of data breaches, unauthorized access, and other privacy violations. Safeguarding the reputation, avoiding potential legal penalties, and bolstering the overall security posture within the institution are by-products of this.
4. Optimize Resource Allocation: Analysis of the main causes of non-compliance will guide management in the allocation of resources to respond most effectively, whether for technology upgrades, additional roles for privacy officers, or continuous professional development for staff.

Beyond the institutional level, patients and the much wider arena within the Ashanti Region will be the major beneficiaries. For EMR privacy policies, the main intent is to protect patient confidentiality, and the benefits of this come about when effective compliance of employees comes into play. Patients will, therefore, enjoy:

1. Improved Trust and Confidence: In so much as knowing that healthcare providers are well-versed in and committed to EMR privacy policies, this goes on to generate much trust toward the healthcare system. Increased confidence leads to a higher tendency of patients disclosing even confidential medical issues, which is of much importance for a complete diagnosis and even treatment.
2. Protection of Personal Health Information: Effective employee compliance can be directly translated into low chances of inappropriate access to, use of, or disclosure of patient data. This secures individuals from identity theft, discrimination, or other potential harms arising from a breach of privacy.
3. Improved Patient Outcomes: When patients have a sense of security and trust, they are more likely to follow treatment plans and participate in their care, ultimately leading to better health outcomes.

Furthermore, the study's findings are valuable to policymakers at both regional and national levels, such as the Ministry of Health and Ghana Health Service. The learnings from Ashanti Region can serve as key reference points for:

1. 1.Informing National EMR Privacy Legislation and Guidelines: Challenges found either to be common or marketing features under which compliance was successfully achieved can serve to influence in one way or another the uplifting or enactment of national policies into practice, measurable, and applicable to the real world.

2. 2.Benchmarking and Replication: This study creates an information base for a one region to understand employee compliance. That benchmark could be used for comparison in other regions in Ghana or possibly in other developing nations that share similar challenges in EMR implementation. The means of Ashanti success could be replicated away.
3. 3.Future Research and Academic Discourse: This study sets a stepping stone for future scholarly investigations in health information management, privacy, and organizational behaviour in Ghana. It could also spur further research on the efficacy of interventions; technological solutions; or the change in privacy perceptions over time.

In conclusion, "Perspective of Employees' Compliance with Electronic Medical Records Privacy Policy in Ashanti Region" is thus more than an academic exercise; it is a viable diagnostic tool for the shifting terrain of digital healthcare in Ghana. By painstakingly dissecting the human angle on EMR privacy, the study proposes to fill the yawning gap between policy intention and practical enforcement. The results would be paramount for the health institutions to set up a sound culture of privacy and employee empowerment through apt knowledge regarding patient information. This advantage cascading through enhanced organizational viability and reduced risk, patient trust, and informed national policy accentuates the essence of this study in creating a safe, credible, and viable health system for Ashanti Region and beyond.

1.7 Scope of the Study

The scope of this research is to evaluate adherence by health professionals to electronic medical records (EMR) privacy policies in public health institutions in the Ashanti

Region of Ghana. More specifically, the focus is on the views, awareness, and behavioural factors related to adherence to privacy regulations on the part of healthcare personnel. The study focuses on three selected government hospitals, particularly, Mampong Government Hospital, Agona Government Hospital, and Ejura Government Hospital, with a multistrata sample of respondents comprising medical doctors, nurses, medical records officers, IT personnel, and administrative staff.

The study is cross-sectional and descriptive; hence, quantitative data collection methods using structured questionnaires on Google Forms were employed to achieve high outreach, cost-effectiveness, and data security. Self-reported adherence to and observation of behaviours on EMR privacy compliance were assessed to yield insights into the individual, organizational, and technological determinants of compliance as well as barriers: operational issues, system usability, and human resistance, among others.

In this regard, the study explores other important variables concerning stakeholders' views, their awareness of privacy policies, and how organizational variables such as leadership support and availability of resources impact EMR privacy compliance. Ethical considerations, including voluntary participation, informed consent, confidentiality, and data security, have been integrated into the research protocols.

The findings are all limited to the public health sector of the Ashanti Region at the time of data collection, as the scope does not extend outside the selected healthcare facilities or involve the qualitative exploration of compliance barriers. The results will inform policy recommendations for enhancing EMR privacy adherence, safeguarding patient

data, and developing targeted interventions to improve compliance practices among healthcare professionals.

1.8 Limitations of the study

The study acknowledges certain limitations that may impact its generalizability and findings. Time Constraints, such as the limited time for data collection, may restrict the depth of engagement with participants, potentially affecting the comprehensiveness of the data. Moreover, Response Bias, that is, respondents may provide socially desirable answers, especially when asked about sensitive topics like privacy compliance. This could result in data that does not accurately reflect actual behaviours. Additionally, although the study employs stratified sampling, the findings may not be fully generalizable to all healthcare facilities in the Ashanti Region, particularly those with varying levels of resource availability or patient demographics.

1.9 Organization of the Study

The study was organized into various chapters. Chapter one introduces the background, statement of the problem, objectives, research questions, justification of the study and scope of the study, limitations and organization of the study. The second chapter consists of literature and conceptual frameworks. The methodology is presented in Chapter three, which includes research design, population, sampling designs, methods to collect data, and analysis of data. Chapter four is about findings and analysis of the data. Chapter five speaks about results concerning other literature. Lastly, Chapter six enumerates the conclusions and recommendations derived from the findings of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents a detailed review of the existing literature on factors influencing employee compliance with the privacy policies of Electronic Medical Records (EMR) systems, with a specific focus on the Ashanti Region of Ghana. The chapter is organized to align with the study's general and specific objectives: (1) to examine the awareness of employees regarding EMR privacy policies in the Ashanti Region of Ghana, (2) to determine the perceived level of compliance with the EMR privacy policies, (3) to examine employee perceptions of factors affecting compliance with EMR privacy policies, and (4) to explore barriers faced by employees in adhering to the EMR privacy policies. By examining previous studies, this review aims to provide a comprehensive understanding of the issues related to EMR privacy compliance and the various factors that impact this compliance within the Ghanaian healthcare sector.

2.2 Theoretical Frameworks for The Study

The study can be guided by Ajzen's Theory of Planned Behaviour (TPB) and Deterrence Theory as the foundation to explain how individual and organizational factors influence compliance with EMR privacy policies. Ajzen's Theory of Planned Behaviour suggests that an individual's Behaviour is influenced by three factors: Attitude toward the Behaviour, which includes employees' positive or negative evaluations of following EMR privacy policies. Subjective norms that perceive social pressure to comply with EMR privacy policies, including peer behaviours, organizational culture, and leadership and perceived behavioral control that refers to the extent to which employees feel they have the ability (resources, knowledge, and technical tools) to comply with EMR privacy policies(Knauder & Koschmieder, 2019).

This theory is relevant because it can help explain why employees may or may not comply with EMR privacy policies. If they have positive attitudes, believe their peers and leaders value compliance, and feel they have control over their actions, they are more likely to follow privacy policies. Moreover, the second thus Deterrence Theory focuses on the role of sanctions and punishments in encouraging compliance. It suggests that employees are more likely to comply with EMR privacy policies if they believe that non-compliance will result in significant penalties, such as disciplinary actions or legal consequences. This theory is relevant for explaining how organizational enforcement of privacy policies and the threat of punishment (e.g., sanctions for breaches of privacy) may motivate employees to adhere to EMR guidelines(*Netherlands Annual Review of Military Studies* , 2020).

2.3 Overview of Electronic Medical Records (EMR) and Privacy Policies

Electronic Medical Records (EMR) are digital versions of patients' paper charts that allow for more streamlined healthcare delivery, improved access to patient data, and enhanced healthcare outcomes.(Harrison & Ramanujan, 2011) .EMRs are increasingly being adopted globally as part of efforts to modernize healthcare systems and improve the efficiency of service delivery. They provide healthcare providers with real-time access to patient information, facilitate better coordination among healthcare professionals, and contribute to improved accuracy in diagnostics and treatment planning.(Janett & Yeracaris, 2020)

However, the adoption of EMRs comes with significant concerns regarding the privacy and security of patient data. Privacy policies play a critical role in safeguarding sensitive patient information against unauthorized access, breaches, and misuse (Keshta & Odeh, 2021).These policies outline the guidelines and standards that healthcare institutions

must follow to protect patient data while complying with local, national, and international regulations(Bhyat et al., 2021) In the Ghanaian context, the Data Protection Act, 2012 (Act 843), mandates organizations to implement robust measures for securing personal data, including sensitive health information stored in EMRs(Mensah, 2023).(Protection, 2012).

The effectiveness of EMR systems in safeguarding patient privacy depends heavily on employee compliance with these privacy policies. Compliance is not merely a matter of following rules but involves a combination of awareness, perceptions, organizational culture, and the availability of resources. Employee attitudes towards data privacy, the level of training provided, the usability of the EMR systems, and leadership support are all factors that contribute to whether or not privacy policies are adhered to effectively.(Bisrat et al., 2021).

2.4 Employee Awareness of EMR Privacy Policies

Employee awareness is a fundamental prerequisite for ensuring compliance with EMR privacy policies. Awareness involves not just knowing that privacy policies exist but understanding the details, purpose, and implications of these policies. It also encompasses an appreciation of the risks associated with non-compliance, such as data breaches, legal penalties, and harm to the institution's reputation(Shahnaz et al., 2019).
Global studies, especially about those from developed countries, reveal variability among healthcare employees regarding EMR privacy policies. An example is a study done in the United States where, after the enactment of the Health Insurance Portability and Accountability Act (HIPAA), the majority of health service workers accepted the concept of privacy regulations but were usually not well versed with the specific provisions, patient rights, and permissible data disclosures that might be significantly different

(Ostlund, 2015). Other studies have shown that awareness tends to be higher among staff directly involved in data entry or management-such as the medical coders or the IT personnel -and less in the clinical staff, who would prioritize patient care instead of the other details(Ibrahim et al., 2022).

International awareness gaps arise from factors such as the frequency and quality of privacy training, the clarity and accessibility of policy documents, enforcement mechanisms, and the organization's culture toward privacy in general (Ibrahim et al., 2022). Organizations with regular, mandatory, and enjoyable privacy training are more likely to report higher employee awareness(AlSadrah, 2020). On the other hand, sites where privacy policies are considered burdensome or training is infrequent and superficial show generally lower levels of awareness that might lead to breaches (Ali et al., 2021). On their own, privacy policies can be perplexing; legal terminology embedded in them often defeats understanding for individuals without a legal background (Nii Lantei Wallace-Bruce, 2018).The African context is particularly poor in research on such issues as employee awareness of EMR privacy policies, more especially in-depth, regional studies. However, there are broad studies on health information systems and IT literacy holding some indirect pointers in the African context. Most African nations are in their infancy in transforming their health services into the digital age, grappling with issues like poor IT infrastructure and lack of budgetary provisions for training, and generally a lack of digital literacy exhibited by some sections of the healthcare workforce (Haag et al., 2021). Such systemic challenges would emanate in lower levels of awareness on advanced EMR privacy regulations. According to a study by Essuman et al.(2020), awareness among healthcare workers in Ghana varies significantly depending on the institution and the level of training provided. The study found that institutions with

regular training programs tend to have higher levels of awareness, which in turn leads to better compliance with privacy guidelines.

In the healthcare sector, continuous education and training are critical for maintaining high levels of awareness among employees. Standards et al., (2020) argue that frequent training sessions help refresh employees' knowledge, update them on new privacy regulations, and reinforce the importance of safeguarding patient information. However, a common challenge in many healthcare facilities in Ghana, including those in the Ashanti Region, is the lack of regular training programs focused specifically on EMR privacy (Essuman et al., 2020). In some instances, training is only provided during the initial introduction of EMR systems, with little follow-up thereafter. This lack of continuous education can lead to a gradual decline in awareness and ultimately to non-compliance.

The mode of communication also plays a significant role in enhancing awareness. Effective communication strategies include workshops, digital reminders, bulletin boards, and regular updates through emails or team meetings. (Chai & Zolkipli, 2021).However, studies suggest that communication regarding privacy policies is often inconsistent or inadequate in many healthcare facilities in Ghana.(Bhyat et al., 2021). When communication is sporadic or unclear, employees may forget critical aspects of the privacy policy or remain unaware of updates, leading to unintentional breaches.

Furthermore, the content and structure of training programs are crucial. Training should be practical, relevant, and tailored to the specific needs of healthcare workers. Training that is too theoretical or disconnected from day-to-day operations may not effectively equip employees with the knowledge they need to comply with privacy guidelines(Kuo

et al., 2019). For instance, role-playing scenarios, interactive sessions, and case studies can be more effective than traditional lecture-based methods in reinforcing key concepts related to data privacy.

2.4.1 Gaps Relevant to the Ashanti Region, Ghana

While EMR adoption is on the rise in Ghana, specific empirical studies assessing healthcare employees' awareness regarding EMR privacy policies in the Ashanti Region remain critically lacking. General evaluations of health information systems may make passing mention of user training, but they do little in the way of considering privacy policy awareness in detail. It would be reasonable to expect that the same challenges experienced in other African settings such as inadequate training and varying levels of digital literacy would also apply to the Ashanti Region. However, without direct research, the true extent of such awareness remains unknown. What remains as knowledge gaps for the Ashanti Region include:

Quantitative measurements of awareness levels among different classes of healthcare workers (practitioners, nurses, pharmacists, administrators), Understanding from whom employees receive information on privacy policies (formal training, informal peer learning, personal initiative).

EMR privacy policy provisions that employees least understand. And also How employee awareness will be affected by varying facility sizes, resources, and EMR system maturity across the Ashanti Region. An appropriate study in the Ashanti Region would furnish baseline data that would be helpful in the design of training programs and communication strategies intended to enhance awareness of the privacy policy.

2.5 Perceived Level of Compliance with EMR Privacy Policies

Perceived compliance refers to how employees evaluate their own adherence to EMR privacy policies as well as their perceptions of organizational compliance as a whole. Self-assessment is often influenced by knowledge of the policies, organizational culture, and the availability of monitoring systems (Bhyat et al., 2021) .While perceived compliance is an important indicator of how employees view their behavior, it may not always align with actual compliance. Studies show that employees may perceive themselves as compliant while engaging in practices that inadvertently violate privacy standards, such as sharing passwords, leaving workstations unattended, or accessing patient records without proper authorization(Janssen et al., 2021).

