SCHOOL OF PUBLIC HEALTH

COLLEGE OF HEALTH SCIENCES

UNIVERSITY OF GHANA

COMPLIANCE WITH ELECTRONIC MEDICAL RECORDS PRIVACY POLICY: A PERSPECTIVE OF EMPLOYEES OF A PRIVATE HOSPITAL IN ACCRA, GHANA

BY

NII LANTEI WALLACE-BRUCE

(10226444)

THIS DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF PUBLIC HEALTH

JULY, 2021

DECLARATION

I hereby declare that apart from referencing other peoples' work that I have duly acknowledged, this project is my original work, produced from a research I have undertaken under supervision. No previous submission of either whole or part of this project has been made elsewhere for a degree. I therefore submit this project to the Department of Social and Behavioural Science, School of Public Health, University of Ghana, in partial fulfilment for the award of Master of Science in Public Health.

SIGNATURE 

NII LANTEI WALLACE-BRUCE DATE: 25/06/2021

(STUDENT)

SIGNATURE 

FRANCES BAABA DA-COSTA VROOM, PhD DATE: 25/06/2021

(SUPERVISOR)

ACKNOWLEDGEMENT

I would like to thank the Almighty God for His grace and strength which enabled me to go through this programme successfully.

I would also like to express my deepest gratitude to my supervisor, Dr. Baaba da-Costa Vroom, for her guidance and meticulous supervision.

I am grateful for the support given to me by the staff of Nyaho Medical Centre, especially Amanda Slagle (Quality Director).

My profound gratitude goes to my supportive mother and brother, Yvonne and Nii Nanka Wallace-Bruce, Naomi Adjepong, and Dzifa Ahiayibor.

Finally, I am grateful to all my course mates who in one way or the other helped me during my course of study.

ABSTRACT

Electronic Medical Records (EMR) are becoming the major technological tools for recording, storing, sharing, and analysing patient records in hospitals. This form of record has replaced the paper-based form of keeping patients' records. However, the increased vulnerability and breach of electronic medical records have also led to concerns about the privacy of patient records. To address this, privacy policies have been put in place by hospitals to protect patient information. In view of this, there is a need to understand what factors will promote compliance to these privacy policies, and to continuously measure the level of compliance. This study, therefore, seeks to identify the factors that influence compliance to EMR privacy policies in a private hospital in Ghana. The study adopted a quantitative approach. A cross-sectional survey design was used. The study used a census to collect data from respondents who are EMR users in the hospital. In all, 154 respondents participated in the survey. The data collected were analysed using SPSS version 25. The study analyses were performed using descriptive analysis and inferential statistics (correlation and regression). The findings suggest that employees of the hospital are aware of the EMR privacy policies. Also, the findings indicate that EMR users do not perceive that there are serious challenges preventing them from complying with the EMR privacy policies. The study found that the level of EMR privacy policy compliance is very high among users of the system, with self-efficacy being a predictor of EMR privacy compliance. The implication of these findings is that hospital management must train their employees to develop the skills and confidence to use the EMR privacy systems to ensure compliance.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

There has been increased development and implementation of electronic medical records (Wang, Xu & Guo, 2013). This increase in the usage of electronic medical records has been enabled by the adoption of technology in healthcare delivery. Technology is seen as the impetus leading to quality health care through the adoption of integrated information systems to manage the administration, financial and clinical aspects of hospital operations (Masrom & Rahimly, 2015). According to Tsai (2010), the development of the internet and information technology has enabled the use of electronic patient records making available patients' records such as lab results, and images to medical professions.

Many hospitals are encouraging electronic health records instead of paper-based medical records, which provide streamlined automated systems that assist healthcare professionals with diagnosis and treatment (Garson & Adams, 2008). Electronic medical records (EMR) are intended to aid medical staff in their daily activities by means of electronic data processing (Likourezos et al., 2004). This is necessary because hospitals face several challenges related to the storage and dissemination of patients' health records using manual means such as pen, paper, and human memory (Masrom & Rahimly, 2015). It is therefore obvious that electronic medical records are replacing manual information storage of medical records. Typical electronic medical records consist of sub-systems such as appointments and scheduling, admission, discharge, transfers, dietary, prescription order entry, planning, routine clinical notes, lab, and other uses (Tsai, 2010).

Apart from just keeping health information in an electronic form, some have moved on to introduce cloud electronic storage systems, where patient information is transmitted through an electronic network, which enables collaborated sharing of electronic medical records through the internet (Huang, Chu, Lien, Hsiao & Kao, 2009). In developing countries, the electronic information system is said to be in its infant stage. Sikhondze and Erasmus (2016) found that in South Africa, the use of EMR was still in the early stages. As of 2012, Acheampong (2012) stated that efforts were made to accelerate the adoption and use of EMR through the development of a health management information system (HMIS) policy and legal framework for health data reporting, medical records policy, computerized district health management information system, and the establishment of a center for health information at a central level. Despite the relatively little use of EMR in developing countries in Africa, even in 2014, Pearce and Bainbridge (2014) assert that nearly all general practitioners in Australia have electronic medical records. However, the past decade has seen a growth in the implementation of EMR in healthcare settings in both developed as well as low and middle-income countries (O'Donnell, Kaner, Shaw & Haighton, 2018).

There is limited use of electronic medical records in sub-Saharan Africa (Akanbi et al., 2012). Due to the proliferation of information technology projects, some developing countries have started implementing electronic medical records (Adjorlolo & Ellingsen, 2013). However, Adjorlolo et al. (2013) stated that most of these projects were in their embryonic stages. In Ghana, studies have provided evidence of the use of electronic medical records. One such study is by Ohemeng-Dapaah, Pronyk, Alosa, and Kanter (2010), which describes the use of real-time registration and verbal autopsy system, using MGV-NET, an open-source health information

system. Another study by Forson et al. (2013) found that Komfo Anokye Teaching Hospital in Ghana uses electronic medical records to perform patient registration, patient search, triage, etc.

Also, Samy, Ahmad, and Ismail (2010) assert that the importance of information and communication technology (ICT) in health care delivery is needed as managers attempt to improve patient safety and reduce the cost of care. The security of electronic medical records is an important issue which focuses on confidentiality (information is only disclosed to users who have the authority), integrity (information is created and modified by only those who have the right to do so), and availability (the ability of authorized users to access information when needed) (Pangalos, Gritzalis & Bozios, 1995). Electronic medical records (EMR) must have strong measures to protect the confidentiality of medical information they contain, provide the validity and accuracy to ensure the patients' rights are protected, and measures to protect the privacy of patient records (Huang et al., 2009).

Electronic medical records, despite their strength in providing quality data and detailed health care information, have issues relating to security and privacy (Perera et al., 2011). Health information privacy (HIP) is of great concern for patients and health professionals (Perera et al., 2011). For patients, the concern is about the secondary use of their health information for other purposes such as research (Perera et al., 2011). For medical care workers, their concern is how to restrict access to medical records (Perera et al., 2011).

Threats to health care information security have witnessed a tremendous increase in recent times (Wang et al., 2013). Health information and management systems security (HIMSS) report (2018) states that about 75.7% of hospitals surveyed indicated they had experienced a major security incident. The HIMSS Report (2018) also provides the category of electronic medical records as online scam or phishing (37.6%), well-meaning but negligent insiders (20.8%)

hackers (20.1%) malicious insider (5.4%), social engineering or vishing (4.7%), and other forms. Considering the lack of policy guidelines with respect to electronic data interchanges and patient-identifiable information in the Ghanaian health sector, ownership and security issues are not well defined (Acheampong, 2012).

The security and privacy issues are seen as the most significant barrier to the adoption of electronic health records (Kruse, Smith, Vanderlinden & Nealand, 2017). This makes the management of electronic health records very challenging considering the perception of patients and health professionals. A number of security and privacy policies have been put in place to ensure the successful implementation of EMR. There is, therefore, the need to investigate compliance with security measures put in place by health facilities in Ghana to manage records from a security breach.

1.2 Problem Statement

While healthcare organisations have access to a large amount of electronic medical records utilised by employees, the system allows the privileged access to patients' valuable and sensitive information (Rahim, Ismail, & Samy, 2016). There is the tendency that health care employees may cause privacy and security breaches to the system, leading to detrimental outcomes (Rahim et al., 2016). A study by Sher et al. (2017) found that fear arousal, self-efficacy, and subjective norms affect hospital staff compliance with EMR privacy policy. In Ghana, a study by Gyamfi *et al*. (2017), using four core implementers and users of EMR at the Komfo Anokye Teaching hospital found data security in terms of non-adherence to privacy and confidentiality is a barrier to the implementation of electronic medical records.

Nyaho Medical Center has been recognised as one of the few health facilities using electronic medical records (EMR) in Ghana (Graphic Online, 2020). The Patient Safety Committee has since then conducted a review of the system to ensure the protection of patients' records. The committee's work involved assessing whether the security policy is being followed by medical practitioners. The committees' report indicates that medical practitioners perceive the EMR system at the hospital could be assessed by others who are not authorised. All medical doctors in the hospital have access to every patient's medical records. The system allows medical doctors unrestricted access to every patient's records. Also, the patient's records can be altered by those that have access to it irrespective of the time they were entered. Apart from medical doctors, nurses in the hospital also have access to medical records.

The current situation at Nyaho Medical Center can be likened to the situation stated by Ariffin et al. (2018) that in practice, doctors and personnel that use the system are required to protect patients' information usually through privacy policies. However, the situation of having multiple access points in an open network of an EMR system creates the possibility of a patient's information interception (Ariffin et al., 2018). Also, Goreva et al. (2016) assert that security breaches do not involve someone hacking into the hospital's system but the issue of negligence and non-compliance with security policies, such as leaving an unattended laptop or iPad with an unauthorised person or sending patients' records to an unauthorised user.

However, it seems this issue has not attracted a lot of attention from researchers in Ghana. There is a need to consider the views of users (health workers) as proposed by Perera et al. (2011). A study on employees' level of compliance to privacy policies of current EMR of a health facility is necessary. This study, therefore, seeks to examine the factors affecting compliance with EMR privacy policies at Nyaho Medical Centre.