Global, most of the literature addressing perceived compliance with EMR privacy policies worldwide recognizes that there is a general trend of healthcare workers-self-reporting on the positive side, varying with profession and organizational setting. Many healthcare practitioners genuinely believe they are acting in accordance with privacy policies, their conviction motivated by ethical considerations and codes of conduct (Bani Issa et al., 2020). However, this high perception of compliance does not always reflect the results of objective audits, which sometimes reveal mismatches or accidental violations caused due to lack of attention, complex systems, or the burden of workload(AlSadrah, 2020).

Research conducted in countries such as the United States, the United Kingdom, and Australia, which are not only equipped with advanced EMR systems but also have well-structured privacy-protecting frameworks, seems to identify other areas where perceived compliance is either lower or more inconsistent. One of these areas is:

Accessing patient records: Whereas employees may perceive themselves to be accessing records for genuine purposes, the concepts of "genuine" can be rather fuzzy in practice; an example would be accessing records to satisfy curiosity about a celebrity patient or to check on a friend's health status when not involved in the actual patient care(Ndlovu et al., 2021).An example would be sharing information on perceived compliance with rules on sharing patient information with family members, outside providers, or for research purposes, depending, sometimes, on the clarity of policies and the training received(Standards et al., 2020).

Security measures: Employees may perceive their use of strong passwords and logging off systems as compliant behavior, ignoring other steps, such as not sharing login credentials and properly securing physical workstations(Williamson & Prybutok, 2024).

Serious organizational variables, including an apparent culture of accountability, reporting mechanisms for breaches, and consistent enforcement of disciplinary actions, are correlated with higher levels of perceived compliance, as employees know of the consequences of violating the policy(Williamson & Prybutok, 2024).

More limited than on awareness are associated data on the possible compliance with EMR privacy policies in an African context. It therefore seems safe to assume, given all the difficulties with awareness, infrastructure, and training, that perceived compliance might be lower or at least very variable across facilities and countries. For that reason, employees working in such environments would probably have issues reconciling the intention to comply with the practicalities of doing so, either in situations where EMR systems have recently begun operations or are not well-integrated.

A few studies on general health information security practices in the African context have indicated that while health workers generally understand the principle of confidentiality, real-life application of these particular EMR privacy regulations would prove quite challenging(Sulaiman & Arifudin, 2024). Hence, erratic supply of electrical power and unreliable internet connection, along with the use of personal devices for work purposes, might in many instances create a perception or typical ground for non-compliance despite the fact that the intent could be giving very best care. Informal sharing of information, which is quite common in some traditional African cultural systems, juxtaposes the EMR strict privacy protocol and would also result in a disconnect between perceived and real compliance (Simon & Aliferis, 2024). Employees tend to work around policies that they think comply but actually do not comply, because there is no clear guidance on culture-related issues or training.

In the Ashanti Region, Ghana, perceived compliance levels are influenced by several factors, including leadership commitment, peer behavior, and the presence of accountability measures. A positive organizational culture that emphasizes the importance of data privacy and routinely monitors compliance tends to result in higher levels of perceived and actual compliance(Li et al., 2022). On the other hand, in environments where privacy policies are seen as secondary to operational demands, compliance may be low, even if employees perceive themselves as adhering to the guidelines(Wong et al., 2020).

The concept of perceived compliance is also linked to employees' trust in the effectiveness of the EMR systems and the privacy policies themselves. Employees who believe that the system is secure and that the policies are practical and relevant are more likely to comply(Filippidou, 2020).However, if employees view the policies as overly

burdensome or if they believe that the EMR system is vulnerable to breaches, their commitment to compliance may wane(Roney et al., 2017).This suggests that fostering a culture of trust, transparency, and accountability is critical for improving both perceived and actual compliance levels. Moreover, feedback mechanisms play a vital role in shaping perceived compliance. Regular audits, performance reviews, and feedback sessions can help employees identify areas where they may be falling short and offer guidance on how to improve(Standards et al., 2020). In Ghana, the implementation of feedback systems is often inconsistent, with some facilities conducting regular reviews while others only assess compliance during crises, such as after a data breach. Establishing a continuous loop of feedback and monitoring can significantly enhance both perceived and actual compliance.

2.5.1 Gaps relevant to the Ashanti Region, Ghana

In the Ashanti Region of Ghana, no acceptance or adherence studies have been conducted to assess the employees' perception of compliance with EMR privacy policies. This gaping hole requires a consider, as getting to know employees' perceptions would largely help in identifying instances whereby policies may be vague, training may be lacking, or where systemic elements may serve as barriers against compliance. Specific gaps for the Ashanti Region include:

Quantitative assessment of perceived compliance rates among various cadres of health care workers and Investigation into the influence of organizational culture and leadership on employees' perceived compliance. Understanding these is crucial for designing targeted interventions, whether clearer communication of policies, better training, or redesigning or reworking aspects the EMR system. This will close the gap between perceived compliance and real compliance.

2.6 Factors Affecting Compliance with EMR Privacy Policies

Globally, literature identifies the factors that influence healthcare practitioners' adherence to EMR privacy policies. These real factors may be broadly classified as individual attitudes, organizational culture, leadership commitment, and the availability of resources.

2.6.1 Individual Factors

Individual factors such as employee attitudes, knowledge, and personal values play a significant role in compliance behavior(Taherdoost, 2019).Employees who prioritize data privacy and recognize its importance are more likely to adhere to EMR privacy guidelines. However, knowledge gaps, misunderstandings, and misconceptions about privacy policies can lead to unintentional non-compliance. Resistance to change is another critical factor; employees who are resistant to new policies or who find them inconvenient may deliberately or inadvertently ignore them(Stephenson, 2021).

Research indicates that the attitudes of employees toward data privacy are shaped by their understanding of the potential consequences of breaches. Employees who are aware of the legal, professional, and reputational risks associated with non-compliance tend to be more diligent in following privacy protocols(Williamson & Prybutok, 2024).Conversely, employees who view privacy policies as bureaucratic or irrelevant may disregard them, especially in high-pressure environments where time and efficiency are prioritized over strict adherence to privacy guidelines(Janett & Yeracaris, 2020).

Furthermore, according to Kadgi and Sarma (2002), high patient loads and time constraints can lead to shortcuts or inadvertent privacy breaches such as leaving a computer unlocked a, not fully logging out and also employee’s belief in their ability to

comply with policies, often linked to adequate training and support, influences their willingness to adhere.

2.6.2 Organizational Factors

The organizational environment is a crucial determinant of compliance. Leadership plays a pivotal role in setting the tone for compliance and fostering a culture of accountability and responsibility (Harrison & Ramanujan, 2011). In organizations where leadership actively promotes data privacy, provides the necessary resources, and monitors adherence to policies, compliance levels are generally higher(Taherdoost, 2019). On the other hand, in settings where privacy policies are not emphasized, employees may not feel compelled to comply, leading to frequent breaches.

The availability of resources, including adequate staffing, up-to-date technology, and access to training, also significantly impacts compliance. Under-resourced environments where employees are overstretched or lack the necessary tools to securely manage patient data often experience lower compliance levels (Standards et al., 2020). In the Ashanti Region, resource constraints are a common challenge, with some healthcare facilities struggling to provide the infrastructure and support needed to enforce privacy policies effectively(Mitchell & Kan, 2019).

Moreover, organizational culture influences compliance behavior. A culture that values transparency, ethics, and accountability encourage employees to adhere to privacy policies. In contrast, a culture where shortcuts are tolerated, and breaches go unpunished, creates an environment where non-compliance becomes normalized. Promoting a positive organizational culture requires consistent leadership commitment, regular

training, and the establishment of clear incentives and consequences for compliance and non-compliance, respectively.

2.6.3 Policy Complexity

The complexity of privacy policies can either facilitate or hinder compliance. Policies that are clear, concise, and easy to understand are more likely to be followed by employees than those that are ambiguous, overly detailed, or filled with technical jargon (Mubarkoot et al., 2023) . In many healthcare facilities in Ghana, privacy policies are often lengthy and filled with complex legal language, making it difficult for employees to fully grasp the requirements.(Shahnaz et al., 2019). Simplifying policy documents and ensuring they are accessible and user-friendly can enhance compliance. Policy complexity is particularly challenging in high-stress environments where healthcare workers need to make quick decisions. Lengthy protocols or unclear guidelines can lead to confusion, resulting in employees either ignoring the policies or following incorrect procedures (Bervell & Al-Samarraie, 2019). Therefore, privacy policies must be designed to be practical and aligned with the realities of the healthcare environment.

2.6.4 Technological Factors

The usability and reliability of the EMR system itself are crucial for ensuring compliance. Systems that are user-friendly, efficient, and incorporate automated privacy features reduce the burden on employees and make it easier to follow privacy guidelines.(Bisrat et al., 2021). Conversely, outdated systems, frequent technical issues, or interfaces that are difficult to navigate can lead to frustration, causing employees to bypass security measures to save time or reduce operational burdens(da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, 2020).

While many global factors apply to Africa, they are either exaggerated or diluted by the socio-economic, infrastructural, and cultural realities present.

Infrastructural Weaknesses: Variability in internet service, power supply interruptions, and a lack of software and hardware for upholding current EMR privacy laws have greatly compromised the ability to be compliant. Staff may find it difficult to access the EMR and end up either using insecure alternative methods or this wears down their morale to comply (Olusanya & Adeoye, 2019).

Training Resources: Due to budgetary constraints, training sessions on privacy are not only few and far between, but they may not always focus on the real-life application of those policies with regard to the local context (Maseko & Shonhe, 2018).

Workload and Understaffing: High staff-to-patient ratios are prevalent in many health facilities across Africa, which increases the workload and may cause health professionals to shortcut privacy at times (Ambe & O'Mahony, 2015).

Cultural Issues: In some traditional settings, privacy with regard to health information may be construed differently or may find itself competing with stronger family-community expectations of sharing information thereby conflicting with Western-oriented interpretations of privacy (Adewuyi & Olaleye, 2018).

Informal Practices: Where informal channels of communication such as WhatsApp for patient discussion become a way of doing things, it constitutes serious privacy breach which may be neither recognised nor viewed with great concern (Uwaezuoke et al., 2020).

Poorly Developed Legal Frameworks and Enforcement: A good number of African countries are formulating laws on the protection of data, but the enforcement thereof has been perceived as slow. This gives the employees little incentive to worry about the consequences of not complying (Muturi, 2017).

In Ghana, many healthcare facilities face challenges related to the technological infrastructure required to support effective EMR privacy management (Shahnaz et al., 2019). Issues such as limited internet connectivity, frequent power outages, and inadequate IT support can disrupt the use of EMR systems and lead to breaches of privacy. Investing in reliable technology and providing adequate support and maintenance are essential for creating an environment where compliance is not only possible but seamless.

2.7 Challenges to Compliance with EMR Privacy Policies

Despite the importance of compliance, employees face several barriers that hinder their ability to adhere to privacy policies effectively. These barriers can be grouped into operational, technological, and human factors.

2.7.1 Operational Barriers

Operational barriers such as high workloads, time constraints, and staff shortages are prevalent in many healthcare settings, including those in the Ashanti Region(Stephenson, 2021). In such environments, employees often prioritize immediate patient care needs over strictly adhering to privacy protocols. For instance, during emergencies or peak times, healthcare workers might share login credentials, leave workstations unattended, or skip security steps to save time, all of which compromise data privacy (Roney et al., 2017).

Operational challenges are exacerbated by inadequate staffing and resource constraints. In under-resourced facilities, employees may be required to multitask, leading to lapses in compliance as they juggle multiple responsibilities. Overburdened staff are more likely to overlook privacy guidelines, especially when they are under pressure to meet urgent care demands (Stephenson, 2021).

2.7.2 Technological Barriers

Technological barriers, including outdated or inefficient EMR systems, also contribute to non-compliance. In many Ghanaian healthcare facilities, the lack of reliable technology infrastructure is a major obstacle. Issues such as slow system performance, frequent downtimes, and inadequate user interfaces can frustrate employees and lead them to bypass privacy control (Filippidou,2020). Additionally, inadequate training on how to use EMR systems effectively can result in employees making mistakes or taking shortcuts that compromise patient data.

In the Ashanti Region, the technological infrastructure in many healthcare facilities remains underdeveloped, with some facilities still relying on hybrid systems that combine both electronic and paper-based records (Essuman et al., 2020). This fragmented approach makes it difficult to enforce consistent privacy protocols and increases the risk of data breaches. Upgrading technology, ensuring seamless integration of EMR systems, and providing continuous technical support are critical for overcoming these barriers.

2.7.3 Human Factors

Human factors such as resistance to change, lack of motivation, and poor understanding of privacy policies are significant barriers to compliance. Employees who are resistant to

new procedures may view privacy policies as cumbersome and unnecessary, leading to deliberate non-compliance (Standards et al., 2020). Additionally, employees who are not properly educated about the importance of privacy policies may not fully grasp the risks associated with non-compliance, resulting in complacency (Roney et al., 2017).

In many cases, the absence of strong incentives or consequences for compliance and non-compliance contributes to lax behaviour (Taherdoost, 2019). In Ghanaian healthcare facilities, inconsistent enforcement of privacy policies and a lack of accountability often lead to a culture where privacy breaches are tolerated or overlooked. To address these human factors, healthcare institutions must prioritize continuous education, promote a culture of compliance, and establish clear consequences for breaches (Standards et al., 2020).

2.8 Strategies for Enhancing Compliance with EMR Privacy Policies

Given the barriers identified, several strategies can be employed to enhance compliance with EMR privacy policies:

Regular Training and Continuous Education: Training should be an ongoing process that equips employees with up-to-date knowledge and practical skills for managing patient data securely. Regular refresher courses, interactive workshops, and real-life case studies can keep employees informed and reinforce the importance of privacy policies (Williamson & Prybutok, 2024).

Simplifying Policy Documents: Privacy policies should be clear, concise, and accessible. Reducing jargon and providing practical examples can help employees better understand what is required of them. (Janett & Yeracaris, 2020). Ensuring that policies are aligned with the realities of the healthcare environment can make them easier to follow.

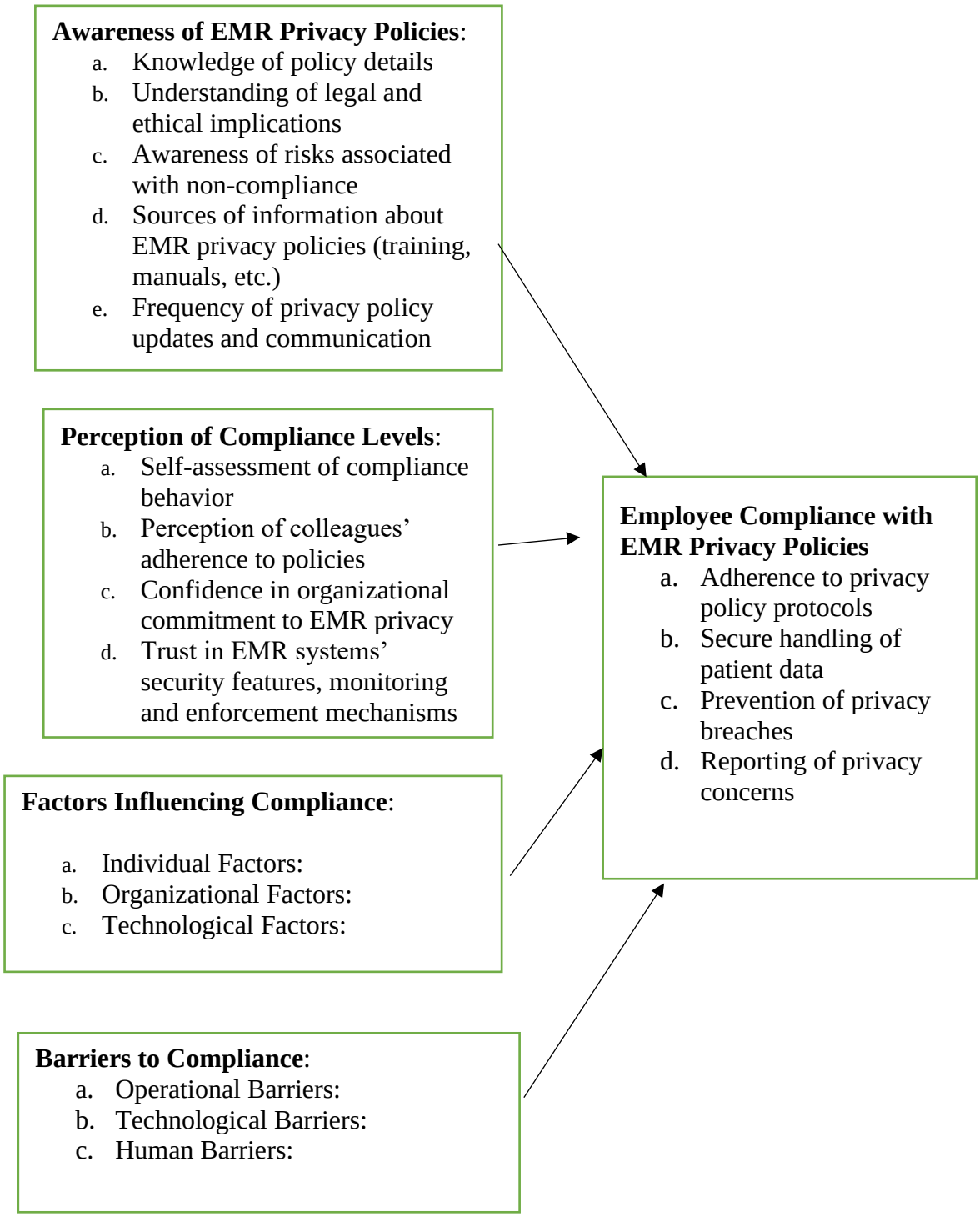
Leadership Involvement and Support: Leaders play a critical role in promoting a culture of compliance. By visibly supporting data privacy initiatives, providing the necessary resources, and holding employees accountable, leaders can foster an environment where compliance is the norm (Harrison & Ramanujan, 2011)

Improving Technological Infrastructure: Investing in secure, user-friendly EMR systems with automated privacy controls can reduce the burden on employees and make compliance easier(Tahir et al., 2020). Ensuring that systems are regularly updated and that employees receive adequate training on how to use them is also crucial.

Monitoring and Feedback Mechanisms: Regular audits, compliance checks, and providing feedback can help identify gaps and areas for improvement. Employees should be encouraged to report potential breaches or issues without fear of retribution (Dong et al., 2021).A continuous loop of monitoring and feedback ensures that compliance is maintained over time.

2.9 Conceptual Framework for the Study:

Perspective of Employees' Compliance with Electronic Medical Records Privacy Policy in the Ashanti Region.



2.10 Perspective of Employees' Compliance with Electronic Medical Records Privacy Policy in the Ashanti Region

This section presents the primary outcome variable of interest for this study, which is the extent to which employees within the Ashanti Region conform to set Electronic Medical

Records (EMR) privacy policies. Understanding employee compliance from different angles is an important aspect of protecting the confidentiality, integrity, and availability of patient data within the healthcare sector.

2.10.1 Dependent Variable

The dependent variable here is Employee Compliance with EMR Privacy Policies. It covers outcomes being investigated on the measure in which healthcare employees perform practices under supervision with respect to the privacy roles, guidelines, and protocols governing the access, use, storage, and sharing of Electronic Medical Records in their everyday professional practices. Effective compliance is paramount for the protection of patients' confidentiality, public trust, and both legal and ethical standards in care. To look broadly about this dependent variable, the study assesses the employee compliance for the following key aspects:

A. Adhering to Policy Protocols: This dimension evaluates how employees uniformly adhere to and accurately follow particular steps, procedures, and rules delineated in the EMR privacy policies. It investigates if employees agree with the regulated protocols concerning data entry, retrieving, sharing, storing, minimizing deviation from definition protocols.

B. Secure Data Handling Practices: This indicator assesses the methods and behaviors employees utilize to protect patient data from unauthorized access, modification, or disclosure, including but not limited to appropriate utilization of access control; proper management of strong passwords; the use of secure data transport protocols; and proper disposal of confidential data.

C. Effectiveness in Breach Prevention: This dimension measures the proactive or reactive nature of employees in preventing privacy breaches. It appraises the individuals' awareness and utilization of measures through which unauthorized disclosure, data loss, or system compromise could be avoided to protect the confidentiality of patient information.

D. Reporting Privacy Concerns and Incidents: This measures the willingness and diligence of employees to report actual or potential privacy breaches, security incidents, or vulnerabilities in the context of EMRs as well as the documentation surrounding them. On an added note, it reflects a culture that encourages transparency and proactiveness with risk management in privacy protection.

2.10.2 Independent Variables

This represents factors that either promote or inhibit compliance with Electronic Medical Records (EMR) privacy policies. They explain why employees may comply or fail to comply with established privacy protocols.

1. Awareness of EMR Privacy Policies

This variable addresses the level of employee knowledge about EMR privacy policies and their significance. Items under this variable include:

a. Existence of Policies: Do employees know that EMR privacy policies exist within their organization? Awareness of the mere existence of policies is the first step toward compliance.

b. Understanding of Policy Details: It measures how well employees comprehend the specific guidelines set by the organization, such as who can access patient data and under what circumstances.
c. Legal and Ethical Obligations: Employees should be aware that non-compliance can result in legal penalties and harm to the organization's reputation. They need to understand both the ethical responsibility to protect patient information and the legal consequences of breaches.
d. Risks of Non-Compliance: Employees should recognize the risks of non-compliance, including data breaches, fines, or disciplinary actions. This also includes understanding the potential harm to patients if their data is mishandled.
e. Source of Information: Where do employees get information about privacy policies? Are there regular training sessions, emails, or workshops that update employees about these policies?

2. Perception of Compliance Levels:

This variable measures how employees view their own and others' compliance with EMR privacy policies. It includes:

a. Self-Assessment: Do employees believe that they personally comply with the privacy policies? This self-assessment can be subjective, but it is essential because it shapes behaviour. Employees who think they are compliant may act more confidently but could overlook some policies.
b. Perception of Peers' Compliance: Employees often mirror the behaviour of their peers. If they see colleagues not following the privacy guidelines or bypassing security measures, they may do the same.
c. Organizational Compliance: This measures the perceived commitment of the healthcare facility as a whole to enforcing privacy policies. If employees believe

the organization is lax about compliance, they may not feel motivated to follow the rules themselves.

d. Trust in EMR Systems: Employees' confidence in the EMR system's security and privacy features impacts their compliance. If they feel that the system is unreliable or easily breached, they may not take privacy seriously.
e. Monitoring and Enforcement: This assesses whether employees believe that compliance is monitored through audits or system checks. If they think that violations go unnoticed or unpunished, compliance may decrease.

3. Factors Influencing Compliance:

These include both internal (individual) and external (organizational and technological) elements that affect how well employees follow privacy guidelines.

a. Individual Factors:

Attitudes Toward Data Privacy: Employees with positive attitudes toward data protection are more likely to follow privacy policies diligently. Those who see privacy as a bureaucratic burden may not comply. Resistance to Change: Employees who resist new technologies or policies may not comply with privacy guidelines, especially if they perceive them as complicated or time-consuming.

Personal Values: Some employees may place high value on patient confidentiality and act in ways that prioritize data protection. Conversely, if data privacy is not personally valued, compliance may be lower. Knowledge and Skills: Employees who understand how EMR systems work and how to securely manage patient data are more likely to follow privacy policies. Lack of knowledge or skill can lead to unintentional breaches.

b. Organizational Factors:

Leadership Support: Strong leadership that prioritizes data security and sets clear expectations for compliance can drive employee adherence. Employees look to leaders to see how important privacy policies are to the organization.

Resource Availability: Adequate staffing levels and access to the right tools and technology help employees comply with privacy policies. Understaffed or under-resourced facilities may see higher rates of non-compliance due to operational pressures.

Training: Regular and comprehensive training ensures employees are updated on privacy policies and how to comply with them. Training should also address new challenges or updates to EMR systems.

Organizational Culture: A workplace culture that values transparency, accountability, and ethical data handling promotes compliance. On the other hand, if shortcuts and breaches are tolerated, non-compliance becomes normalized.

c. Technological Factors:

Usability of EMR Systems: The more user-friendly an EMR system is, the easier it will be for employees to follow privacy guidelines. Complex systems can lead to frustration and the temptation to bypass security measures. Technical Support: Quick access to technical help is essential when systems fail or employees face challenges in using them securely.

System Security Features: Effective security features, such as strong passwords, authentication protocols, and encryption, help prevent data breaches. However, overly complex security measures may frustrate employees, leading to non-compliance.

Up-to-Date Technology: Outdated EMR systems can lead to inefficiencies, causing employees to take shortcuts that could compromise privacy.

d. Barriers to Compliance:

These are the obstacles employees face when trying to follow EMR privacy policies. They fall into three categories:

- **Operational Barriers:**

High Workloads: When employees are overwhelmed with work, they may prioritize efficiency over privacy, leading to shortcuts like sharing passwords or leaving workstations unattended.

Time Constraints: In time-pressured situations, especially emergencies, employees may skip privacy protocols to focus on patient care.

Staff Shortages: When facilities are understaffed, employees are stretched thin, leading to a lack of focus on compliance.

- **Technological Barriers:**

System Downtimes: Frequent downtimes or slow performance of EMR systems frustrate employees and lead them to bypass privacy protocols to get their work done.

Outdated Technology: If systems are outdated, they may lack critical security features, making compliance more difficult or ineffective.

Hybrid Systems: In some facilities, employees use both paper-based and electronic systems, which complicate privacy protocols and increase the risk of breaches.

- **Human Barriers:**

Resistance to Change: Employees who resist new EMR systems or privacy policies may avoid or neglect compliance.

Lack of Motivation: If employees do not see the value of following privacy policies or do not face consequences for violations, they may not prioritize compliance.

Insufficient Knowledge: Employees who are not trained or updated on new policies or technologies may unintentionally violate privacy rules.

2.10.3 Relationships between independent and dependent variables

The arrows in the diagram represent the influence of each independent variable on the dependent variable. They demonstrate that: Higher Awareness leads to better compliance, as employees are more informed and conscious of the policies. Moreover, Positive Perception of Compliance Levels within the organization fosters an environment where adherence to privacy policies is the norm.

Favorable Individual, Organizational, and Technological Factors increase the likelihood of compliance. Barriers such as operational pressures, technical challenges, and human resistance reduce the chances of employees complying with privacy policies. This conceptual framework explains the relationships between the factors that influence employee compliance with EMR privacy policies. By understanding how awareness, perception, individual and organizational factors, and barriers interact, the study can identify key areas for intervention to improve compliance and enhance the security of patient data in healthcare facilities.

2.11 Chapter Summary

The chapter explores a much deeper review of Electronic Medical Record (EMR) privacy laws with respect to the understanding of the new phase of health care involving close attention paid to the way patients share their data with their health providers and the

necessity of closely incorporating those privacy laws into EMRs. Without such privacy laws, it would be difficult to maintain the patient trust necessary to satisfy legal and ethical standards or ensure that the confidentiality, security, and integrity of data are addressed. Apart from comparative advantages such as increased efficiency, effective management of healthcare records, and an improved delivery of health services, EMR systems have some identified drawbacks, one of which includes cyber threats, data breaches, and user-related issues such as lack of awareness and resistance to change. The review shows how compliance with EMR privacy policy is influenced by many factors, such as the commitment of an organization towards it, technological infrastructure at its disposal, training of the workforce, leadership support, and an organizational culture related to it. Theories like the Theory of Planned Behaviour and Technology Acceptance Model (TAM) are discussed to explain health workers' compliance behaviour. The literature also emphasizes the disparity between developed and developing countries, where restrictions on resources greatly limit the implementation and compliance with privacy standards. Closing the chapter, compliance improvement efforts with EMR privacy policies in low-resource contexts, such as Ghana, would be recommended for context-specific strategies, especially those using combinations of policy reforms, continuous training, leadership engagement, and technological upgrades.

2.11.1 Gaps in literature

The literature review under consideration specifies many visible gaps in the existing studies on employee compliance to EMR privacy policies in the context of the Ashanti Region of Ghana. The first gap indicated here is the absence of empirical studies regarding healthcare employees' awareness levels concerning EMR privacy policies in this region. Although there are generalizations of health information systems, there is no

detailed data on how much employees know regarding privacy policies, from where they can get such information, or how such information would help them understand particular provisions of the policy better.

Moreover, little research has paid attention to the perceived compliance of employees - how they self-evaluate their adherence and how organizational and technological factors influence these perceptions. This is important: according to perceptions, behaviors are generally influenced, and very few studies analyze such connection in low-resource settings.