1.3 Research Objectives

The general objective of this study is to investigate factors affecting employee compliance with the privacy policies of Electronic Medical Records of Nyaho Medical Center.

Specifically, the study seeks to:

1. Examine the awareness of employees of the EMR privacy policy at Nyaho Medical Centre.
2. Examine the challenges faced by employees in using the EMR privacy policy at Nyaho Medical Centre.
3. Determine the perceived level of compliance with the EMR privacy policy at Nyaho Medical Centre.
4. Examine the perceptions of employees of factors affecting compliance with the EMR privacy policy at Nyaho Medical Centre.

1.4 Research Questions

1. What is the level of awareness of the EMR privacy policy at Nyaho Medical Centre?
2. What are the challenges faced by employees in using the EMR privacy policies at Nyaho Medical Centre?
3. What is the perceived level of compliance with the EMR privacy policy at Nyaho Medical Center?
4. What are the factors employees perceive influence compliance with the EMR privacy policy at Nyaho Medical Centre?

1.5 Research Hypotheses

To examine the factors affecting compliance with EMR privacy policies, the following hypotheses are proposed:

H1: Perceived susceptibility of EMR privacy has a significant effect on compliance with EMR privacy policy.

H2: Perceived severity of EMR privacy breach has a significant effect on compliance with EMR privacy policy.

H3: Perceived benefits of having EMR privacy policies have a significant effect on compliance.

H4: Perceived barriers to complying with EMR privacy policies will have a negative effect on the level of compliance.

H5: Self-efficacy of employees will have a significant effect on EMR privacy compliance.

H6: Cues to action has a significant relationship with EMR privacy compliance.

H7: Sanction severity will have a positive and significant effect on EMR privacy policy compliance.

H8: Sanction certainty will have a positive and significant effect on EMR privacy policy compliance.

1.6 Justification of the Study

The findings of this research could be a source of information for the management of hospitals on the awareness of EMR privacy policies, level of compliance, and factors motivating or factors inhibiting compliance. On the awareness aspect of the study, hospital management will

understand whether employees understand and have knowledge of the existing EMR privacy policies. This will therefore inform hospital management on the need to intensify awareness on EMR privacy policies. The results of the study will also help hospital management to identify the challenges affecting compliance with EMR privacy policies. The understanding of these challenges will aid hospital management in developing strategies and policies to ensure employees can easily comply with EMR privacy policies. Hospital management will be able to understand specific factors that enhance EMR privacy policy compliance and therefore adhere to them to improve the level of EMR privacy compliance. For policymakers such as the Ministry of Health, Ministry of Communication, and any other relevant body, the results of the study could help with the implementation of strategies to improve the level of EMR privacy compliance among health workers. This will enable the Ministry of Health to determine whether employees comply with privacy issues, and if not, suggest measures to address it. The study contributes to the literature on compliance with EMR policies in a developing country context.

1.7 Organisation of the Study

This study is organised into six chapters. Chapter one introduces the study. It comprises the background, statement of the problem, research objectives, research questions, study hypotheses, justification for the study, and organisation of the study. Chapter two presents the literature review relating to existing studies on EMR privacy compliance. This chapter presents a review of concepts, a theoretical review, and an empirical review. Chapter three provides a description of the research methodology comprising the research approach, research design, study population, sampling technique, sample size determination, data collection, data analysis, and ethical considerations. Chapter four presents the findings of the study while Chapter five

discusses the study findings with existing literature. Chapter six presents conclusions and outlines recommendations based on the findings of the study.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The literature review of this study will focus on pertinent conceptual and empirical literature on EMR privacy compliance. The literature review will begin with the explanation of EMR, and issues of EMR privacy, and compliance. The literature review will also focus on the prevention motivation theory and deterrence theory that can be used to explain the compliance of EMR privacy policy. The literature review presents some empirical results. The conceptual framework showing the relationship between compliance factors and compliance behaviour will be presented.

2.1 Concept of Electronic Medical Record (EMR)

Tamaritz et al. (2018) define electronic medical records as information recorded in any form of electronic health records from a clinical encounter. Sher et al. (2017) also define EMR as a collection of software applications commonly utilized to communicate orders for medical care, record related facts concerning a patient's medical history, and to circulate results of laboratory testing. Reis et al. (2017) state that some papers also refer to electronic medical records (EMR) as an electronic health record (EHR). EMR refers to an organisational system that allows for the sharing of clinical information, while health medical records is a system that provides the ability to share health or clinical data across health-related institutions. This study defines EMR as the computerization of health record content, which is available through computers and personal digital assistants, or tablets. The EMR system enables physicians to record patient data on a computer system, which can be accessed by others to perform a medical function.

2.1.1 Benefits of Electronic Medical Records

There are many benefits to using electronic medical records. Some of the benefits of EMR, as identified in Miller and Sim's (2004) study are explained below:

2.1.1.1 Documentation of Health Information

One of the benefits of EMR is the documentation of the progress of a patient's health status. Detailed health information is transcribed and imported into EMR in unstructured text boxes. Apart from unstructured text boxes, data entry templates are also available. It is also used to indicate important prompts. This documentation enhances the legibility and accessibility of the progress of a patient's health status using electronic means.

2.1.1.2 Ordering

One of the most important duties of physicians is ordering medications for patients. This duty can be performed using EMR by typing in prescription orders, handling alerts relating to adverse drug reactions, and printing prescriptions. Also, EMRs are used to perform referrals and diagnostic tests.

2.1.1.3 Messaging

An important benefit of EMR is information sharing. The system allows for messages to be delivered accurately and in a timely manner amongst service providers. This leads to the provision of the readily available information in a timely manner. For advanced EMR systems, messages can be sent to external providers to improve health delivery coordination.

2.1.1.4 Analysis and Reporting

EMR systems are efficient in performing quality control, performance management, and provision of feedback to improve efficient service delivery. EMR makes it possible to generate reports on the standard of service delivery.

2.1.1.5 Billing

EMR allows for the integration of financial and health records. It enables the entry of costs of service delivery and records financial transactions between the service provider and patient. This reduces inefficiencies and delays in the provision of financial records.

2.2 EMR Privacy Policies

According to Bélanger and Crossler (2011) information privacy refers to the desire of individuals to control or have some influence over data about themselves. Due to advances in information technology, there has been an increase in the threat posed by breaches in information privacy and its impact, leading to increased research to address it (Bélanger & Crossler, 2011). With the development of a more comprehensive EMR, a highly increased volume of medical records will become easily accessible to both authorized and unauthorized users both inside and outside the health care facilities (Sher et al., 2017). This has led to the development of EMR privacy policies to protect patient medical records. The compliance to EMR privacy policies in Kuo et al.'s (2017) view, can be explained using the Deterrence theory, which is the rational decisions individuals make toward committing any criminal activity based on a trade-off between inherent benefits and supposed costs. Compliance in this study describes the intentions of hospital employees using the EMR system to adhere to privacy policies.

2.2.1 Potential Breach of Privacy of EMR Information

There are a number of issues that can be described as breaches of EMR privacy. The relationship between the health care provider and the patient is one characterized by intimacy and trust, and confidentiality is embedded at least implicitly in patient-provider interactions (Barrows et al., 1996). A common breach may be an unauthorised transmission of information between health employees. A study by Harman et al. (2012) stated that physicians text other physicians about work, and there is the likelihood that it will be difficult to control the sharing of information among them.

A study by Hassidam et al. (2017) found that about 73.6% out of 299 health workers reported that they had obtained the password of another medical member of staff. The report found that at least 171 of these workers had shared their EMR credentials about 4.75 times (Hassidam et al., 2017). Also, the EMR data can be hacked, manipulated, or destroyed by internal and external users. This study considers access to EMR systems by unauthorised users, and the possible use of information by external users.

2.2.2 EMR Confidentiality Techniques

The confidentiality of the EMR system is protected using some techniques. According to El Kettani et al. (2018), the following are some of the data protection techniques that are applied in managing the confidentiality of EMR:

a. De-identification - the process of removing (or modifying) identifiers from personal health data so that identification is not reasonably possible. This technique is used to prevent the misuse of health data.

b. Pseudonymisation- consists of transforming and then replacing personal data with a pseudonym that cannot be associated with the identification data without knowing a certain secret.
c. Encryption is the process of encoding information in such a way that only authorized users can read it. EHRs should encrypt patient data in order to protect data if the hardware is stolen, or messages are intercepted.

2.2.3 Electronic Medical Records at Nyaho Medical Centre

The medical department policies (2020) of the hospital indicate that the EMR system focuses on obtaining, studying, and protecting digital health information. From this, the issue of confidentiality lies in the need to protect digital health information. Also, the medical department states that the EMR system is used in patient care planning, continuity of patient care, quality assessment and review, medical research and education, business record keeping, and legal defence.

The Data Protection Act of Ghana 2012 (Act 842, section 99) guides the management of EMR at the hospital. This law guides the control and maintenance of the EMR. The hospital's policies on EMR are confidential and therefore cannot be documented in this study. However, the study provides some details on the management of EMR as stated by law. The following issues have been documented by the hospital to guide the management of EMR as deduced from the Data Protection Act of Ghana:

a) Records must be maintained of patients who receive health care at the hospital, including inpatients and outpatients.

b) Patients and visitors who cannot be identified must be recorded as, for example, Mr. XYZ until identification is confirmed.

c) All medical records of services provided for patients shall be maintained as the property of the hospital. The hospital must ensure these records are complete, accurate, secure, and confidential. The hospital, therefore, holds legal responsibility for all medical records.

d) The medical staff and employees of the hospital are responsible for safeguarding the records of patients against loss, alteration, defacement, tampering, or use by unauthorized persons.

e) The medical records must not leave the hospital unless under the authorization of the Medical Director or a court, and in this case, the original document will be presented in court by the Medical Director.

f) All staff of the hospital must sign a confidentiality clause on the assumption of duty with the Human Resource (HR) department and a non-disclosure agreement (NDA) on resignation/termination of a contract.

2.3 Review of Related Theory

The review of literature on the factors affecting compliance with EMR privacy policy found that two main theories, namely protection motivation theory and deterrence theory seem to be widely used.

2.3.1 Protection Motivation Theory

The protection motivation theory (PMT) proposed by Rogers (1975) postulates that there are three main components of fear appeal, namely (a) the magnitude of the seriousness of the event

occurring (b) the probability of the event occurring and (c) the efficacy of the protective response. Bubeck et al. (2018) state that PMT proposes that protective behaviour is motivated by threat and coping appraisals. In the view of Tsai et al. (2016), threat appraisals are determined by perceived vulnerability and susceptibility to risks, as well as rewards associated with unsafe behaviours. On the other hand, Tsai et al. (2016) stated that coping appraisals are based on coping self-efficacy, response efficacy, and response costs associated with safe or adaptive behaviours. Coping self-efficacy is the belief that individuals can successfully carry out protective behaviours. Response efficacy is the belief in the effectiveness of the protections. Response costs refer to the costs of using security protections. Threat appraisals and coping appraisals determine behavioural intentions to adopt protections (security intentions) in the current study. Individuals undertake safety precautions they believe are effective in protecting them online and are able to enact these precautions with reasonable resource expenditure. Otherwise, they may ignore the risk and refrain from taking any protective actions.

The PMT has been applied by many studies investigating security behaviour such as desktop security behaviour (Hanus & Wu, 2016), online safety (Tsai et al., 2016), and mobile device security behaviour (Thompson et al., 2017). Additionally, it has been employed in studies on factors that affect privacy compliance (e.g. Kuo et al., 2019; Kuo et al., 2017; Sher et al., 2017).

2.3.2 The Deterrence Theory

The deterrence theory proposes the adoption of strategy on conditional threats with the goal of persuading the opponent to behave in ways that are desirable (Taddeo, 2018). In Trang and Brendel's (2019) view, a typical measure of the decreasing level of deviation from desired behaviours by employees is based on the deterrence mechanism. In information security studies,

the deterrence theory explains issues relating to sanction certainty, sanction severity, and sanction clarity (Trang & Brendel, 2019). This theory works better in explaining the factors that deter information system users from breaching security protocols. Kuo et al. (2019) state that deterrence explains the actions taken by an organisation to deter potential perpetrators from committing unlawful behaviours through the use of serious sanctions related to security breaches. Also, the theory describes how individuals will be deterred from performing undesirable behaviours due to the fact that they will be punished. For this to work, there must therefore be prescribed organisational policies and rules.

Although emanating from the criminology discipline, Kuo et al (2019) assert that the theory assumes that an individual's decision to come up with a rational decision to commit a crime is based on a cost-benefit analysis. Studies on EMR have applied the deterrence theory to study compliance with EMR privacy policies (e.g. Kuo et al., 2019; Kuo et al., 2017). With EMR studies, factors emanating from the theory include sanction severity and sanction certainty (Kuo et al., 2019).

2.4 Factors Affecting EMR Privacy Compliance

There are some factors identified in the literature as affecting compliance with EMR privacy policies. This review will discuss factors affecting compliance with EMR privacy policies.

2.4.1 Fear Arousal

Fear arousal has emerged as one of the most studied issues that have enriched the protection motivation theory in IT security research (Orazi et al., 2019). Fear arousal refers to the extent to which IT members of staff are concerned with EMR being threatened. Renaud and Dupius (2019) assert that fear appeals in ensuring security is aimed at first making people care about

something, eliciting fear emotions, and increasing the likelihood that they will perform a recommended action to avert unpleasant consequences. To ensure security compliance, fear appeals are used to motivate a behaviour change, and recent security research has explored its effect on motivating technology users to protect themselves from threats (House & Raja, 2019).

2.4.1.1 Perceived Susceptibility (Vulnerability)

Fear arousal is explained by the perceived severity and perceived vulnerability of the EMR system (Sher et al., 2017). Warner and Wang (2019) assert that vulnerability is a major factor in defining privacy because of the possibility that control of information could be at stake. In our study, perceived vulnerability refers to the IT members of staff's probability assessment of a threat resulting from non-compliance with the EMR privacy policy. Fear arousal leads to the development of a danger control process leading to positive outcomes such as employees promoting fear appeals to ensure the security of a technology (Johnston & Warkentin, 2010).

Perceived vulnerability explains the perceived potential risk of revealing personal information (Dinev & Hart, 2004). The tendency of disclosing information that is deemed as private in the health sector fits perfectly into the scenario where health workers assume that the system has lapses. The attempt to protect medical information must start with the agreement that the system is vulnerable. The vulnerability of an information system is a result of little control over information collection and the use of information beyond the original purpose for collecting the information (Youn, 2009).

2.4.1.2 Perceived Severity

Perceived severity pertains to the understood consequences of a threat originating from non-compliance with privacy policy. Ifinedo (2012) asserts that the perceived severity relates to the consequences of events, for instance, the threats to the security of an organisation's information arising from non-compliance. In Vance et al.'s (2012) view, the severity is the level of the potential effect of the threat (i.e. the damage that it can cause) in the context of information system security. Herath and Rao (2009) also assert that perceived severity refers to the degree of harm associated with a security threat to an information system. Pham et al. (2017) state that end-users of technology will be motivated to respond to security threats in the case where users feel the threat is evident and relevant to them.

2.4.2 Self - Efficacy

Self-efficacy refers to IT staff's compliance with a privacy policy as being a useful means for diminishing the threat of EMR breaches (Sher et al., 2017). The perception of employees that are capable of complying with EMR privacy policy can effectively avert the threat of EMR breaches.

In social cognitive theory, Bandura (1977), describes self-confidence as the ability to mobilise cognitive resources, motivation, and actions to ensure successful completion of a task (Pham et al., 2017). Self-efficacy assesses IT members of staff's judgment of himself or herself to be capable of compliance with the privacy policy. If they consider themselves as being incapable of compliance with a privacy policy due to inherently complicated procedures, employees may not likely comply with EMR policies (Sher et al., 2017). The appraisal conducted by an individual regarding their ability to carry out a recommendation or policy is crucial in technology adherence

policy (Johnston & Warkentin, 2010). Pham et al. (2017) explain that the human aspect must be incorporated into an information security system to ensure co-created outcomes. This, therefore, calls for a need to consider human systems to support IT systems so that a secure information environment is ensured.

Self-efficacy can also be enhanced due to response costs. This explains IT staff members' perceived cost of complying with privacy policy and may be inclusive of the money, time, or personal effort involved. In the case where the compliance behaviour requires inordinate amounts of time and effort, they may, thus, be unlikely to adhere to the given privacy policy (Sher et al., 2017).

The social norm at the workplace can also enhances self-efficacy. The theory of planned behaviour considers subjective norms, which explains the IT staff's subjective beliefs about the extent of disapproval for non-adherence to EMR privacy policy among those members who are of paramount importance to the IT staff. The influence of peers or the IT officials in an organisation will help provide guidance and warning to users concerning the security of the technology system (Johnston & Warkentin, 2010). According to the Theory of Reasoned Action, an individual's intention toward a specific behaviour can be collectively predicted by his or her attitude toward that behaviour and subjective norm posed by important others (Sher et al., 2017).

2.4.3 Perceived Benefits

Perceived benefit refers to a health information management staff member's belief in the potential benefit of protecting EMR privacy (Sher et al., 2017). Therefore, it is only when a health information management member of staff perceives the overall benefit of securing EMR privacy that he or she will engage in that protective behaviour. Several studies have reported that

perceived benefit is one of the most consistent predictors of health- or preventive-related behaviours (e.g. Kim et al., 2013).

2.4.4 Perceived Barrier

Perceived barrier measures the extent to which a health information management staff member's belief regarding the physical and psychological costs to protect EMR privacy (Sher et al., 2017). Humaidi and Balakrishan (2015) assert that the barriers in information security compliance are a major reason why employees cannot practice computer security behaviour at the workplace. A health information management staff member may hold that despite the effectiveness of protecting EMR privacy to alleviate the perceived threat, he or she may still regard the required procedures for such protective behaviour to be inconvenient or costly to him- or herself, which might constrain engagement in such behaviour.

2.4.5 Cues to Action

The term 'cues to action' refers to possible behavioural triggers that may cause health information management staff members to protect EMR privacy (Sher et al., 2017). Therefore, a health information management staff member may be inclined to protect the privacy of EMRs whenever prompted with reminder messages (Sher et al., 2017). Ng et al. (2009) for example state that some organisations use newsletters to promote the compliance of computer security behaviour in organisations.

2.4.6 Sanction Severity

From the deterrence theory, one factor that could lead to compliance with EMR privacy policies is the severity of sanctions. Kuo et al (2019) from literature assert that sanction severity refers to the degree of punishment pertinent to non-adherence to stated EMR privacy policy. This view supports that of Siponen et al. (2010) that employees will be discouraged from not following security policies because they will be punished. In terms of sanction severity, the deterrence theory suggests that if the level of sanction increases, an individual will be less likely to act illegally. In this study, it is proposed that employees' perceptions about the existence of severe sanctions will lead to lower tendencies of committing breaches of the EMR policies. Drawing from the assumption proposed by Kuo et al (2019), as the level of sanction increases conversely, hospital employees are more likely to adhere to stated privacy policy as a result. Otherwise, they are subject to punishment with severe civil or criminal penalties if they are caught breaking stated privacy policy. Guo and Yuan's (2012) study found that sanction severity has a significant effect on compliance with information security policies.