Also, the evaluation of training and communication strategies is a critical gap. Education is continuous for consistent compliance, but little is known about the effectiveness of current training programs, their frequency, relevance, or practicality in the Ghanaian healthcare context. Furthermore, much more needs to be understood regarding how modes of communication affect privacy policies awareness and adherence.

Furthermore, studies on how the size of the facility, availability of resources, and maturity of the EMR system are related to awareness as well as compliance behavior of employees in the Ashanti region are scarce.

In a nutshell, salient gaps revolve around a limited evidence base on awareness, perceptions, and training effectiveness, along with scant insights into systemic and contextual barriers to compliance. Addressing these gaps through carefully targeted research would prove pivotal in the design of effective interventions to improve EMR privacy compliance within the Ghanaian health sector.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter discusses the research methodology employed for the study titled "Perspective of Employees' Compliance with Electronic Medical Records Privacy Policy in Ashanti Region." The methodology is structured to align with the research objectives, providing detailed descriptions of the research design, study area, population, sampling techniques, data collection methods, data analysis, ethical considerations, and study limitations. These methodological strategies aim to provide a comprehensive framework for understanding the factors influencing employees' compliance with EMR privacy policies in the selected health facilities within the Ashanti Region.

3.2 Research Design

The study adopts a cross-sectional design. In this study, the cross-sectional design helps in capturing the existing perceptions, awareness, and compliance behaviours of healthcare employees regarding EMR privacy policies. The cross-sectional aspect involves collecting data at a single point in time, allowing for a snapshot analysis of the variables related to compliance within the selected healthcare facilities. This design is ideal for analyzing relationships between awareness, perception, and compliance factors without manipulating the environment.(Lee et al., 2020).

3.3 Study Area

The study was conducted in three public healthcare facilities located in the Ashanti Region of Ghana: Mampong Government Hospital, Agona Government Hospital, and Ejura Government Hospital. The Ashanti Region is one of the most populous regions in

Ghana. It serves as a central hub for healthcare delivery, with numerous healthcare institutions adopting electronic medical records (EMR) systems. The study sites were strategically selected due to their simultaneous adoption of EMR systems and the diversity in their service delivery, staffing levels, and patient populations. Understanding compliance within these hospitals provides valuable insights into the broader regional dynamics affecting EMR privacy. These facilities were chosen not only for their geographical location within the Ashanti Region but also for their diversity in patient load, healthcare delivery, and administrative structure, which were all divided from the then Sekyere West District. This diversity provides a comprehensive view of the factors influencing compliance with privacy policies across various healthcare settings within the region.

1. Mampong Government Hospital: Situated in the Mampong Municipality, this hospital is a key health service provider for the surrounding communities, offering a range of healthcare services. It has a total staff population of 268 employees, encompassing doctors, nurses, medical records officers, administrative staff, and other healthcare professionals. The hospital serves as a referral centre and plays a vital role in the municipality's health delivery system.
2. Agona Government Hospital: Located in the Sekyere South District, Agona Government Hospital serves as the primary healthcare facility for residents in Agona and its environs. With a staff of 189 employees, the hospital offers a comprehensive range of medical services, including primary care, maternal health, and emergency care. The hospital’s adoption of EMR systems has made it a critical site for examining compliance behaviours related to data privacy.

   3. Ejura Government Hospital: Positioned in the Ejura-Sekyedumase District, Ejura Government Hospital caters to a population spread across multiple

communities and serves as a referral centre for smaller healthcare facilities in the district. With a staff population of 250 employees, the hospital is an important case study for understanding how varying resource levels and staff sizes influence compliance with EMR privacy policies.

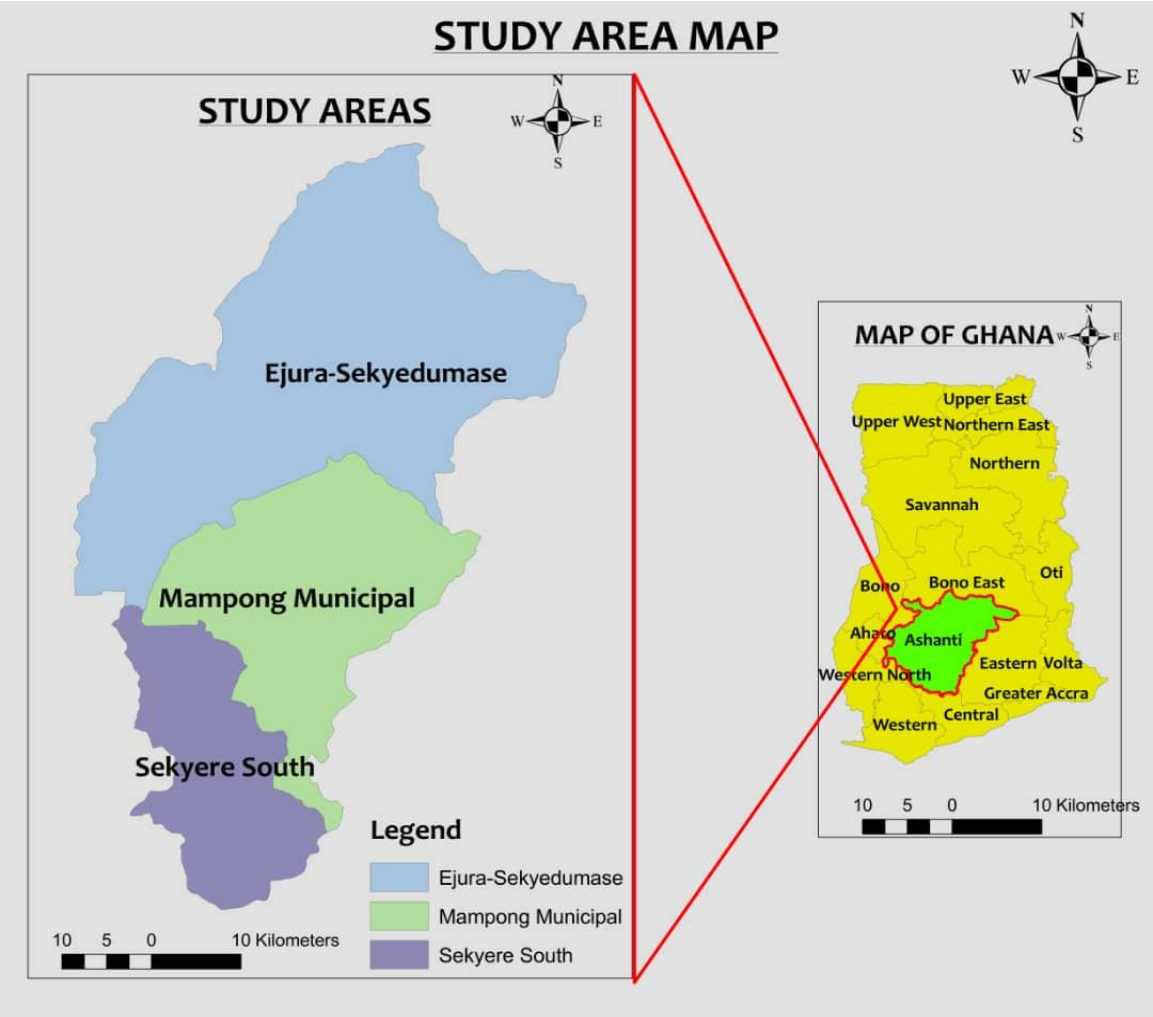


Figure 3.1: Map of the Study Area

Constructed by author, 2024.

3.3 Study Population

The study population includes all staff involved in the handling and management of electronic medical records in the three selected hospitals: Mampong Government

Hospital, Agona Government Hospital, and Ejura Government Hospital. This includes a wide range of professionals such as doctors, nurses, medical records officers, IT personnel, and administrative staff. Each category of staff interacts with the EMR systems at various levels, and their perspectives on compliance are crucial for understanding the factors that influence privacy behaviours.

Table 3.1 Staff population across the three hospitals

Name of hospital	Number of employees
Mampong Government Hospital	238
Agona Government Hospital	179
Ejura Government Hospital	196

The combined total population is 613 employees. Given that each category of healthcare professional plays a distinct role in data management and privacy, the study aims to capture a representative sample from each category to provide a comprehensive view of compliance issues.

3.4 Sampling

A multi-stage sampling method was used for achieving a representative selection of study participants across the three target health facilities in the Ashanti Region. First, the population was stratified along the lines of job roles such as doctors, nurses, medical records officers, IT personnel, and administrative staff. This was necessary to induce representation for any variation in perspective and interaction with the EMR system by different categories of health workers. Simple random sampling was then employed within each stratum to select individual respondents, as it affords equal chance to all and minimizes selection bias. The sample size was calculated using Yamane's formula,

factoring the total population of 613 health professionals across the three hospitals, with a 10% allowance for non-response, and arriving at a target sample of 269 participants. This sampling design guarantees representativeness and generalizability of the findings to the larger population of healthcare workers who are engaged in EMR management within the region.

3.4.1 Sampling Techniques

The study used multi-stage sampling in the selection of respondents for the survey. For example, in the first stage, the population was stratified according to job roles into doctors, nurses, medical records officers, IT personnel, and administrative staff to ensure that no professional category was significantly over-represented or under-represented. Such stratification was done to capture the variation in experiences and views regarding EMR privacy policies. The second stage involved simple random sampling within strata where individual respondents were selected at random to ensure inclusion. This provided every single person within that stratum with equal chances of being included thereby reducing bias and increasing the representation of the sample. Thus, the combined processes of stratification followed by randomization ensured that one has a fair and unbiased sample quite representative of the distribution of staff involvement in EMR systems spread through the sampled hospitals.

3.4.2 Sample Size Estimation

The sample size was determined using Yamane's (1967) formula for calculating sample size from a finite population:

$$n = \frac{N}{1 + Ne^2}$$

Where n *is* the sample size to be determined N = the population frame of health professionals from the three selected government hospitals and e= the precision term or margin of error (0.05). Therefore:

$$n = \frac{613}{1+613(0.05)^2} = 242$$

However, adjust for a 10% Non-Response Rate.

Adjusted sample size =

$$\frac{Desired\ sample\ size}{1 - Expected\ Non\ Response\ Rate}$$

non-response rate =10% it means 1 - 0.10 = 0.90

So Adjusted sample size = $n = \frac{242}{0.90} = 269$

Therefore, 269 health professionals were sampled from the three health facilities in the region. Proportional allocation to each hospital

Mampong = $\frac{238}{613} x269$ =104

Agona = $\frac{179}{613} x269$ = 79

Ejura = $\frac{196}{613} x269$ = 86

Table 3. 2 Proportional allocations to each hospital

Hospital	Population	Proportional sample
Mampong Govt Hospital	238	104
Agona Govt Hospital	179	79
Ejura Govt Hospital	196	86

3.5 Data Collection Methods

This study's data collection adopted structured questionnaires to gather quantitative data on compliance with EMR privacy policies by health professionals in the Ashanti Region. The questionnaires sought to encompass various domains, inclusive of demographic details, awareness levels, perceptions, and factors affecting compliance with EMR privacy policies.

The questionnaires contained five principal sections: one referring to demographic data, another to awareness of EMR privacy issues (including sources of knowledge), one for perceptions regarding compliance levels, one about organizational and individual factors affecting compliance, and finally, one on the operational barriers faced by health workers. The questions included closed-ended options and Likert-scale statements that respondents used to denote their degree of agreement/frequency of behaviors.

Data collection was carried out over four weeks with an online structured questionnaire on Google Forms. This way, the selected hospital staff members could easily access it through the hospital administrators, who were fully briefed on the objectives of the study and asked to disseminate the link to the staff in their network. The responses were captured automatically in real-time, securely stored on the Google Forms platform, and accessible only to the researcher through password protection. This method promoted wide reach, low-cost engagement, and convenience to the respondents while ensuring the high fidelity of the proceedings and the integrity of the data collected.

3.6 Data Collection Tools

Structured questionnaires were designed to capture quantitative data. The questionnaire was divided into five key sections, each focusing on different aspects of compliance with EMR privacy policies: Section A: Demographic information (age, gender, educational level, years of experience, job role). Section B: Awareness of EMR privacy policies, including the extent of knowledge about policy details and sources of information.

Section C: Perceptions of compliance levels within the organization, including self-reported adherence and observed behaviours among colleagues. Section D: Factors influencing compliance, covering individual factors (attitudes, resistance to change), organizational factors (leadership support, resources, training), and technological factors (system usability, access to updated technology). Section E: Barriers to compliance, addressing operational challenges, technological limitations, and human factors.

The questionnaire was a mix of closed-ended and Likert-scale questions, allowing respondents to express the degree to which they agree or disagree with various statements related to compliance. The questionnaire was pre-tested at a different healthcare facility in the Ashanti Region to ensure clarity, validity, and reliability.

3.7 Data Collection Procedure

Data collection was conducted over a period of four weeks. Data for the study were collected using a structured questionnaire design and hosted on Google Forms. The use of Google Forms enabled easy distribution, real-time tracking, and data security during the collection process. The electronic link to the questionnaire was initially shared with selected hospitals. These administrators were briefed on the objectives of the study and requested to forward the questionnaire link to the official work platforms of their respective staff members, particularly those involved in handling electronic health

records. The responses were automatically captured and stored securely within the Google Forms platform, accessible only to the researcher using password-protected credentials. This method ensured wide reach cost-effectiveness, and convenience for respondents while maintaining data accuracy and integrity.

3.8 Data Management and Analysis

3.8.1 Data Management

The data management practices concerning this study aimed at establishing the safety, confidentiality, and integrity of the data collected. The data were gathered with structured questionnaires using Google Forms so that electronic collection of responses could be in real-time. However, they automatically store the collected responses in their platform, an environment that supports secure storage. Access to the data has also restricted to the researcher using password-protected credentials, thus preventing all potential unauthorized access and safeguarding sensitive information.

The data management process consisted of collating and classifying the responses according to questionnaire section demography, awareness levels, compliance perception, and adherence-influencing variables; it allowed for statistical analyses employing descriptive statistics and regression models. Confidentiality was ensured throughout data handling by presenting the descriptive results in aggregates such that anonymity of the participants was afforded.

Data security measures also included storing the data in password-protected and access-restricted devices for the authorized few. This was in line with ethical standards of managing confidential information, considering healthcare data related to patients and

staff. Thus, the above data management practice made data security, confidentiality, and accuracy propelling valid and reliable research outcomes.

3.8.2 Data Analysis

In this study, data analysis was multifaceted using descriptive and inferential methods to fulfill the research objectives on the awareness, perceptions, compliance levels, and influencing factors of health professionals concerning EMR privacy policies.