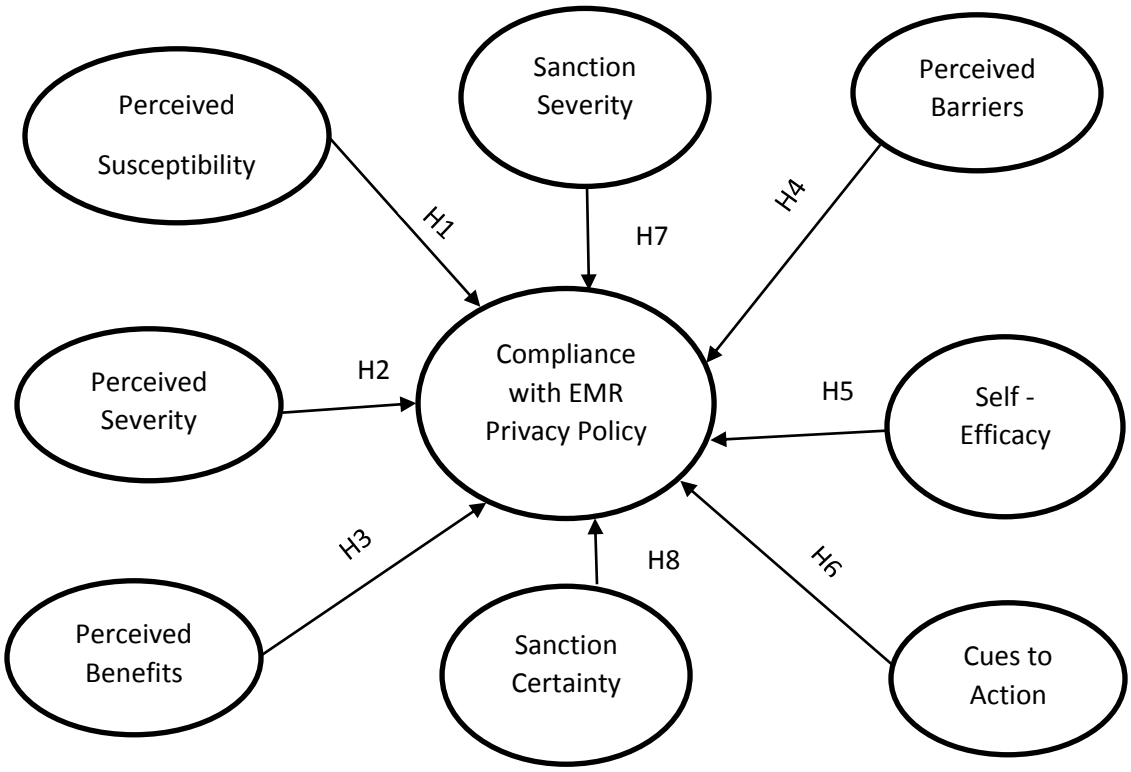
2.4.7 Sanction Certainty

The deterrence theory leads to considering sanction certainty as a major factor in studying compliance with privacy policies**. S**anction certainty means the real probability of receiving punishment related to non-adherence to EMR privacy policy (Kuo et al., 2019). The deterrence theory presumes that potential perpetrators are made aware of compliance assurance efforts such as rules and punishments necessary to restrain from illicit behaviours. In an organizational context, rules for regulating employees, however, will not be effective if the rules are not immediately enforceable. Perceived sanction certainty in the study of Sommestad et al. (2014)

was found to be a predictor of compliance with information security policy. Therefore, if employees' misbehaviours are circumvented, and they become fully aware that they will undoubtedly be penalized for such misbehaviours, employees will then more likely comply with stated rules and regulations.

2.5 Conceptual Framework

The study developed a conceptual framework using the protection motivation theory, and the deterrence theory. This framework is therefore a fusion of these two theories. The study proposes that the factors affecting compliance with EMR privacy policies include perceived vulnerability, perceived severity, perceived benefits, perceived barriers, self-efficacy, and cues to action. Also, sanction severity and sanction certainty, from the deterrence theory, were proposed to influence EMR privacy compliance. These proposed relationships lead to the formulation of eight (8) hypotheses linking these factors to EMR privacy compliance.



Source: Adapted from Sher et al. (2017) and Kuo et al (2019)

Figure 1: Conceptual Framework

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter discusses the methodology adopted to conduct this study. The chapter discusses the research design, study site, population, sampling technique and sample size, data collection, data analysis, and ethical consideration.

3.1 Research Design

The study adopted an explanatory, cross-sectional study design in finding out the factors that influence compliance with EMR policies. Saunders et al. (2009) explain that cross-sectional designs are used to study a particular phenomenon or phenomena at a particular time and tend to dominate quantitative studies. Bryman and Bell (2015) explain that cross-sectional surveys usually have large samples, are not experimental in nature, unlike longitudinal studies where the phenomenon is studied on further occasions.

This study adopted a quantitative approach to analyse the phenomena systematically. The researcher strongly believes that the quantitative technique is more appropriate for the study because of its efficacy in analysing the impact of causal factors on a phenomenon (Hair et al., 2015).

3.2 Study Site

The study was conducted at Nyaho Medical Centre, a reputable health care provider in Ghana for the past 50 years. The hospital provides services in healthcare including anaesthesia, cardiology, dentistry, dermatology, dietetics, ear, nose, and throat (ENT), endoscopy, family practice care,

haematology/sickle cell, internal medicine, neurosurgery, obstetrics/gynaecology, orthopaedics, surgery, urology, psychiatry and many more.

Nyaho Medical Centre has been recognised as one of the health facilities using electronic medical records (EMR) in Ghana (Graphic Online, 2020). Nyaho Medical Centre was chosen since it has used EMR for close to a decade.

3.3 Study Population

The target population of the study was the clinical and non-clinical staff who use the electronic medical records of Nyaho Medical Center. From the data presented to the researcher, the departments that use the EMR include medical, pharmacy, customer experience, nursing, quality control, and public health. As of May 31st, 2020, the following breakdown in table 1 represents the number of employees using the EMR.

Table 1: Users of EMR in the Hospital

Category	Department	Number of Staff Using EMR
Clinical	Medical	45
	Diagnostics	28
	Pharmacy	20
	Nursing	107
Non-Clinical	Quality Control	2
	Customer Experience	29
	Public Health	1
Total		**252**

Source: Human Resource Department, 2020

3.4 Sampling Technique

The study adopted a census sampling technique. This is because this research collected data from all employees using EMR at Nyaho Medical Center who have used and are knowledgeable about the use of EMR. Saunders et al. (2009) state that it is possible to sometimes collect data from all possible cases. A census was used because it was practicable to collect data from the entire population. Also, budgetary and time constraints may not hinder the collection of data since the Human Resource Department of the hospital managed the data collection by sending the questionnaires to all employees. In this study, the researcher only included participants who use the EMR and not every employee.

To select study participants, the human resource department of the hospital aided the researcher to get access to the employees who use the EMR system. The permission obtained from the human resource department led to the selection and distribution of the survey questionnaire. The department sent out information about the study to the work emails of the employees inviting them to willingly participate in the study. Using a population of 252 (see table 1), the response rate of the survey was 61%. In all, 154 participants responded to the survey.

3.5 Data Collection Instrument and Measurement

The data from respondents were collected using survey questionnaires. The questionnaire was developed using measurement scales adopted from Sher et al. (2017) and Kuo et al. (2019). The questionnaires were designed using Likert scale responses from ranging from strongly disagree (1) to strongly agree (5). This is to help measure employees' perceptions of the privacy and security of EMR. The questionnaire was administered using Google Forms. Google forms allows for study participants to fill surveys through online sources such as email and social media

platforms like WhatsApp. This is recommended due to the inability of the researcher to have access to respondents due to COVID 19 pandemic. The Google forms were sent to respondents through their work emails and WhatsApp. The responses were automatically recorded in Excel which were imported into SPSS for further analysis.

3.6 Data Analysis

The data were analysed using SPSS version 25 by conducting descriptive, correlation, and regression analysis. The first part of the analysis was focused on the demographic profile of respondents. Also, the descriptive analysis using mean and standard deviation were used to measure the employees' perceptions of all items used. The analysis using means and standard deviation sought to examine the perception of respondents on a number of issues related to EMR. The issues considered were awareness of EMR privacy policies, challenges in EMR privacy policies, perceived susceptibility of EMR system, perceived severity of EMR breach, perceived benefits in complying with EMR privacy policies, perceived barriers in complying with EMR, cues to action, sanction severity, sanction certainty, and finally compliance with EMR privacy policies. Using a Likert scale of 1(strongly disagree), 2 (disagree), 3 (neutral), 4 (agree) to 5 strongly agree, a high score on the scale implies there is an agreement to the questions.

Finally, to test the eight hypotheses, which seek to establish the relationship between perceived vulnerability, perceived severity, perceived benefits, perceived barriers, self-efficacy, cues to action, sanction severity, and sanction certainty and EMR privacy compliance, correlation and regression analyses were performed. The ANOVA test and t-test were used to examine the statistical significance of the proposed hypotheses.

3.7 Ethical Issues

Ethical clearance was sought from Nyaho Medical Centre Research and Development Committee (Reference Number: NMC/QUA/RES/CEMR/1/20). A letter of introduction, seeking permission from the hospital, was sent to the Human Resource Department of Nyaho Medical Centre. Participants were recruited after their consent was secured. Confidentiality was maintained since the identity and information of the participants were not disclosed. To ensure anonymity, respondents were not asked to indicate their identity. The use of an online survey also served to maintain the anonymity of respondents. The researcher sought the consent of participants using a participants' consent form. The consent form was attached to the survey and sent to the study participants. Participants were not offered any reward for participating in the study.

CHAPTER FOUR

RESULTS

4.0 Introduction

This chapter presents the results and discussion. The study results are presented using descriptive and inferential statistics. The descriptive analysis is used to analyse the demographic profile of respondents, and the perception of respondents regarding the questions. This is done using frequencies, mean, and standard deviation. The inferential statistics on the other hand presents results on the relationship between study variables using correlation and regression analysis.

4.1 Demography of Respondents

The demographic profile of respondents analysed in this study includes the age, gender, department, and the number of years working at the hospital. Using a population of 252, the response rate of the survey was 61%. In all, 154 participants responded to the survey. The results in Table 2 are presented using frequencies and percentages.

The gender of respondents is presented in Table 2. The study respondents were mostly (64.9%) female. The number of females is more than that of males since there is a higher proportion of females working in the hospital.