The first objective of the study sought to assess health professionals' awareness of the EMR privacy policy in the Ashanti Region. This objective was achieved using Fisher's Student T-test model. This approach enabled the researcher to estimate the mean differences among both the EMR complaints and non-complaints and help establish the significance level of awareness differences across the two groups. The variables were measured on a four-point Likert scale, ranging from very well informed, well informed, somewhat informed and not informed on the compliance of the privacy policies.

The second objective examined the perception of health workers on electronic medical record privacy policy compliance. This objective was achieved using the weighted average index model (WAI).

The model is specified as:

$$WAI = \sum \frac{S_i F_i}{N} \quad (1)$$

Where the WAI is ($0 \leq \text{WAI} \leq 1$), F_i is the frequency of response; S_i is the scale value assigned to i priority and N is the total number of responses. This statistical model enables scholars to measure the level of perception on a five-point scale with differences in weights (Ndamani and Watanabe, 2015; Gunawan et al., 2019). The accumulative

weight of the included variables ranged from 0-1. With 1 representing Very Strong (VS), 0.75 for "strong" (S), 0.5 for "medium" (M), 0.25 for "weak" (W) and 0 for very weak (VW).

Objective three explored the factors that influence the adoption of EMR privacy policy compliance among health professionals. This objective was achieved using logistic regression analysis. The model can be specified as:

$$Logit = \ln\left(\frac{p}{1-P}\right) = \alpha + \beta X \qquad (2)$$

Where P can mathematically be represented as:

$$=P = \frac{Exp(\alpha+\beta X)}{1+\exp(\alpha+\beta X)} \qquad (3)$$

Accordingly, the term on the right-hand side of the equation is the logistic function. The extension of the multiple models is obtained when we represent the βX with the linear combination of the independent variables to be estimated and their respective coefficients thus: $\beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \cdots B_m X_{m4} + \varepsilon$

Therefore, the model can mathematically be represented as:

$$\mathrm{Y}\left(\frac{p}{1-P}\right) = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \cdots B_m X_{m4} + \varepsilon$$

The fourth objective of the study also identified the challenges faced by health professionals in complying with the EMR privacy policies. This objective was achieved using Friedman's Test approach backed by the Kendall coefficient of concordance. The integration of the Kendall coefficient of concordance enabled the assessment of the level of agreement among the health professionals. In sum, Kendall's *W* was specified as:

$$\mathrm{W}=\frac{12[\sum_{T^2} - \frac{\sum T^2}{n}]}{nm^2(n^2-1)} \qquad \textbf{(4)}$$

Where *T*= Total weight score W= Kendall's coefficient of concordance

n= Number of constraints being ranked m = Number of respondents

Also, F – Distribution was utilized to test the significance of the coefficient of concordance.

Thus the F- ratio is specified as:

$$F - \text{Ratio} = \frac{[(m-1)WC]}{(1-WC} \quad (5)$$

Where Wc = Calculated Kendall's coefficient of concordance.

3.9 Ethical Considerations

Ethical approval for this study was obtained from the KNUST Committee on Human Research, Publication, and Ethics, following a support letter from the Ghana Health Service. Additionally, permission was obtained from the management of Mampong Government Hospital, Agona Government Hospital, and Ejura Government Hospital. The study adhered to the ethical principles of voluntary participation, informed consent, confidentiality, and anonymity. Participants are provided with an informed consent form that outlines the purpose of the study, their rights as participants, and assurances that their identity will be kept confidential. They were informed of their right to withdraw from the study at any point without any negative consequences. The data collected was securely stored in password-protected files, accessible only to the research team. The findings were reported in aggregate form to prevent the identification of individual respondents.

CHAPTER FOUR

RESULTS

4.1 Demographic Characteristics of Health Care Professionals

This section of the paper analyses the demographic characteristics of health professionals, the awareness level of healthcare electronic data privacy compliance, factors influencing health professionals to adopt EMR compliance policies, their perception of the privacy policy, and the challenges**.**

Table 4.1: Demographic characteristics

Variable	Frequency	Percentage
Gender		
Female	212	80.00
Male	53	20.00
Age		
Below 25	175	66.04
25-34	76	28.68
35-44	11	4.15
45-54	3	1.13
Education		
Certificate/Diploma	237	88.10
Bachelor	24	8.92
Masters	6	2.23
Doctorate	2	0.74
Job Position		
Doctor	4	1.51
Nurse	156	58.87
Medical Record	3	1.13
IT Personnel	8	3.02
Administration	14	5.28
Midwife	80	30.19
Years in Health Service		
Below 1year	125	47.17
1-5yr	127	47.92
6-10years	7	2.64
11-15years	5	1.89
16years and above	1	0.38

Table 4.1: Demographic characteristics (Con't)

Variable	Frequency	Percentage
Experience in EMR Usage		
Less than 1 year	148	55.85
1-5 years	108	40.75
6-10years	5	1.89
11-15years	4	1.51
Health Centres		
Mampong Hospital	102	37.92
Ejura Hospital	72	26.77
Agonal Hospital	95	35.32
EMR Privacy Policy Exposu		
Orientation/Onboarding Progr	110	41.51
Training Workshops/Seminars	72	27.17
Departmental Meetings	10	3.77
Internal Communications (e.g. Memos, Emails)	16	6.04
Through Colleagues	46	17.36
Hospital Noticeboards/Posters	11	4.15

Based on field data, 2023.

The demographic and professional characteristics of the respondents revealed distinct patterns across various variables. In terms of gender distribution, the data showed a predominantly female workforce, with 80% of respondents being female compared to 20% male. This aligns with the global and national trends where nursing and midwifery, which make up a large proportion of the healthcare sector, are primarily female-dominated professions.

When examining the age distribution, the majority of respondents were relatively young, with 66.04% being below 25 years, while 28.68% were between 25 and 34 years. Only a small proportion fell within the 35–44 years (4.15%) and 45–54 years (1.13%) categories. This trend indicates a youthful healthcare workforce, likely due to recent graduations and recruitment of younger professionals into the system. The presence of a younger workforce could have implications for adaptability to technological systems like

electronic medical records (EMRs), as younger employees often demonstrate higher technology acceptance. With regard to educational attainment, the analysis showed that most respondents held Certificate or Diploma qualifications (88.10%), while 8.92% had a Bachelor's degree. Advanced qualifications such as Master's (2.23%) and Doctorate degrees (0.74%) were very rare among participants. This pattern reflects a concentration of entry-level and mid-level professionals, suggesting limited postgraduate educational advancement among healthcare workers in the studied facilities.

Considering job positions, nurses formed the largest group (58.87%), followed by midwives (30.19%). Other categories such as administrative staff (5.28%), IT personnel (3.02%), medical record officers (1.13%), and doctors (1.51%) accounted for a small proportion of the sample. This distribution highlights that the study predominantly involved nursing and midwifery professionals, with minimal representation from other healthcare roles, which may influence perspectives on clinical systems like EMRs.

An analysis of years of service in the health sector showed that nearly equal proportions of respondents had less than one year (47.17%) and 1–5 years (47.92%) of work experience. A very small percentage reported longer service durations, including 6–10 years (2.64%), 11–15 years (1.89%), and 16 years and above (0.38%). These findings suggest a highly inexperienced workforce, with almost all respondents having less than five years of service. Such a trend could be attributed to recent recruitment drives or high turnover rates in the healthcare sector.

Regarding experience in EMR usage, more than half of the respondents (55.85%) had used the system for less than one year, while 40.75% had between 1–5 years of

experience. Only a small fraction had extensive experience, with 1.89% and 1.51% having used EMRs for 6–10 years and 11–15 years, respectively. This indicates that EMR implementation is relatively new in these health facilities, with the majority of staff still in the early stages of adoption.

The distribution by health centers showed that respondents were fairly represented across the three study sites, with Mampong Hospital contributing 37.92%, Agona Hospital 35.32%, and Ejura Hospital 26.77%. This balanced distribution enhances the generalizability of findings across the facilities studied.

Lastly, exposure to the EMR privacy policy primarily occurred through orientation or onboarding programs (41.51%) and training workshops/seminars (27.17%). Other channels included colleagues (17.36%), internal communications such as memos or emails (6.04%), noticeboards/posters (4.15%), and departmental meetings (3.77%). These results suggest that initial orientation programs serve as the dominant means of disseminating EMR privacy policy information, with minimal reinforcement through other continuous education platforms.

4.2 Awareness of Healthcare Workers

Table 4. 2, shows the statistical analysis of the awareness level of healthcare professionals on Electronic Medical Record compliance and policy in their various organizations. Per the initial assessment, the awareness and knowledge level of EMR policy compliance were rated on a four-point Likert scale, ranging from 1 being the highest and 4 being the lowest. Using Student t-test, we estimated the awareness level of health professionals, assessing the significance level of the mean differences between

both EMR complaints and non-complaints. The findings indicate a significant mean difference between the EMR-compliant and non-compliant on their awareness level of receiving frequent updates or reminders regarding the EMR privacy policies, with the compliant group exhibiting a higher level of awareness compared to the non-compliant of the EMR policy. The EMR policy complaints indicated that they have adequate knowledge of the content and guidelines within the EMR privacy policies compared to non-complaints, as evidenced by the significant mean differences. Similarly, there was a huge difference in the participation in training sessions purposely focused on EMR privacy policies, with EMR complaints exhibiting greater participation compared to the non-EMR complaints. The study also indicates that EMR complaints are highly aware that participation in EMR policy compliance training can contribute to improving health professionals' understanding compared to the non-complaints.

Table 4.2: Awareness of EMR privacy policy

	Variables	Non-Compliant Mean	SD	Complaint Mean	SD	T-statistics	Mean difference
1.	Frequent updates or reminders regarding the EMR privacy policies?	3.266	0.883	1.897	1.016	5.102	1.369***
2.	Adequate knowledge of the content and guidelines within the EMR privacy policies?	3.133	0.990	1.728	0.885	5.934	1.806***
3.	Training sessions specifically focused on EMR privacy policies in the last month	0.133	0.351	0.590	0.030	-3.538	-0.457***
4.	Training you attended effectively improved your understanding of EMR privacy policies.	3.466	0.990	2.291	1.251	3.568	2.356***

Based on field data, 2024.

From table 4. 2, the analysis of respondents' awareness of EMR privacy policies revealed significant differences between compliant and non-compliant groups across all measured variables. The first variable examined whether respondents received frequent updates or reminders regarding EMR privacy policies. The non-compliant group reported a higher mean score of 3.266 (SD = 0.883) compared to the compliant group with a mean of 1.897

(SD = 1.016). The calculated t-statistic of 5.102 and a mean difference of 1.369 ($p < 0.001$) indicate a significant disparity, suggesting that frequent reminders alone do not necessarily result in compliance, as non-compliant individuals reported more frequent updates.

The second variable assessed whether respondents believed they had adequate knowledge of the content and guidelines within EMR privacy policies. Again, the non-compliant group scored higher (Mean = 3.133, SD = 0.990) compared to the compliant group (Mean = 1.728, SD = 0.885). The t-statistic of 5.934 and a mean difference of 1.806 ($p < 0.001$) highlight a paradox where non-compliant individuals perceive themselves as knowledgeable yet still fail to comply. This suggests that perceived knowledge does not guarantee compliance, pointing to possible attitudinal or behavioral factors.

For the third variable, which asked if respondents had participated in any training sessions specifically focused on EMR privacy policies in the last month, the results showed an opposite trend. The compliant group reported higher participation (Mean = 0.590, SD = 0.030) compared to the non-compliant group (Mean = 0.133, SD = 0.351). The negative t-statistic (-3.538) and mean difference of -0.457 ($p < 0.001$) confirm that recent training participation strongly correlates with compliance, underlining the effectiveness of training programs in improving adherence.

The fourth variable explored whether respondents believed the training they attended effectively improved their understanding of EMR privacy policies. Non-compliant individuals reported a higher mean (3.466, SD = 0.990) compared to the compliant group (2.291, SD = 1.251), with a t-statistic of 3.568 and a mean difference of 2.356 ($p < 0.001$). This again suggests that self-reported perceptions of training impact do not necessarily translate into behavioral compliance

4.3 Determinants of Health Professionals' Compliance with The EMR Privacy Policy

An analysis of the factors that influence health workers' compliance with electronic medical record privacy policy has been presented in Table 4.3.

Table 4.3: Factors influencing health workers' compliance with the EMR Privacy Policy

Variables	Coefficient	Robust Standard Error	P>Z
Gender	0.905	1.268	0.475
Age group	-0.583	0.524	0.266
Education	1.565	1.011	0.122
Years of Experience (Health)	0.138	0.594	0.816
Years of Experience (EMR usage)	-0.209	0.840	0.803
Organizational Commitment	0.251	0.218	0.250
EMR Breach	1.713	0.677	0.011**
Organizational priority	2.019	0.813	0.013**
Regular training	0.256	0.299	0.392
User-Friendly	0.247	0.505	0.624
Leadership support	-0.806	0.392	0.040**
Organizational Communication	1.057	0.597	0.077*
Organizational-culture	-0.389	0.468	0.406
Cons	-2.175	1.701	0.201
Number of observations	265		
Wald chi2(13)	43.19		
Prob > chi2	0.000***		
Pseudo R2	0.2394		
Log pseudolikelihood	-43.841		

Note: ***=1%,**=5% and * = 10% ;

Based on field data, 2024.

From table 4. 3, the analysis of factors influencing health workers' compliance with the EMR privacy policy reveals varying degrees of influence among demographic, organizational, and system-related variables. The logistic regression model was statistically significant (Wald $chi^2 = 43.19$; Prob > $chi^2 = 0.000$), indicating that the selected predictors collectively explain a meaningful portion of the variation in

compliance behavior. The pseudo-R^2 value of 0.2394 suggests that approximately 24% of the variability in compliance is accounted for by these factors.

Among the variables examined, organizational priority, EMR breach experience, and leadership support emerged as the most influential predictors of compliance. Specifically, organizational priority exhibited the highest positive effect (Coefficient = 2.019, p = 0.013), implying that when compliance with EMR policies is emphasized as a key institutional priority, health workers are significantly more likely to adhere to privacy requirements. Similarly, the occurrence or awareness of an EMR breach was positively associated with compliance (Coefficient = 1.713, p = 0.011), suggesting that previous breaches may heighten awareness and encourage stricter adherence to privacy standards. In contrast, leadership support, though statistically significant (p = 0.040), showed a negative coefficient (-0.806). This counterintuitive finding may indicate that leadership interventions often occur in reactive contexts, such as after non-compliance issues arise, rather than as proactive measures that foster compliance. Furthermore, organizational communication demonstrated a marginally significant relationship (Coefficient = 1.057, p = 0.077), highlighting that effective communication channels within health facilities can moderately enhance compliance with EMR privacy policies.