From the data, nursing (35.1%) and medical departments (26%) form the majority of respondents. Also, the study included 28 (18.2%) respondents from the customer experience department, followed by 18 (11.7%) respondents from the Pharmacy department. Data were collected from only 2 respondents from the quality control department. However, all departments that had employees that use EMR were duly represented.

From the results, respondents who are 33 to 38 years made up 37.7% of the participants. This is followed by 40 respondents who are between the ages of 23 to 27, On the other hand, 38 respondents are between the ages of 28-32. The study also found that 2 respondents were between ages 45-49.

The study examined the number of years the respondents have worked in the case organisation. 110 (71.4%) respondents have worked in the organisation for 1 to 5 years, 30 representing 19.5 % for 6 to 10 years, and 8 (5.2%) for 11 to 15 years. The study also found that 2 (1.3%) of the respondents have worked with the hospital for 21 to 25 years. Finally, 4 respondents indicated they have worked with the hospital for 26 to 30 (2.6%) years.

Table 2: Demographic Profile of Respondents

Demography	**Frequency**	**Percentage**
Gender of Respondents		
Male	54	35.1
Female	100	64.9
Department of Respondents		
Medical	40	26.0
Nursing	54	35.1
Pharmacy	18	11.7
Diagnostics	12	7.8
Customer Experience	28	18.2
Quality Control	2	1.3
Age of Respondents		
23 – 27	40	26
28 – 32	38	24.7
33 -38	58	37.7
40 – 45	16	10.4
45-49	2	1.3
Years of Work		
1 – 5	110	71.4
6 – 10	30	19.5
11 -15	8	5.2
21 – 25	2	1.3
26 – 30	4	2.6

Source: Field Survey, 2020

4.2 Awareness of EMR Policies

The study results presented in Table 3 show the level of awareness of EMR privacy policies in the organisation. Generally, the respondents level of EMR policy awareness was high (mean > 3.5).. The results imply that the respondents agreed that the hospital has clear guidelines on privacy compliance of EMR systems. Also, the respondents indicated the use of personal data is protected. The respondents agreed that there does not exist unauthorised removal of personal data, sharing of data with other hospitals, disclosure of patient information, and reproducing health information without the approval of the medical director. The respondents did not agree that the hospital discloses the way health data about patients are collected, processed, and used (mean = 3.1688).

Table 3: Respondents' Level of EMR Privacy Policy Awareness

Item	Mean	Standard Deviation
The hospital discloses the way health data about patients is collected, processed, and used	3.1688	1.22504
The hospital has clear and conspicuous guidelines on the disclosure of health information of patient	4.0132	.85341
I am very aware about how personal health information will be used	4.1429	.77061
The hospital does not use personal information for any purpose unless it has been authorized	4.3117	.82857
The hospital does not share personal information with other hospitals unless it has been authorised	4.4805	.81826
The hospital has a policy that all health information will not be removed by any employee	4.2727	.75210
The hospital has a policy that patients identifiable information must not be disclosed	4.5714	.57003
The hospital has a policy that records can only be reproduced with approval from the Medical Director	4.2597	.76530

Source: Field Survey, 2020

4.3 Challenges of EMR Privacy Policies

The study sought to assess the challenges the respondents face in complying with EMR privacy policies. Generally, study respondents did not perceive there are challenges in using the EMR system (mean < 3.5). The respondents did not agree that the hospital does not have EMR authentication features such as biometric (mean = 3.2857). Also, respondents perceived that patients' privacy policies do not override EMR privacy policies (mean = 3.2933). Respondents disagreed that the EMR allows employees to share information with unauthorised third parties (mean = 2.0130). The respondents also disagreed that they find it difficult to enter data into the EMR system (mean = 1.9221), the EMR system usually fails in imputing ad retrieving data (mean = 2.1948), and is complex to understand (mean = 2.2857).

Table 4: EMR Challenges

Item	Mean	Standard Deviation
The EMR/health information system used by the hospital does not have authentication features such as biometric	3.2857	1.16436
The EMR /health information system allows employees to share information to unauthorised third parties	2.0130	1.04154
The patients' privacy (preference with regard to EMR), override EMR/health information system implementation in the work I do	3.2933	.86348
I find it very difficult to enter data in EMR/health information system	1.9221	.83652
The EMR/ health information system usually fails when inputting and retrieving patient information	2.1948	.92939
The EMR/ health information system privacy policy is complex to understand and use	2.2857	.91262

Source: Field Survey, 2020

4.4 EMR Privacy Compliance

The study sought to examine the level of compliance with EMR privacy policies. The results found that there is a high level of compliance with EMR privacy policies (mean > 3.5). The results indicate that the study participants perceive that they follow EMR privacy policies, will continue to protect the EMR privacy policy, and that they are certain that they will follow the hospital EMR privacy policy. The mean values indicating the perception of EMR privacy compliance are presented in Table 5.

Table 5: Respondents' Perception of EMR Privacy Compliance

Item	Mean	Standard Deviation
I follow privacy policies of the hospital	4.4156	.67351
I continue to protect EMR/health information system privacy	4.3636	.58094
I am certain that I follow the hospital EMR/health information system policies	4.3377	.67853
Level of EMR privacy Compliance	4.3761	.55663

Source: Field Survey, 2020

To determine the level of compliance with the EMR privacy policy, an average mean of the various research questions measuring the level of compliance was computed. From the analysis, the overall mean for the level of compliance of the EMR privacy policy is 4.3761, which implies that the level of compliance is high.

4.5 Factors Affecting EMR Privacy Compliance

The study sought to explain the factors that influence EMR privacy compliance. The factors that were analysed included perceived susceptibility, perceived severity, perceived benefits, perceived barriers, cues to action, sanction certainty, and sanction severity. Table 6 provides the mean scores of all the questions asked.

Table 6: Descriptive Results of Factors Predicting EMR Compliance

Item	Mean	Standard Deviation
Susceptibility to EMR Privacy Breach		
The chances that EMR/health information system privacy may be breached is high	2.8442	1.09741
There is a strong probability that EMR/health information system privacy breaches may lead to privacy issues	3.4026	.98697
The use of EMR/health information system is likely to cause privacy problems	2.7532	1.04982
Perceived Severity		
Having EMR/health information system privacy breaches is a severe problem for me	3.5526	1.15540
Losing EMR/health information system data is a severe problem for me	3.9351	.89058
Perceived Benefits of EMR Privacy		
Complying with the privacy policy prevents future EMR/health information system privacy breaches	3.7403	.86171
The privacy policy can ensure EMR/health information system privacy	3.9351	.72918
I am less anxious about EMR/health information system privacy breaches if I can comply with the privacy policy	3.6623	.80213
Perceived Barrier of EMR Compliance		
Complying with the privacy policy may interfere with many work activities	2.4079	.99239
Complying with the privacy policy is difficult	2.2078	.90514
Self-Efficacy		
I am confident that I can comply with the privacy policy	4.2468	.66972
I am confident that I can recognise the potential problems of violating EMR /health information system privacy	4.0260	.68550
I am confident that I can comply with the privacy policy even if there is no one around to help me	4.1039	.65847
Cues to Action		
My hospital regularly distributes newsletters or articles concerning the protection of EMR/health information system privacy	3.1299	1.14733
My hospital regularly sends out alert messages regarding EMR/health information system privacy	2.8831	1.13153
My hospital regularly organizes talks on EMR/health information system privacy	3.0649	1.02693
Perception of Sanction Severity		
My hospital disciplines employees who break EMR/health information system privacy rules.	3.9870	.78372
My hospital terminates employees who repeatedly break EMR/ health information system privacy rules	3.5325	.89420
Perception of Sanction Certainty		

If I do not follow EMR/health information system privacy policies, I will be penalized	3.9221	.77149
I would be formally reprimanded if management learned that I had violated EMR/health information system privacy policy	4.0260	.87034

Source: Field Survey, 2020

4.5.1 Perceived Susceptibility of EMR Privacy Breach

This study examined the perceived susceptibility of EMR privacy breaches by respondents. As shown in Table 6, the respondents indicated that they do not agree the EMR privacy system is susceptible to breaches since the mean results were less than 3.5. A mean of 2.8442 is an indication that respondents do not agree there is a high possibility of an EMR breach. Respondents did not perceive the hospital's EMR system to create privacy issues (3.4026). In general, perceived susceptibility to EMR privacy breach is low.

4.5.2 Perceived Severity of EMR Privacy Breach

This study sought to examine the employees' perception of how severe it is for an EMR privacy breach to occur. The results in Table 6 on the perception of the severity of the EMR privacy breach found that the severity of an EMR privacy breach is high (means >3.5). Respondents indicated that they agree an EMR privacy breach is a serious problem for them (mean = 3.5526), and also agreed that losing EMR system data will lead to a serious problem (mean =3.9351).

4.5.3 Perceived Benefits of EMR Privacy

The study also sought to examine the perceived benefits of EMR privacy policies in the hospital. In table 6, the results reveal that the study participants agree that there are benefits in using EMR privacy policies (mean = 3.5). The highest mean was recorded for the use of privacy policy to ensure EMR system privacy (mean = 3.9351), followed by the use of privacy policy to protect

future EMR system breach (mean = 3.7403). Also, the compliance with EMR privacy policy reduces employees' anxiety (mean = 3.6623).

4.5.4 Perceived Barriers to Compliance with EMR Privacy Policies

The study also sought to investigate some barriers that may hinder the use of EMR privacy policies. The results in table 6 reveal that respondents indicated that they do not agree they experience barriers in complying with EMR privacy policies (mean <3.5). Respondents do not agree EMR privacy policy compliance will interfere with work activities (mean = 2.4079), and are difficult to comply with (mean = 2.2078).

4.5.5 Self-Efficacy in Using EMR Privacy Policies

The study also sought to assess the ability of users to use EMR privacy policies. Self-efficacy measures the level of confidence to comply with privacy policies. In Table 6, the results indicate the perceptions of their self-efficacy to be very high (mean > 3.5). The respondents indicate they are confident to use EMR privacy policies (mean = 4.2468), are confident to recognise potential problems in the EMR system (mean = 4.0260), and are confident to comply with EMR privacy policy even when no one is around (mean = 4.1039).