4.4 Health Worker's Perception of the Compliance of the EMR Privacy Policy

Table 4.4 presents the results on the level of health professionals' perception of compliance with electronic medical record privacy policy. The weighted average index was computed and assigned to the individual variables. The interpretation of the scores has also been provided to aid the understanding of healthcare professionals' perception of EMR privacy policy.

Table 4.4: Perception of compliance of the EMR Privacy Policy

S/N	Variable	Weighted Averag Index	Interpretation
1.	Comply with the EMR privacy policies in our daily work the hospital	0.16	Weak
2	Our department and team frequently ensure that we comp with the EMR privacy policies	0.52	Moderate
3.	Logging out of the EMR system after use can ensure the privacy of health data	0.68	Strong
4.	Avoiding the sharing of login details can contribute to compliance with EMR privacy policy	0.74	Strongly
5.	Ensuring that screens are not visible to others can lead to EMR privacy policy compliance	0.63	Strongly
6.	Reporting suspicious activities or breaches can help stren EMR privacy policy compliance	0.64	Strongly
7.	Following established protocols for accessing records car encourage EMR privacy policy compliance	0.72	Strongly
8.	Enforcement on the part of management can ensure EMR privacy policies in our hospital	0.57	Moderate

Based on field data, 2024.

From Table 4.4 Perceptions of EMR privacy policy compliance varied across indicators. self-reported compliance in daily work was weak (WAI = 0.16), while departmental enforcement was rated moderate (WAI = 0.52). Conversely, specific behavioral practices

received strong endorsement. Avoiding login detail sharing (WAI = 0.74) and following access protocols (WAI = 0.72) were perceived as the most critical compliance measures. Similarly, logging out after use (0.68), reporting breaches (0.64), and ensuring screen confidentiality (0.63) were strongly associated with compliance. Management enforcement scored moderately (0.57), indicating gaps in institutional control. These findings suggest high awareness of individual actions but low overall compliance integration at organizational level.

4.5 Challenges of EMR Privacy Policy

The challenges faced by healthcare workers in complying with the EMR privacy policy are outlined in Table 4.5. The challenges were ranked from highly severe to less severe using Friedman's test. From the result, we found that the agreement level among the health professionals was moderately significant, consistent with Kendall's coefficient of concordance index score (0.357). The average score for each of the challenges was recorded and ranked according to their level of severity (x=2.7-3.62*)*. High workload and time constraints were rated as the most pressing challenges, followed by inadequate training and workshops, limited access to innovation technologies and resistance to change from colleagues. Complexity of the EMR privacy policy and lack of motivation or incentives were rated as less severe according to the result obtained in Table 4.5.

Table 4.5 Challenges Faced by Health professionals in complying with the EMR Privacy Policy

Challenges	Mean Scores	Ranking
High workload and time constraints	2.791	1st
Inadequate training and workshops	3.148	2nd
Limited access to new technologies	3.414	3rd
Resistance to change from colleagues	3.605	4th
Complexity of the EMR privacy policy	3.624	5th
Lack of motivation or incentives	3.624	5th
Friedman(X^2)	1700	
Kendall's W	0.357	
P-value	0.023**	

Based on field data, 2024.

The analysis of challenges experienced by health professionals in adhering to the EMR privacy policy highlights several key issues. Among the identified challenges, high workload and time constraints ranked first with a mean score of 2.791. This suggests that the pressure of clinical responsibilities significantly limits the ability of healthcare workers to comply with privacy regulations, indicating a major structural barrier.

The second-ranked challenge was inadequate training and workshops, which had a mean score of 3.148. This finding underscores the importance of continuous education and refresher training on EMR privacy requirements to enhance compliance among staff. The lack of adequate training opportunities suggests that compliance issues may stem from knowledge gaps rather than unwillingness.

Limited access to new technologies followed as the third-ranked challenge (mean = 3.414). This reflects infrastructural and resource-related constraints that hinder the full integration and use of EMR systems. Without proper technological support, adherence to privacy policies becomes difficult.

The challenges related to resistance to change from colleagues (mean = 3.605) were ranked fourth. This implies a degree of cultural or behavioral reluctance to adopt new procedures, which could result from fear of increased workload or lack of perceived benefits.

Interestingly, the complexity of the EMR privacy policy and lack of motivation or incentives were tied for the fifth position, each with a mean score of 3.624. This suggests that both policy design and motivational factors equally contribute to the difficulty in achieving compliance. The complexity of regulations may create confusion, while the absence of incentives reduces the perceived value of compliance.

The Friedman test statistic ($\chi^2 = 1700$, $p = 0.023$) indicates a statistically significant difference in the rankings of these challenges. Moreover, Kendall's coefficient of concordance ($W = 0.357$) shows a moderate level of agreement among respondents regarding these challenges, affirming the reliability of the observed patterns

CHAPTER FIVE

DISCUSSIONS

5.1 Demographic Characteristics of Health Workers

Table 1 presents the results of an analysis of the respondents' demographic characteristics. According to the survey's findings, women employees made up the majority of respondents roughly 80% while men made up only 20%. The bulk of healthcare professionals (66.04%) were under 25, with those between the ages of 25 and 34 coming in the second position. This outcome is in line with the findings of Osei et al. (2020), who also discovered that people in their younger years make up the majority of healthcare professionals in the Ashanti region. We discovered that most health personnel have a certificate or diploma as their highest level of education (88.10%). This is also followed by individuals' health professions with bachelor's degrees (8.92%). With a percentage score of 58.87%, nursing claimed the top spot in the region's various healthcare facilities, followed by midwives (30.19%); this pattern is consistent with the findings of Dassah et al. (2023) and Osei et al. (2021).

The health professionals who have been in the health sector for about 1-5 years (47.92%) constituted the majority, followed by individuals with less than 1 year of service experience. Surprisingly, the findings revealed that health professionals who have used the EMR system for less than a year formed the largest percentage share of the population (55.85%) followed by 40.75% of the health professionals who have used the EMR for close to 5 years. The result can be explained that despite the EMR systems being predominant in health facilities in the Ashanti Region, their adoption and implementation have been a new subject in the sector. Additionally, the study also found that health workers in the Mampong and Ejura government hospitals formed a greater portion of the

survey, constituting about 38% and 35% respectively (Figure 1). Also, the results indicate that employee orientation and onboarding programme were the major means through which health professionals become highly aware of the EMR privacy policy exposure (41.51%), followed by training workshops and seminars (27.17%), through colleagues and departmental meetings (3.77%). This is because different directors or heads of health institutions arrange special orientation and training programs for newly hired staff members, allowing them to comprehend the notion of EMR privacy regulations and their significance in incorporating them into their operations. According to Otto (2013) and Alharbi (2023) offering special orientation and training to health professionals on EMR intensifies its adoption and awareness of the privacy policies concerning its usage

5.2 Awareness of EMR Privacy Policy Among Health Workers

This section presents the analysis of awareness of the EMR privacy policy as captured in Table 4.2. The result in Table 4.2, indicates that 94.34% of the health care professionals are aware of and comply with the Electronic Medical Records Privacy Policy in their hospital. The findings indicate a significant mean difference between the EMR-compliant and non-compliant on their awareness level of receiving frequent updates or reminders regarding the EMR privacy policies, with the compliant group exhibiting a higher level of awareness compared to the non-compliant of the EMR policy. This can be explained that the medical facilities consistently keep their staff members up to date regularly to avoid compromising the confidentiality of the information gathered about the health behaviours of their patients, because they are extremely worried about the privacy of their medical records.

The EMR policy complaints indicated that they have adequate knowledge of the content and guidelines within the EMR privacy policies compared to non-complaints, as

evidenced by the significant mean differences. An interpretation for the high awareness level of EMR complaints could be that that during orientation and training, the employees are regularly exposed to detailed content and instructions in complying with the privacy policies as well as the implications associated with its usage; which in turn underscores the relevance of contributing to the data protection of patients within the health facilities (Keshta and Odeh, 2021; Haas et al., 2011).

Similarly, there was a huge difference in the participation in training sessions purposely focused on EMR privacy policies, with EMR complaints exhibiting greater participation compared to the non-EMR complaints. The study also indicates that EMR complaints are highly aware that participation in EMR policy compliance training can contribute to improving health professionals' understanding compared to the non-complaints. A justifiable interpretation could be that individual healthcare professionals who take part in the EMR privacy policy training boost their confidence and their motivation to comply with the privacy rules put in place by their organizations.

5.3 Factors that Influence Health Workers' Compliance with EMR Privacy Policy in Ghana

The estimated factors influencing health professionals' adherence to the electronic medical record privacy policy are shown in Table 4.3. From the result, the model has considerable explanatory power (23.94%) at the 1% level. This indicates that the adopted model was able to explain the variation between the dependent and independent variables included in the study. The independent variables include the age of the health professionals, education, years of working experience, years of EMR usage, organizational commitment, the emergence of EMR privacy policy breach,

organizational priority, regular training, user-friendly nature of the EMR device, leadership support, internal communication and organizational culture. Out of the 13 variables included, four of them were found to be significant in determining health professionals' compliance with electronic health records. For instance, the emergence of electronic medical record breaches was found to be significant at a 5% significance level. This implies that a unit increase in EMR privacy policy breaches increases the decision of health professionals to comply with the EMR policies.

The outcome might be that when administrators or directors of healthcare facilities notice a rise in breach cases, they implement special regulations and penalties that compel employees to closely follow the privacy policy for electronic health records set up by the facilities. In conformity with the result, Pool et al. (2024) argued that the exposure of health data in an authorized manner may sometimes occur in forms such as non-compliance, lack of awareness, data protection failure in third-party sources; this poses serious risks, harms individuals and attracts hackers. Tackling this issue may result in health facilities introducing stricter regulations and policies to ensure full compliance. Prioritization of the electronic medical record privacy policy by health facilities was found to be significant at a 5% level and had a positive effect on compliance. This is because when health facilities place a high priority on safeguarding medical records, staff members are constantly vigilant or quick to pledge to abide by the EMR privacy policy. At a 5% significance level, an increase in leadership support was found to decrease workers' health data privacy compliance. A possible interpretation of the result could be that the current leadership support offered to health professionals in the selected health facilities does not directly affect employee compliance.

This can also be attributed to the leadership style exhibited at the workplace by the heads or directors of their various facilities. In justification of the result, Vignoli et al. (2018), Ali et al. (2015), and Sarti (2014) argued that the quality of leadership support is related to the leadership style in the workplace. The authors contend that effective leadership at work can foster a high-quality workplace, which in turn can influence how well staff members perform in providing excellent customer service. Given that it aligns with the employee's adherence to the EMR privacy policies. On the contrary, when leadership style does not create a quality work environment, health professionals may be discouraged from adhering to the EMR privacy policies. An increase in organizational communication was found to increase health workers' compliance with EMR compliance. This is because organizational internal communication enables workers to be more updated frequently on the need to comply with EMR privacy policies, which also may influence their work engagement as information is easily relayed to them regularly (Abu Dalal et al.,2022).

5.4 Perception of Compliance of EMR Privacy Policy Among Health Workers

Table 4.4 presents the estimation of health professionals' perception of compliance with electronic medical records. From the result, we observe weak (0.16) perceptions of employees on employees' compliance with EMR privacy policies in their daily work. This can be explained by the fact that, even though different health centres have made an effort to encourage adherence to the EMR privacy policy, employees occasionally fail to follow instructions in their day-to-day work, particularly when there are technical difficulties or emergencies involving the electronic device. Meanwhile, irregular adherence to the privacy policy may lead to data breaches, which could harm the company's reputation as well as the patients. (Pool et al., 2024). It was discovered that

employees' perceptions of department and team frequency in guaranteeing adherence to EMR privacy were moderate (0.52). The outcome shows that department heads or directors do not consistently police the policies; nonetheless, the frequency of privacy policy enforcement may depend only on onboarding meetings and occasionally on incidents of breaches within the company.

Health professionals strongly (0.68) perceived that logging out of the EMR system after use can ensure the privacy of the health data. This could be explained that when staff members exit EMR systems after utilizing them, the data exposure to outside parties or people who could alter the data is reduced. The staff firmly believed that keeping login information private may help ensure adherence to the EMR privacy policy. This is because the health sectors have been educated on the relevance of keeping logging details secret to avoid external parties having access to the EMR systems. Medical data records are accessible by several degrees of authorization, according to Vora et al. (2019), emphasizing that illegal access could lead to a policy violation. Accordingly, to improve the confidentiality of the organizational data, it may be necessary to first avoid providing login credentials to prevent external access to the health data. In addition, the result also revealed a strong and positive perception (0.63) of health workers that ensuring screens are not visible to others can lead to EMR privacy policy compliance. This is because it would be difficult for individuals outside of their department or third parties to access the private information of their patients, as well as information that is important to the health Centre, if medical professionals avoided sharing the screens of smartphones, tablets, and laptops that held the data in their respective departments.

Normally, this data contains patients' names and addresses, tests, diagnoses, treatments and medical history, which demonstrates that avoiding screen and sharing of logging details of such devices can prevent the issue of data manipulation and fraudulent use (Keshta and Odeh, 2020; Muacevic et al., 2022). A strong perception score (0.63) was recorded for the idea that reporting suspicious activities or breaches can help strengthen EMR privacy policy compliance. This can be explained that when health professionals observe or encounter an action that results in a breach of the policy, they turn to report to their superiors or authorities, who also take immediate action to ensure full security and protection of patient data. This is particularly important as it prompts privacy breaches and could enable management to draw up training and educational plans to enlighten the workers. Health professionals strongly believed (0.73) that adhering to established standards can help ensure compliance with EMR privacy policies. This is because the established procedures and training act as a master's guide, which, more significantly, keeps employees from interfering with patient data confidentiality while doing their duties. These procedures guarantee uniformity and eradicate the problem of data manipulation and the disclosure of private information to outside parties (Pool et al., 2024). The degree to which health professionals believed that management was enforcing the EMR privacy policy was moderate (0.57). This suggests that management's dedication to enforcing privacy policies merely aligns with the anticipated enforcement efforts to ensure that employees integrate them into their everyday routines or activities. The management board or team's workload may also be to may be a key factor, as they rarely have enough time to assess the degree of compliance of their subordinates in the health centres.