4.5.6 Cues to Action

The study sought to examine the existence of some activities the hospital management employs to promote the use of EMR privacy policies. The study results in Table 6 generally indicate that respondents do not agree hospital management performs activities that will encourage them to use EMR privacy policies (mean < 3.5). The respondents do not perceive the hospital is doing

very well in using newsletters to encourage the use of the EMR privacy policy (mean = 3.1299). Respondents also perceive that not much effort has been put into sharing alert messages regarding the EMR privacy policy (mean = 2.8831).

4.5.7 Sanction Severity of EMR Privacy Policy Breach

The study sought to assess the severity of sanctions the hospital imposes on employees for breaching EMR privacy policies. A shown in Table 6, the mean results reveal that respondents were of the view that the hospital's sanctions are severe (mean > 3.5). The study reveals that the hospital disciplines employees who breach the EMR privacy policies (mean = 3.970) and may also terminate their appointments when they repeatedly break EMR privacy policies (mean = 3.5325).

4.5.8 Sanction Certainty of EMR Privacy Policy Breach

The study examined the perception of the hospital ensuring that sanctions that are proposed for employees who breach EMR privacy policies are enforced. The study findings in Table 6 reveal that employees perceive the hospital will ensure employees who breach EMR privacy policies are sanctioned (mean > 3.5). Respondents are certain they will be penalized (mean = 3.9221), and formally reprimanded for violation of the EMR privacy policy (mean = 4.0260).

4.6 Relationship between Antecedents of Technology Privacy Compliance and EMR Compliance

4.6.1 Correlation between Study Variables

The Pearson correlation analysis results are presented in Table 7. The analysis revealed that there is a negative relationship between perceived susceptibility and almost all other variables (perceived severity, perceived benefits, self-efficacy, cues to action, sanction severity, sanction certainty, and compliance). However, there is a positive relationship between perceived susceptibility and perceived barriers.

The relationship between the antecedents of technology privacy compliance factors (perceived susceptibility, perceived severity, perceived benefits, perceived barriers, self-efficacy, cues to action, sanction severity, and sanction certainty) and EMR privacy compliance was also analysed. The results indicate that there is a strong positive relationship between self-efficacy (.703), sanction certainty (.546), and EMR compliance. Also, there is a weak positive relationship between perceived severity (.317), perceived benefits (.310), cues to action (.128), sanction severity (.472), and EMR privacy compliance. However, there is a negative relationship between perceived susceptibility (-.199), perceived barrier (-.125), and EMR privacy compliance. These results indicate that self-efficacy and sanction certainty have the strongest positive relationship with EMR compliance.

Table 7: Correlation between the Antecedents of Information Privacy and EMR Privacy Compliance

PerSus	Persus	Persev	PerBen	PerBar	SelfE	Cues	SansSev	SansCer	Comp
Persus	*1*								
Persev	*.100*	1							
Perben	*-.098*	.297**	1						
PerBar	*.500***	.206*	-.111	1					
SelfEff	*-.318***	.334**	.272**	-.219**	1				
CuesA	*-.416***	-.161	.160	-.394**	.163*	1			
SanSev	*-.329***	.191	.139	-.017	.416**	.403**	1		
SancCer	*-.235***	.224**	.409**	-.054	516**	.219**	.632**	1	
Comp	*-.199*	.317**	.310**	-.125	.703**	.128	.472**	.546**	1

Source: Field Study, 2020

4.6.2 Predictors of EMR Privacy Compliance

The regression analysis performed sought to establish the relationship between the antecedents or predictors of compliance with technology privacy policies and actual EMR privacy compliance. The adjusted R square of .545 means that perceived susceptibility, perceived severity, perceived benefits, perceived barriers, self-efficacy, cues to action, sanction severity, and sanction certainty explain 54.5 percent of the variance in EMR compliance (see table 8).

Table 8: Regression Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.754a	.569	.545	.37100

To determine the effect of antecedents of information privacy compliance have on EMR privacy compliance, the study analysed the level of statistical significance for each of the independent variables. The results are presented in Table 9.

Table 9: How the Antecedents of Information Privacy Predict EMR Privacy Compliance

Independent Variables	Std Error	Beta	T	Sig
(Constant)	.358		2.993	.003
Perceived Susceptibility	.044	.045	.641	.522
Perceived Severity	.044	.051	.775	.440
Perceived Benefits	.059	.064	.971	.333
Perceived Barriers	.045	-.045	-.632	.528
Self-Efficacy	**.068**	**.568**	**7.982**	**.000**
Cues to Action	.040	-.057	-.819	.414
Sanction Severity	.064	.106	1.253	.212
Sanction Certainty	.065	.164	1.955	.053

Dependent Variable: EMR Privacy Compliance

From the regression results, self-efficacy has a statistically significant relationship with EMR privacy compliance. A p-value of < 0.05 was used to declare that self-efficacy is statistically significant to EMR privacy compliance and a t-statistic of 1.96 is an indication that the hypotheses proposing a positive and significant relationship between self-efficacy is supported. Though there is a positive relationship between perceived severity, perceived benefits, cues to action, sanction severity, sanction certainty and EMR privacy compliance, the results do not support the hypotheses proposing a statistically significant relationship. The study hypothesised that perceived barrier has a negative relationship with EMR privacy compliance but did not have

a statistically significant relationship with EMR privacy compliance. Table 10 indicates the hypotheses and whether they were supported or not.

Table 10. Decision of Proposed Hypotheses

	Independent Variables	Decision
H1	Perceived Susceptibility → EMR Privacy Compliance	Not Supported
H2	Perceived Severity → EMR Privacy Compliance	Not Supported
H3	Perceived Benefits → EMR Privacy Compliance	Not Supported
H4	Perceived Barriers → EMR Privacy Compliance	Not Supported
H5	Self-Efficacy → EMR Privacy Compliance	Supported
H6	Cues to Action → EMR Privacy Compliance	Not Supported
H7	Sanction Severity → EMR Privacy Compliance	Not Supported
H8	Sanction Certainty → EMR Privacy Compliance	Not Supported

Source: Field Survey, 2020

CHAPTER FIVE

DISCUSSION

5.0 Introduction

This chapter discusses the findings of the study in relation to existing literature. The chapter explains how the study results on the factors affecting EMR privacy compliance are supported or otherwise, by existing studies. The implications of the findings are also discussed.

5.1 Awareness of EMR Privacy Policies

The study found that the level of awareness of EMR privacy policies seems to be high. This is because the responses were very positive in terms of the agreement with statements relating to the various EMR privacy policies. The study considers that the level of privacy policy awareness will be determined by the existence of an EMR privacy policy. Also, the education of employees during orientation when they were recruited, and in-service training on EMR privacy policies may improve the awareness of EMR privacy policies. In line with a study by Rahim et al. (2017), the existence of an EMR privacy policy will lead to employees having knowledge and an awareness of the policy. A high level of awareness of EMR privacy policies among the study participants seems to be higher than that of Rahim et al. (2017), who report that employees indicated they were not aware of EMR privacy policies and therefore relied on their professional code of ethics.

In this study, it was found that the medical centre has an EMR privacy policy, hence, leading to employees indicating a high level of awareness of EMR privacy policies. The implication of this finding is that hospitals that organise orientation, training, and education for their employees on existing EMR privacy policies will lead to employees getting educated about it. Over time, it is

expected that the policies spelled out to employees will become a part of the workplace rules and regulations they follow. On the other hand, the absence of existing EMR policies will lead to employees forming their own professional code of ethics, as explained by Rahim et al. (2017).

5.2 Challenges Affecting EMR Privacy Policy Compliance

The study found that the employees do not perceive that there are many challenges confronting them in adhering to the EMR privacy policies. The responses were an indication that they do not face many challenges in complying with the EMR privacy policies.

On the challenge the EMR could face due to lack of authentication, the study did not find this a major challenge. Keshta and Odeh (2020) propose that the existence of authentication mechanisms such as password logins, digital signatures, etc. is important to protect the privacy of the information on EMR systems. This study finds that the medical centre has in place some form of authentication mechanism. Also, the study results indicate that EMR privacy seems not to allow unauthorised sharing of patients' records. Keshta and Odeh (2020) identified that the situation where there is an unpreventable system for sharing patient information on an EMR system makes the system prone to a privacy breach.

One important issue of concern is the challenge of privacy concerns overriding the use of the EMR patient records. Yan et al. (2012) identified that EMR privacy concerns reduce the level of patient-doctor interaction. The over-emphasis on patient privacy may be a hindrance in the use of the EMR system as employees may be concerned about the consequences, such as sanctions, when a breach occurs. In the case of the medical centre, study participants do not regard the privacy concerns over using the EMR system.

On the complex nature of the EMR system, the study found that respondents did not find it complex to use and understand. Yan et al. (2012) identified that since there are different groups of employees, the lack of computer skills and the unavailable technical support may be potential barriers. A complex EMR system may make it difficult for users to comply with the aspects that concern privacy issues. Another issue of concern identified by Hwang et al. (2012) is the issue of errors in the EMR system. The findings from the study participants indicated that there are low levels of errors in the EMR system. In the medical centre, it is possible that there is support for employees in using the EMR system. Also, the respondents may not perceive the system as complicated due to their high level of self-efficacy as found by the study.

5.3 Level of EMR Privacy Compliance

The level of reported EMR privacy compliance in this current study was found to be high. The results of the level of compliance with the EMR privacy policy is high compared to the study of Kuo et al. (2018); Kuo et al. (2019), Sher et al. (2017). This implies that the hospital employees using the EMR system are complying with the existing privacy policies.

5.4 Factors Affecting EMR Privacy Compliance

The final objective of the study was to determine the factors affecting EMR privacy policy compliance in the case hospital. Using variables drawn from the deterrence theory and the prevention motivation theory, this study sought to ascertain what factors predict EMR privacy compliance behaviour among study participants.

Perceived susceptibility in this study was found to be negatively related to EMR privacy compliance. The study participants did not find EMR privacy as susceptible to breach. This is an

indication that respondents do not perceive that the current EMR system can be breached, thus leading to the question of whether there is awareness on the likely privacy breaches that can occur. It is expected that the general concern of privacy of health information will make employees who use EMR systems to be conscious about the dangers of privacy breaches. A reason that can be attributed to low levels of susceptibility of the EMR privacy system is that users may not be educated enough on the dangers of EMR privacy breach. The hypothesis that perceived susceptibility has a statistically significant relationship with EMR privacy compliance is not supported. This finding is in line with that of Sher et al. (2017), which did not find perceived susceptibility as a predictor of EMR privacy compliance. The finding is also supported by the Humaidi et al.'s study (2014) that perceived susceptibility has an insignificant effect on health information system security policy compliance. This study finds that employees' perception of the likelihood of an EMR privacy breach will not influence them to comply with EMR privacy policies.

Perceived severity was also found to not be a predictor of EMR privacy compliance, even though it has a positive relationship with EMR privacy compliance. Again, Sher et al. (2017) support this finding that a perception of the severity of an EMR privacy breach may not necessarily influence EMR privacy compliance. However, this does not support the finding of Humaidi et al. (2014) that perceived severity is a predictor of health information system policy compliance. This study reveals that employees may assume EMR privacy breaches lead to severe consequences, but this may not influence them to comply with EMR privacy policies.

The study finds that the perceived benefit of using EMR privacy policies is not a predictor of EMR privacy compliance and does not support the hypothesis proposed. This finding is not in

line with that of Sher et al. (2017) that the perceived benefit of using privacy policies is a predictor of EMR privacy compliance. Humaidi et al. (2014) also found that the perceived benefit of using health information system privacy has a significant effect on privacy compliance. These study findings imply that the perception of benefits hospitals gain from EMR privacy policies will not predict EMR privacy compliance.

Perceived barriers and EMR privacy compliance support the assertion made by scholars that barriers to complying with privacy policies will have a negative relationship with EMR privacy compliance (Sher et al. 2017). Also, Humaidi et al.'s (2014) study found that there is a negative relationship between perceived barriers and compliance with health information system privacy compliance. This study supports the literature that the existence of barriers such as difficulty in complying with privacy policies, and interference with work are likely to prevent employees from adhering to EMR privacy policies.

The self-efficacy of employees was found to be a predictor of EMR privacy compliance. This finding implies that EMR users' confidence to follow policies and detect problems with the EMR is very important in influencing compliance to EMR privacy policies. These study findings support that of Sher et al. (2017), that self-efficacy is a predictor of EMR privacy compliance. This result corroborates that of Humaidi et al. (2014), that employees' self-efficacy is a predictor of health information system privacy compliance. Also, a study by Chen et al. (2018) found that self-efficacy is important because it mediates the relationship between sanction severity and compliance with information security policy. The existing literature linking self-efficacy and compliance with information privacy has been confirmed in this study.

Cues to action in this study was found to have a positive relationship with EMR privacy compliance but is not a predictor of EMR privacy compliance. However, Humaidi et al. (2014)

found that cues to action was found to be a predictor of health information system privacy compliance. This study finding also does not confirm the results of Sher et al. (2017), which found that cues to action influences the level of EMR privacy compliance. In this study, it is surprising that cues to action, involving actions taken by hospital management to communicate the existence of EMR privacy policies and encourage users to comply, was not found to be a predictor of compliance. A possible reason could be that the hospital administration focuses on providing information about the need to comply with EMR privacy but does not provide the needed support to ensure actual compliance. The provision of information and encouragement may not be enough, and are not complemented with training sessions, simulations, rewards, supervision, and role plays.

Sanction severity in this study was found to have a positive relationship with EMR privacy compliance but was not a predictor of compliance, thus not supporting the proposed hypothesis. This study's finding is supported by that of Kuo et al. (2017) and Chen et al. (2018), that sanction severity has no direct impact on information security policy compliance. However, the study of Kuo et al. (2019) found that sanction severity is a predictor of EMR privacy compliance. This study finding is therefore not in line with that of Kuo et al. (2019). It implies that in the context of this study, employees' perception of sanction severity does not predict EMR privacy compliance. Drawing from the study of Chen et al. (2018), sanction severity has a relationship with compliance with information security policy when the relationship is mediated by self-efficacy. This means that sanction severity is not adequate to influence compliance to information privacy policy but this relationship can be created when employees have the required skills and confidence to perform compliance behaviours.

The hypothesis that sanction certainty has a positive and significant relationship with EMR privacy compliance is not supported. This means that the perception that there will certainly be sanctions for employees who breach EMR privacy policies will not influence them to comply. This result does not support the finding of Kuo et al. (2017) and Kuo et al. (2019) that sanction certainty is a predictor of EMR privacy compliance. The findings in the studies of Kuo et al., 2017 and Kuo et al., 2019 are an indication that sanction certainty is an important predictor of compliance with EMR privacy policies. The study's result indicating sanction certainty is not a predictor of EMR privacy compliance, is therefore surprising considering how employees may be deterred from engaging in an EMR privacy breach since they strongly perceive that they will be sanctioned. A reason for this may be that though sanctions may exist, the mechanism to detect the occurrence of a breach of EMR privacy may lead to hospital management not detecting when a breach has occurred, thus resulting in sanctions not being enforced.

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

6.0 Introduction

This chapter presents the conclusions and provides some recommendations for policymaking, management of EMR privacy policies, and future research.

6.1 Conclusion of Study

The study sought to achieve four main objectives relating to the level of awareness of EMR privacy policies, the challenges in complying with EMR privacy policies, the level of EMR privacy policy compliance, and the factors that influence EMR privacy compliance. The study found that there is a high level of awareness of EMR privacy policies among hospital employees. A reason ascribed to this was that hospitals that have existing EMR privacy policies and continuously educate EMR users about privacy issues will have employees who are knowledgeable about these policies and not resort to their professional codes of ethics to guide their behaviour.

The study also found that the study participants do not see adherence to EMR privacy policies as a challenge. This study, therefore, concludes that the existence of policies relating to the sharing of information, the use of authentication mechanisms, the support from the information technology department on the use of the EMR system, and a high level of self-efficacy of employees will reduce the challenges in using EMR privacy compliance policies.

The study also identified that the level of compliance of EMR privacy policy among the employees of the hospital is high. However, this might not be the case for other health facilities

in Ghana. The study concludes that hospital has an effective EMR privacy system, thus leading to a higher level of compliance.

Finally, the study identified self-efficacy as the only predictor of EMR privacy policy compliance. The study therefore concludes that the improvement in EMR privacy compliance can be attributed to the skills and competencies of their employees in using the system. In a developing country, self-efficacy in using information technologies is a key issue that predicts the use of these innovative technologies. Also, the existence of policies and sanctions on health information privacy may not be enough to ensure compliance, but it takes the skills, initiative, competency, and personal decision to comply with EMR privacy policies.

6.2 Recommendations

This study provides recommendations for health care management and future research.

6.2.1 Recommendation for Management

This study suggests the following recommendations:

1. Health facilities must intensify education on the need to comply with EMR privacy policies. Also, policymakers such as the Ministry of Health, and the Ministry of Information must educate health professionals on the need to comply with patient information privacy. This will help create awareness on compliance with EMR privacy policies.
2. Management of health institutions must also ensure there is the existence of EMR privacy policies as this prevents the use of personal judgement and professional codes. This also helps to improve the awareness of EMR privacy policies.

3. Ensure there is continuous training for staff on the EMR privacy policies. This will help develop higher self-efficacy for users to possess the skills and be confident in using EMR privacy policies.

6.2.2 Recommendations for Future Research

The following recommendations are proposed for future research:

1. The study of EMR privacy policy compliance must be done in other hospitals including private and public. A study in Ghana with a large sample drawn from many hospitals will lead to generalised results of the level of EMR privacy compliance, and the factors that predict the level of compliance.
2. Future studies can also adopt a qualitative approach to study in-depth the factors affecting EMR privacy compliance.

REFERENCES

Acheampong, E.A., (2012). The state of information and communication technology and health informatics in Ghana. Online Journal of Public Health Informatics. 4 (2).

Adjorlolo, S., & Ellingsen, G. (2013). Readiness assessment for implementation of electronic patient record in Ghana: a case of university of Ghana hospital. *Journal of Health Informatics in Developing Countries*, *7*(2).

Akanbi, M. O., Ocheke, A. N., Agaba, P. A., Daniyam, C. A., Agaba, E. I., Okeke, E. N., & Ukoli, C. O. (2012). Use of electronic health records in sub-Saharan Africa: progress and challenges. *Journal of Medicine in the Tropics*, *14*(1), 1.

Ariffin, N. A. N., Ismail, A. K., & Kadir, I. K. A. (2018). Implementation of electronic medical records in developing countries: challenges & barriers. *Int J Acad Res Prog Educ Dev*, *7*, 187-99.

Bandura, A. (1977). Self-efficacy Toward a Unifying Theory of come expectations. Psychological Review, 84 (2), 191-215.

Barrows Jr, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, *3*(2), 139-148.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, *35*(4), 1017-1042.

Bryman, A., & Bell, E. (2015). Business research methods (Vol. 4th). *Glasgow: Bell & Bain Ltd*.

Bubeck, P., Wouter Botzen, W. J., Laudan, J., Aerts, J. C., & Thieken, A. H. (2018). Insights into flood- coping appraisals of protection motivation theory: Empirical evidence from Germany and France. *Risk Analysis*, *38*(6), 1239-1257.

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049-1060.

College of Health Service. Ethical and Protocol Review Committee (EPRC). http://chs.ug.edu.gh/research/ethical-protocol-review

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422.

El Kettani, A., Housban, S., Serhier, Z., & Othmani, M. B. (2018). Confidentiality in Electronic Health Records Systems: a Review. *Journal of Medical and Surgical Research*, *5*, 551-554.

Forson, P. K., G. Oduro, M. S. Forson, R. Oteng, J. Bonney, C. Oppong, M. Osei-Ampofo et al. The use of open source electronic medical records in an urban ED in Kumasi-Ghana. *African Journal of Emergency Medicine* 3, no. 4 (2013): S14.