5.5 Challenges Faced by Workers in Complying with EMR Privacy Policy

Table 4.5 shows the estimation of some challenges that impact workers' compliance with electronic medical data privacy policies. The results indicate that high workload and time constraints are the most significant challenges (π=2.79), preventing them from adhering to the policies. This is because when healthcare workers are overloaded with multiple tasks, they often lack the time to read instructions during service delivery. Additionally, heavy workload can cause stress and burnout, which may reduce their ability to follow protocols, potentially leading to patient data breaches (Provenzano et al., 2024). Inadequate training and workshops were identified as the second most common challenges faced by employees in complying with EMR privacy policies (π=3.14). This can be explained by the fact that healthcare staff in various institutions are not regularly provided with training that emphasises the importance of maintaining patient confidentiality and how it can help prevent manipulation and fraudulent activities.

Moreover, limited access to modern technological devices had an index of (π=3.41), indicating its significant role in affecting employees' compliance with electronic health data privacy. A possible reason for this higher index is that many health institutions continue to rely on outdated technology with weak security features, making patient data more vulnerable to external tampering. According to Provenzano et al. (2024), limited access to advanced technologies and difficulties in managing existing systems can lead to technostress, which hampers their ability to comply with new privacy policies at their workplaces. Challenges such as resistance to change from colleagues, the complexity of the EMR privacy policy, and lack of motivation and incentives were also found to hinder

compliance among health professionals; however, their impact is less significant compared to the first three challenges.

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

6.1 Introduction

This study specifically examines how health professionals comply with Electronic Medical Record (EMR) Privacy Policies of health facilities. With the increasing application of digital systems in health care, patient data privacy has developed into an important issue. This chapter summarizes the findings of the study, draws conclusions, and gives recommendations to policymakers, health practitioners, and future research.

6.2 Summary of Findings

The study assessed the awareness and knowledge level of healthcare professionals regarding the Electronic Medical Record (EMR) privacy policies within their respective healthcare facilities. The results indicated that the overwhelming majority (94.34%) of healthcare professionals were aware of the EMR privacy policies in place, a finding consistent across various demographic groups (e.g., age, gender, and education level). Most participants reported that they were introduced to the policies through formal orientation and onboarding programs (41.51%), followed by training workshops and seminars (27.17%).

Despite high levels of awareness, there was a notable gap in the application of these policies to everyday clinical practice. For instance, although 94.34% of healthcare workers were aware of the policies, only a small proportion were fully compliant with the practices in their daily routines. The discrepancy between knowledge and practice suggests that while health professionals are cognizant of the policy contents, there

remains a challenge in consistently adhering to the protocols, indicating that further integration into everyday workflows may be necessary to ensure full compliance.

The study examined various factors that influence healthcare professionals' compliance with EMR privacy policies, employing logistic regression models to quantify their impact. Significant organizational and environmental factors emerged as strong predictors of compliance. The prioritization of EMR privacy policies within the healthcare facilities had a significant positive effect on compliance (coefficient = 2.019, p = 0.013). This indicates that when healthcare organizations emphasize EMR privacy as a critical aspect of their operations, healthcare professionals are more likely to adhere to the policies.

The occurrence of EMR breaches was another critical factor influencing compliance. Respondents who had previously encountered or were aware of breaches were significantly more likely to comply with privacy policies (coefficient = 1.713, p = 0.011). The awareness of potential risks and consequences of non-compliance acted as a strong motivator to adhere to privacy protocols.

Interestingly, leadership support showed a counterintuitive effect, with a negative coefficient (-0.806, p = 0.040). This suggests that in some instances, leadership interventions were reactive rather than proactive, potentially limiting the long-term effectiveness of leadership support in fostering a culture of privacy compliance.

Moreover**,** Effective communication channels within healthcare organizations (coefficient = 1.057, p = 0.077) were found to have a marginally significant positive effect on compliance. This indicates that clear and consistent communication about the importance of EMR privacy policies can enhance adherence among healthcare

professionals. These findings underscore the importance of organizational factors, particularly leadership and communication, in promoting compliance. Moreover, they suggest that compliance can be fostered through the proactive prioritization of EMR privacy, alongside robust mechanisms for breach awareness and support from organizational leadership.

Furthermore, Healthcare professionals' perceptions of compliance practices were assessed using a weighted average index (WAI) to measure the strength of their beliefs regarding the effectiveness of certain EMR privacy practices. The results revealed strong perceptions regarding specific privacy measures, including:

Avoiding Sharing Login Details (WAI = 0.74). The overwhelming majority of respondents believed that preventing unauthorized access by keeping login credentials confidential was one of the most critical practices for ensuring compliance with EMR privacy policies.

Logging Out After Use (WAI = 0.68), Respondents strongly supported the practice of logging out of the EMR system after use to prevent unauthorized access, which was seen as an effective measure for maintaining data confidentiality. Ensuring Screens Are Not Visible (WAI = 0.63), Protecting patient data by ensuring that screens displaying sensitive information are not visible to unauthorized individuals also received strong endorsement.

Following Established Access Protocols (WAI = 0.72), Respondents reported strong support for adhering to institutional protocols regarding access to EMR systems as a

necessary measure for ensuring privacy compliance. Despite the strong perceptions of these compliance practices, the study found that these behaviors were inconsistently implemented in daily clinical routines. Compliance was often undermined by operational challenges such as time constraints and high workloads, which hindered the regular enforcement of privacy policies. This gap between perception and practice emphasizes the need for continuous monitoring and enforcement of these practices to improve compliance.

The study identified and ranked several challenges that healthcare professionals face when attempting to comply with EMR privacy policies. These challenges were analyzed using Friedman's test, revealing the following results:

High Workload and Time Constraints (Mean = 2.791): The most significant challenge identified was high workload and time constraints, which were perceived as major obstacles to adhering to EMR privacy policies. Healthcare professionals often reported feeling overwhelmed by clinical duties, leaving little time for consistent application of privacy policies.

Inadequate Training and Workshops (Mean = 3.148): Inadequate training was ranked as the second most significant barrier to compliance. Many respondents reported that they had not received sufficient or ongoing training to keep them up-to-date on the latest EMR privacy policies and best practices for safeguarding patient data.

Limited Access to Modern Technologies (Mean = 3.414): A lack of access to up-to-date technological infrastructure was another key challenge. Many health facilities were

found to rely on outdated EMR systems with insufficient security features, which hampered compliance with privacy protocols.

Resistance to Change (Mean = 3.605)**:** Resistance to adopting new policies and technologies from colleagues was also identified as a challenge. This reluctance, often stemming from a perceived increase in workload or a lack of motivation, prevented some staff members from fully engaging with new privacy protocols.

Complexity of EMR Privacy Policies (Mean = 3.624): The complexity of the privacy policies was considered a significant barrier. Respondents indicated that the technical language and the detailed nature of the policies made them difficult to fully understand and apply, further hindering compliance. These findings suggest that addressing these challenges by providing adequate training, improving technological infrastructure, and promoting organizational change could significantly enhance compliance with EMR privacy policies. The barriers identified here emphasize the need for systemic interventions at both the organizational and policy levels.

6.3 Conclusion

Awareness of EMR privacy policies among healthcare professionals in the Ashanti Region is generally high. However, there is a clear gap between awareness and the integration of privacy practices into daily clinical routines. Knowledge alone does not translate into behavior change, highlighting the need for more effective training and practical applications. For the organizational culture and leadership play a crucial role in influencing compliance with EMR privacy policies. Policies should emphasize the importance of organizational commitment, frequent training, and leadership support to

enhance compliance. Moreover, Perceptions of EMR privacy policy compliance were strong in terms of individual practices, yet weak when it came to routine integration. This highlights a need for better enforcement of compliance practices at the organizational level and continuous reminders for healthcare workers to incorporate these practices into their daily routines. Also, high workload and insufficient training are major obstacles to EMR privacy policy compliance. Organizations need to address these issues by redistributing responsibilities, investing in modern technologies, and offering regular training sessions to keep staff updated on best practices. The study also reveals that organizational-level factors such as prioritization of EMR policies, experience with privacy breaches, and internal communication are more influential in predicting compliance than individual demographic factors. These finding challenges earlier research emphasizing personal characteristics and shifts focus toward institutional accountability.

An important theoretical insight emerging from this study is the observed disparity between perceived knowledge and actual compliance. Non-compliant respondents reported higher self-rated knowledge of EMR policies, suggesting that awareness alone does not guarantee behavioral change. This highlights the need for behaviorally informed interventions beyond conventional training models.

6.4 Recommendations

6.4.1 For Policymakers:

1. Increase and Enhance Continuous Orientation Training

Policymakers should encourage regular, practice-based training and refresher courses for all healthcare workers on the privacy policies concerning EMR. Such events should be

showcasing real-life examples to exhibit the need to connect the gap between knowledge and practice.

2. **Strengthened Organizational Enforcement and Monitoring**

The guidelines for monitoring compliance with EMR privacy policies should be put in place in health facilities. This can be done through conducting and implementing regular audits, spot checks, and accountability mechanisms.

For Healthcare Practitioners:

1. **Improvement of Technology Infrastructure**

Health facilities should go for modern, user-friendly EMR systems with solid security features attached to them. This will reduce the hassles related to compliance and ensure that the systems are intuitive and secure.

2. **Workload and Staffing Constraints**

Health facility managers should analyze the workload distribution and even consider employing additional staff to ease the pressure of time. When the workload is manageable, it will enable healthcare professionals to devote time to observing privacy policy requirements without the distraction of too many tasks.

3. **Incentivize Compliance**

Introduce rewards programs for employees who comply with EMR privacy policies more consistently. Noting compliance with the privacy policy can motivate other employees toward compliance.

For Future Research:

1. Explore Leadership Styles and Their Impact

Future studies should investigate the styles of leadership that lead toward complying with EMR privacy policies demonstrated by health professionals. Leadership dynamics would, therefore, clear the field on the organization factors that affect compliance.

2. Causes and Effects of Data Breaches

The future should direct studies to the causes within health institutions and the resulting long-term effects both on patients and healthcare organizations.

3. Effectiveness of Compliance Training

Future research could involve evaluating how effective various models of training have been especially in resource-poor settings such as Ghana, in order to uncover which mechanisms, improve compliance toward EMR privacy policies the most.

REFERENCES

Aithal, P. S., & Madhushree, L. M. (2019). *Information Communication & Computation Technology (ICCT) as a Strategic Tool for Industry Sectors*. *1*.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences (Switzerland)*, *11*(8). https://doi.org/10.3390/app11083383

AlSadrah, S. A. (2020). Electronic medical records and health care promotion in Saudi Arabia. *Saudi Medical Journal*, *41*(6), 538–589. https://doi.org/10.15537/SMJ.2020.6.25115

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review*, *67*(2), 218–230. https://doi.org/10.1111/inr.12585

Bervell, B., & Al-Samarraie, H. (2019). A comparative review of mobile health and electronic health utilization in sub-Saharan African countries. *Social Science and Medicine*, *232*, 1–16. https://doi.org/10.1016/j.socscimed.2019.04.024

Bhyat, R., Hagens, S., Bryski, K., & Kohlmaier, J. F. (2021). Digital Health Value Realization Through Active Change Efforts. *Frontiers in Public Health*, *9*(October), 1–9. https://doi.org/10.3389/fpubh.2021.741424

Bisrat, A., Minda, D., Assamnew, B., Abebe, B., & Abegaz, T. (2021). Implementation challenges and perception of care providers on Electronic Medical Records at St. Paul's and Ayder Hospitals, Ethiopia. *BMC Medical Informatics and Decision Making*, *21*(1), 1–12. https://doi.org/10.1186/s12911-021-01670-z

Caliskan, Y. (2016). 국회선진화법' 에 관한 보론No Title'. 입법학연구, *제13집 1호*(May), 31–48.

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, *120*(c), 0–32. https://doi.org/10.1016/j.technovation.2022.102480

Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and

Availability in Information Security. *Journal of ICT In Education*, *8*(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). *THIS IS A DRAFT VERSION – GO TO PUBLISHER FOR FINAL https://doi.org/10.1016/j.cose.2020.101713*.

Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: the mediating effect of social bonding towards healthcare nurses. *Sustainability (Switzerland)*, *13*(5), 1–25. https://doi.org/10.3390/su13052800

Essuman, L. R., Apaak, D., Ansah, E. W., Sambah, F., Ansah, J. E., Opare, M., & Ahinkorah, B. O. (2020). Factors associated with the utilization of electronic medical records in the Eastern Region of Ghana. *Health Policy and Technology*, *9*(3), 362–367. https://doi.org/10.1016/j.hlpt.2020.08.002

Filippidou, A. (2020). Deterrence: Concepts and Approaches for Current and Emerging Threats. *Advanced Sciences and Technologies for Security Applications*, 1–18. https://doi.org/10.1007/978-3-030-29367-3_1

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *Data Base for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Harrison, P. J., & Ramanujan, S. (2011). Electronic Medical Records: Great Idea Or Great Threat To Privacy? *Review of Business Information Systems (RBIS)*, *15*(1), 1–8. https://doi.org/10.19030/rbis.v15i1.3992

Ibrahim, A. A., Ahmad Zamzuri, M. A. I., Ismail, R., Ariffin, A. H., Ismail, A., Muhamad Hasani, M. H., & Abdul Manaf, M. R. (2022). The role of electronic medical records in improving health care quality: A quasi-experimental study. *Medicine (United States)*, *101*(30), E29627. https://doi.org/10.1097/MD.0000000000029627

Janett, R. S., & Yeracaris, P. P. (2020). Electronic medical records in the american health system: Challenges and lessons learned. *Ciencia e Saude Coletiva*, *25*(4), 1293–1304. https://doi.org/10.1590/1413-81232020254.28922019

Janssen, A., Donnelly, C., Elder, E., Pathmanathan, N., & Shaw, T. (2021). Electronic medical record implementation in tertiary care: factors influencing adoption of an electronic medical record in a cancer centre. *BMC Health Services Research*,

21(1), 1–9. https://doi.org/10.1186/s12913-020-06015-6

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Knauder, H., & Koschmieder, C. (2019). Individualized student support in primary school teaching : A review of in fl uencing factors using the Theory of Planned Behavior (TPB). *Teaching and Teacher Education*, *77*, 66–76. https://doi.org/10.1016/j.tate.2018.09.012

Kuo, K. M., Talley, P. C., & Cheng, T. J. (2019). Deterrence approach on the compliance with electronic medical records privacy policy: The moderating role of computer monitoring. *BMC Medical Informatics and Decision Making*, *19*(1), 1–12. https://doi.org/10.1186/s12911-019-0957-y

Kurniawati, putri. (2017). No Titleالابتزاز الإلكتروني. ..جرائم تتغذى على طفرة »التواصل ال. *Universitas Nusantara PGRI Kediri*, *01*, 1–7.

Lee, L. Y. K., Lam, E. P. W., Chan, C. K., Chan, S. Y., Chiu, M. K., Chong, W. H., Chu, K. W., Hon, M. S., Kwan, L. K., Tsang, K. L., Tsoi, S. L., & Wu, C. W. (2020). Practice and technique of using face mask amongst adults in the community: A cross-sectional descriptive study. *BMC Public Health*, *20*(1), 1–11. https://doi.org/10.1186/s12889-020-09087-5

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*, 1–21. https://doi.org/10.1016/j.infsof.2022.106868

Mensah, G. B. (2023). INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION AI-Augmented Public Health Administration in sub-Saharan Africa: Addressing Challenges in Ghana's Cyberlaws Regimes for Smooth and Effective Use. *International Journal of Legal Science and Innovation*, *5*, 26–54.

Mitchell, M., & Kan, L. (2019). Digital Technology and the Future of Health Systems. *Health Systems and Reform*, *5*(2), 113–120. https://doi.org/10.1080/23288604.2019.1583040

Mubarkoot, M., Altmann, J., Rasti-Barzoki, M., Egger, B., & Lee, H. (2023). Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review. *Computers and Security*, *124*, 102985. https://doi.org/10.1016/j.cose.2022.102985

Ndlovu, K., Mars, M., & Scott, R. E. (2021). Interoperability frameworks linking mHealth applications to electronic record systems. *BMC Health Services*

Research, *21*(1), 1–10. https://doi.org/10.1186/s12913-021-06473-6

Netherlands Annual Review of Military Studies 2020. (2020).

Niang, K., Fall, A., Ndiaye, S., Sarr, M., Ba, K., & Masquelier, B. (2023). Enhancing the value of death registration with verbal autopsy data: a pilot study in the Senegalese urban population in 2019. *Archives of Public Health*, *81*(1), 1–12. https://doi.org/10.1186/s13690-023-01067-6

Nii Lantei Wallace-bruce, B. (2018). *Compliance With Electronic Medical Records Privacy Policy: a Perspective of Employees of a Private Hospital in Accra, Ghana*. *10226444*.

Ostlund, A. (2013). HIPAA (Health Insurance Portability and Accountability Act). *Consumer Survival: An Encyclopedia of Consumer Rights, Safety, and Protection: Volume 1-2*, *2*, 505–509.

Protection, D. (2012). Data Protection Act, 2012. *Parliament of Ghana*, 1–43. https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf

Roney, L. N., Westrick, S. J., Acri, M. C., Aronson, B. S., & Rebeschi, L. M. (2017). Technology use and technological self-efficacy among undergraduate nursing faculty. *Nursing Education Perspectives*, *38*(3), 113–118. https://doi.org/10.1097/01.NEP.0000000000000141

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. *Healthcare (Switzerland)*, *10*(12). https://doi.org/10.3390/healthcare10122531

Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The recent progress and applications of digital technologies in healthcare: A review. *International Journal of Telemedicine and Applications*, *2020*. https://doi.org/10.1155/2020/8830200

Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*, *8*, 136947–136965. https://doi.org/10.1109/ACCESS.2020.3011099

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, *7*, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

Simon, G., & Aliferis, C. (2024). *Data Design in Biomedical AI/ML*. (G. J. Simon & C.

Aliferis (Eds.); pp. 341–375). https://doi.org/10.1007/978-3-031-39355-6_7

Sriram, C., & Mohanasuundaram, V. (2020). Adoption of Health Management Information System (HMIS) among ESIC Healthcare Professionals in Southern Districts of Tamil Nadu: An Integrated Model. *Indian Journal of Public Health Research & Development*, *11*(03), 559–563. https://doi.org/10.37506/ijphrd.v11i3.1212

Standards, A. U. S. D., Stevens, R., Dykstra, J., Everette, W. K., & Chapman, J. (2020). *Compliance Cautions : Investigating Security Issues*. *February*.

Stephenson, M. (2021). Northumbria Research Link (www.northumbria.ac.uk/nrl). *Academy of Management*, *51*(September), 1–51.

Sulaiman, M., & Arifudin, A. (2024). *Electronic Medical Records (EMR) For Nursing Documentation : A Concept Analysis*. Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-467-9

Taherdoost, H. (2019). What Is the Best Response Scale for Survey and Questionnaire Design; Review of Different Lengths of Rating Scale / Attitude Scale / Likert Scale. *International Journal of Academic Research in Management (IJARM)*, *8*(1), 1–10.

Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A systematic review on cloud storage mechanisms concerning e-healthcare systems. *Sensors (Switzerland)*, *20*(18), 1–32. https://doi.org/10.3390/s20185392

Tsai, C. H., Eghdam, A., Davoody, N., Wright, G., Flowerday, S., & Koch, S. (2020). Effects of electronic health record implementation and barriers to adoption and use: A scoping review and qualitative analysis of the content. *Life*, *10*(12), 1–27. https://doi.org/10.3390/life10120327

Williamson, S. M., & Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences (Switzerland)*, *14*(2). https://doi.org/10.3390/app14020675

Wong, L. P., Alias, H., Wong, P. F., Lee, H. Y., & AbuBakar, S. (2020). The use of the health belief model to assess predictors of intent to receive the COVID-19 vaccine and willingness to pay. *Human Vaccines and Immunotherapeutics*, *16*(9), 2204–2214. https://doi.org/10.1080/21645515.2020.1790279

APPENDICE

APPENDIX A

QUESTIONNAIRE

Dear Respondent,

I am conducting a study on perspective of employees' compliance with electronic medical records privacy policy in Ashanti Region. Your participation is crucial to the success of this study. Your responses will be treated with strict confidentiality, and the data will be used solely for academic purposes. Please answer the questions truthfully.

Section A: Demographic Information

1 . Gender:

[ ] Male

[ ] Female

2. Age Group:

[ ] Below 25 years

[ ] 25- 34 years

[ ] 35 - 44 years

[ ] 45 - 54 years

3. Highest Educational Qualification:

[ ] Certificate/Diploma

[ ] Bachelor’s Degree

[ ] Master’s Degree

[ ] Doctorate

[ ] Other (please specify):……..

4. Job Title:

[ ] Doctor

[ ] Nurse

[ ] Medical Records Officer

[ ] IT Personnel

[ ] Administrative Staff

[ ] Other (please specify): …….

5. Years of Experience in the Healthcare Sector:

[ ] Below 1 year

[ ] 1-5 years

[ ] 6 -10 years

[ ] 11-15 years

[ ] 16 years and above

6. Years of Experience Using EMR Systems:

[ ] Less than 1 year

[ ] 1-5 years

[ ] 6 -10 years

[ ] 11-15 years

7. Hospital Affiliation:

[ ] Mampong Government Hospital

[ ] Agona Government Hospital

[ ] Ejura Government Hospital

Section B: Awareness of EMR Privacy Policies

8. Are you aware that your hospital has an EMR privacy policy in place?

[ ] Yes

[ ] No

9. How did you first become aware of the EMR privacy policy in your hospital? (Select all that apply)

[ ] Orientation/Onboarding Program

[ ] Training Workshops/Seminars

[ ] Departmental Meetings

[ ] Internal Communications (e.g., Memos, Emails)

[ ] Through Colleagues

[ ] Hospital Noticeboards/Posters

[ ] Other (please specify):……..

10. How frequently do you receive updates or reminders regarding the EMR privacy policies?

[ ] Regularly (Monthly/Quarterly)

[ ] Occasionally (Once or Twice a Year)

[ ] Rarely

[ ] Never

11. Do you believe you have adequate knowledge of the content and guidelines within the EMR privacy policies?

[ ] Yes, very well informed

[ ] Somewhat informed

[ ] No, not well informed

[ ] Not aware of the details at all

1 2. Have you participated in any training sessions specifically focused on EMR privacy policies in the last [ ] 2 months?

[ ] Yes

[ ] No

1 3. If yes, how effective do you think the training was in improving your understanding of EMR privacy policies?

[ ] Very Effective

[ ] Moderately Effective

[ ] Not Effective

[ ] I did not attend any training

Section C: Perceived Level of Compliance with EMR Privacy Policies

1 4. On a scale of [ ] to 5, how would you rate your own compliance with the EMR privacy policies in your daily work?

[ ] [ ] Very Low

[ ] 2 Low

[ ] 3 Moderate

[ ] 4 High

[ ] 5 Very High

1 5. On a scale of [ ] to 5, how would you rate the compliance level of your department/team with the EMR privacy policies?

[ ] 1.Very Low

[ ] 2 Low

[ ] 3 Moderate

[ ] 4 High

[ ] 5 Very High

1 6. How often do you practice the following behaviors to ensure compliance with EMR privacy policies? (Indicate the frequency for each behavior)

Behavior	**Always**	**Often**	**Sometimes**	**Rarely**	**Never**
Logging out of the EMR system after use					
Avoiding sharing of login credentials					
Ensuring that screens are not visible to others					
Reporting suspicious activities or breaches					
Following established protocols for accessing records					

1 7. In your view, how strictly does management enforce EMR privacy policies in your hospital?

[ ] Very Strictly

[ ] Moderately Strictly

[ ] Not Very Strictly

[ ] Not at All

1 8. Have you ever reported or been aware of a breach in EMR privacy policies in your hospital?

[ ] Yes

[ ] No

Section D: Factors Affecting Compliance with EMR Privacy Policies

1 9. Please indicate your level of agreement with the following statements regarding factors that influence compliance with EMR privacy policies. (Rate each from [ ] Strongly Disagree to 5 Strongly Agree)

Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
Regular training is provided to support compliance					
The EMR system is user friendly and easy to navigate					
There is adequate leadership support for compliance initiatives					
The privacy policies are clearly communicated and easy to understand					
Colleagues actively promote a culture of compliance					

20. In your opinion, what factors have the most significant impact on compliance with EMR privacy policies in your hospital? (Select all that apply)

[ ] Availability of regular training

[ ] The complexity of the policies

[ ] Technological infrastructure and support

[ ] Leadership and management commitment

[ ] Peer influence and culture

[ ] Others (please specify):……..

21. Do you think that compliance with EMR privacy policies is prioritized in your hospital compared to other operational demands?

[ ] Yes, it is a top priority

[ ] It is somewhat prioritized

[ ] No, it is often secondary to other demands

Section E: challenges to Compliance with EMR Privacy Policies

22. What challenges do you face in complying with EMR privacy policies? (Select all that apply)

[ ] High workload and time constraints

[ ] Limited access to updated technology and resources

[ ] Inadequate training and workshops

[ ] Complexity of the privacy policies

[ ] Resistance to change from colleagues

[ ] Lack of motivation or incentives

[ ] Other (please specify): ……..

23. How often do you encounter technological issues (e.g., system crashes, slow performance) that hinder your ability to comply with EMR privacy policies?

[ ] Frequently

[ ] Occasionally

[ ] Rarely

[ ] Never

24. Do you believe that the current EMR privacy policies are realistic and practical in your daily work environment?

[ ] Yes

[ ] No

[ ] Unsure

25. Which of the following barriers do you think management should address to improve compliance with EMR privacy policies? (Select all that apply):

[ ] Lack of adequate training on privacy policies

[ ] Insufficient enforcement of privacy regulations

[ ] Limited access to necessary resources (e.g., secure systems, updated technology)

[ ] High workload and time constraints

[ ] Lack of clear communication from management

[ ] Poor monitoring and auditing of compliance

[ ] Inadequate support from IT staff

[ ] Lack of employee accountability and consequences for non-compliance

[ ] Other (please specify): _____

26. Have you ever experienced any disciplinary action or seen others disciplined for noncompliance with EMR privacy policies?

[ ] Yes

[ ] No

27. **In your view, which of the following additional measures can be taken to improve adherence to EMR privacy policies in your hospital? (Select all that apply):**

[ ] Increase staff training on EMR privacy policies.

[ ] Implement stricter penalties for policy violations.

[ ] Enhance monitoring and auditing of EMR access.

[ ] Provide more resources and support for secure EMR usage.

[ ] Improve user authentication systems (e.g., biometrics, two-factor authentication).

[ ] Increase awareness campaigns on EMR privacy policies.

[ ] Other (Please specify): _____

APPENDIX B

AKENTEN APPIAH-MENKA UNIVERSITY
of Skills Training and Entrepreneurial Development

FACULTY OF ENVIRONMENT & HEALTH EDU.
DEPARTMENT OF PUBLIC HEALTH EDUCATION

P.O. Box 40, Asante Mampong 0209777318

M/DPHE/ADM/G/03/24/57 August 6, 2024

The Regional Director
Ghana Health Service Directorate
Ashanti Region, Ghana

Dear Sir/Madam,

PERMISSION TO CONDUCT RESEARCH

Mr. Simms Ofosu (Index Number: 8222030015) is our M.Phil. Public Health student at the Department of Public Health Education, Faculty of Environment and Health Education, AAMUSTED-Mampong Campus.

Mr. Ofosu, as part of his academic requirements for the award of Master of Philosophy Degree in Public Health Education, is to undertake a project dissertation on **"Perspective of Employee's Compliance with Electronic Medical Records Privacy Policy in Ashanti Region"**.

We seek your official approval and permission to allow him to conduct this study among electronic records workers and health workers who use electronic records at the following health facilities under your jurisdiction;

1. Mampong Government Hospital
2. Nsuta Government Hospital
3. Ejura Government Hospital

Your approval letter will pave the way for him to apply for ethical clearance before the commencement of the research. The data collected will be used solely for academic purposes. The outcome of this study would provide empirical data on the privacy policy compliance among employees at health facilities in Ashanti Region. Relevant recommendations would be made to stakeholders for policy consideration and formulation.

We would be grateful if your outfit would accord him the needed assistance for the successful execution of this proposed study. Therefore, your kind approval is required to conduct this study to fulfil this academic obligation.

Yours faithfully,

DR. DENIS DEKUGMEN YAR
HEAD OF DEPARTMENT
ddyar@aamusted.edu.gh / (0243236810)

cc: The Health Director, Mampong Government Hospital
The Health Director, Nsuta Government Hospital
The Health Director, Ejura Government Hospital