Garson, K., & Adams, C. (2008, March). Security and privacy system architecture for an e-hospital environment. In *Proceedings of the 7th symposium on Identity and trust on the Internet* (pp. 122-130).

Graphic Online (2020). Nyaho Medical Center marks 50th anniversary; lays a strong foundation for the future. Retrieved from: https://www.graphic.com.gh/news/general-news/nyaho-medical-centre-marks-50th-anniversary-lays-strong-foundation-for-future.html). Accessed on 3 June, 2021.

Goreva, N., Mishra, S., Draus, P., Bromall, G., & Caputo, D. (2016). A study of the security of electronic medical records utilizing six knowledge categories and subjects demographics. *International Journal of Management & Information Systems (IJMIS)*, *20*(3), 51-58.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & management*, *49*(6), 320-326.

Gyamfi, A., Mensah, K. A., Oduro, G., Donkor, P., & Mock, C. N. (2017). Barriers and facilitators to electronic medical records usage in the Emergency Centre at Komfo Anokye Teaching Hospital, Kumasi-Ghana. *African Journal of Emergency Medicine*, *7*(4), 177-182.

Hair, J. F. (2015). *Essentials of business research methods*. ME Sharpe.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16.

Harman, J. S., Rost, K. M., Harle, C. A., & Cook, R. L. (2012). Electronic medical record availability and primary care depression treatment. *Journal of General Internal Medicine*, *27*(8), 962-967.

Hassidim, A., Korach, T., Shreberk-Hassidim, R., Thomaidou, E., Uzefovsky, F., Ayal, S., & Ariely, D. (2017). Prevalence of sharing access credentials in electronic medical records. *Healthcare informatics research*, *23*(3), 176-182.

Health Information and Management Systems Security Report (2018). Retrieved from: https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Fina_Report.pdf

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106- 125.

Herman, L. B., Flite. C. A., Bond. K., (2012). Electronic Health Records: Privacy confidentiality, and security. AMA Journal of Ethics.

House, D., & Raja, M. K. (2019). Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology*, 1-21.

Huang, L. C., Chu, H. C., Lien, C. Y., Hsiao, C. H., & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine*, *39*(9), 743-750.

Huang, Y. M., Hsieh, M. Y., Chao, H. C., Hung, S. H., & Park, J. H. (2009). Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. *IEEE journal on selected areas in communications*, *27*(4), 400-411.

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014, December). Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model. In *2014 IEEE Conference on E-Learning, e-Management and E-Services* (pp. 30-35). IEEE.

Hwang, H. G., Han, H. E., Kuo, K. M., & Liu, C. F. (2012). The differing privacy concerns regarding exchanging electronic medical records of internet users in Taiwan. *Journal of Medical Systems*, *36*(6), 3783-3793.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*.

Kim, Y. (2013). Differences in physical activity and perceived benefits and barriers among normal weight, overweight, and obese adolescents. *Perceptual and Motor Skills*, *116*(3), 981-991.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607-610.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of medical systems*, *41*(8), 127.

Kuo, K. M., Chen, Y. C., Talley, P. C., & Huang, C. H. (2018). Continuance compliance of privacy policy of electronic medical records: the roles of both motivation and habit. *BMC medical informatics and decision making*, *18*(1), 135.

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), 254.

Kuo, K. M., Talley, P. C., Hung, M. C., & Chen, Y. L. (2017). A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *Journal of medical systems*, *41*(12), 198.

Likourezos, A., Chalfin, D. B., Murphy, D. G., Sommer, B., Darcy, K., & Davidson, S. J. (2004). Physician and nurse satisfaction with an electronic medical record system. *The Journal of Emergency Medicine*, *27*(4), 419-424.

Masrom, M., & Rahimly, A. (2015). Overview of data security issues in hospital information systems. *Pacific Asia Journal of the Association for Information Systems*, *7*(4).

Miller, R. H., Sim, I., & Newman, J. (2004). Electronic medical records in solo/small groups: a qualitative study of physician user types. *Studies in health technology and informatics*, *107*(1), 658-662.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

O'Donnell, A., Kaner, E., Shaw, C., & Haighton, C. (2018). Primary care physicians' attitudes to the adoption of electronic medical records: a systematic review and evidence synthesis using the clinical adoption framework. *BMC medical informatics and decision making*, *18*(1), 101.

Ohemeng-Dapaah, S., Pronyk, P., Akosa, E., Nemser, B., & Kanter, A. S. (2010). Combining vital events registration, verbal autopsy and electronic medical records in rural Ghana for improved health services delivery. *Studies in health technology and informatics*, *160*, 416- 420.

Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*, *45*(1), 22.

Pangalos, G., Gritzalis, D., Khair, M., & Bozios, L. (1995). Improving the security of medical database systems. In *Information Security—the Next Decade* (pp. 11-25). Springer, Boston, MA.

Pearce, C., & Bainbridge, M. (2014). A personally controlled electronic health record for Australia. *Journal of the American Medical Informatics Association*, *21*(4), 707-713.

Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International journal of medical informatics*, *80*(2), 94-101.

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems*, *21*.

Rahim, F. A., Ismail, Z., & Samy, G. N. (2016). A review on influential factors of information privacy concerns in the use of electronic medical records. *International Journal of Computer Science and Information Security*, *14*(7), 17.

Rahim, F. A., Ismail, Z., & Samy, G. N. (2017). Healthcare employees' perception on information privacy concerns. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

Reis, Z. S. N., Maia, T. A., Marcolino, M. S., Becerra-Posada, F., Novillo-Ortiz, D., & Ribeiro, A. L. P. (2017). Is there evidence of cost benefits of electronic medical records, standards, or interoperability in hospital information systems? Overview of systematic reviews. *JMIR Medical Informatics*, *5*(3), e26.

Renaud, K., & Dupuis, M. (2019, September). Cyber security fear appeals: unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop* (pp. 42-56).

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

Samy, G. N., Ahmad, R., & Ismail, Z. (2010, August). A framework for integrated risk management process using survival analysis approach in information security. In *2010 Sixth International Conference on Information Assurance and Security* (pp. 185-190).

Saunders, M. L., & Lewis, P. & Thornhill, A. (2009). *Research methods for business students*, *4*th Edition.

Sher, M. L., Talley, P. C., Yang, C. W., & Kuo, K. M. (2017). Compliance with electronic medical records privacy policy: An empirical investigation of hospital information

technology staff. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, *54*.

Sikhondze, N. C., & Erasmus, L. (2016). Electronic medical records: a developing and developed country analysis.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64-71.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security*.

Taddeo, M. (2018). The limits of deterrence theory in cyberspace. *Philosophy & Technology*, *31*(3), 339-355.

Tamariz, L., Medina, H., Suarez, M., Seo, D., & Palacio, A. (2018). Linking census data with electronic medical records for clinical research: A systematic review. *Journal of Economic and Social Measurement*, *43*(1-2), 105-118.

Thompson, N., McGill, T. J., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391.

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*(6), 1265-1284.

Tsai, F. S. (2010). Security issues in e-healthcare. *Journal of Medical and Biological Engineering*, *30*(4), 209-214.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Wang, J., Zhang, Z., Xu, K., Yin, Y., & Guo, P. (2013). A research on security and privacy issues for patient related data in medical organization system. *International Journal of Security and Its Applications*, *7*(4), 287-298.

Warner, M., & Wang, V. (2019). Self-censorship in social networking sites (SNSs)–privacy concerns, privacy awareness, perceived vulnerability and information management. *Journal of Information, Communication and Ethics in Society*.

Yan, H., Gardner, R., & Baier, R. (2012). Beyond the focus group: understanding physicians' barriers to electronic medical records. *The Joint Commission Journal on Quality and Patient Safety*, *38*(4), 184-AP1.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, *43*(3), 389-418.

APPENDIX: SURVEY QUESTIONNAIRE

University of Ghana

Dear Respondent

This survey is to examine the compliance of Hospital employees to the privacy guidelines in using the electronic medical records (EMR). The researcher is collecting this data in fulfilment of attainment of Masters of Public Health. Your responses will be for academic purposes. You are also assured of confidentiality and anonymity.

Section A: Demography Profile of Respondent

For the following questions by ticking (√) in the box

1. Gender of Respondent Male ( ) Female ( )
2. Indicate your age ……
3. Role in Hospital Nurse ( ) Pharmacist ( ) Medical Surgeon/ Doctor ( ) Laboratory Technicians ( ) Administrator ( )
4. Number of years working at the Hospital …….

Section B: Awareness of EMR Compliance Policies

5. The hospital discloses the way health data about patients is collected, processed, and used

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

6. The hospital has clear and conspicuous guidelines on the disclosure of health information of patients

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

7. I am very aware about how personal health information will be used

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

8. The hospital does not use personal information for any purpose unless it has been authorized

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

9. The hospital does not share personal information with other hospitals unless it has been authorised

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

10. The hospital has a policy that all health information will not be removed by any employee.

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

11. The hospital has a policy that patient's identifiable information must not be disclosed.

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

12. The hospital has a policy that medical records can only be reproduced with approval from Medical Director.

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

EMR Privacy Challenges

Indicate the challenges you face in using EMR privacy policies. Indicate your response by ticking.

13. The EMR system used by the hospital does not have authentication features such as biometric

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

14. The EMR system allows employees to share information to unauthorised third parties

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

15. The patients privacy (preference with regard to EMR), override EMR implementation in the work I do

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

16. I find it very difficult to enter data in EMR

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

17. The EMR system usually fails when inputting and retrieving patient information

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

18. The EMR privacy policy is complex to understand and use

Strongly Disagree ( ) Disagree ( ) Not Sure/Neutral ( ) Agree ( ) Strongly Agree ( )

Section C: Item Scales on Factors Determining EMR Privacy compliance and Level of

For each of the questions, indicate your perception by ticking (√) on a scale of 1 (strongly disagree), 2 (disagree), 3 (neutral), 4 (agree) and 5 (strongly agree).

	Perceived Susceptibility	**1**	**2**	**3**	**4**	**5**
19	The chances that EMR privacy may be breached is high					
20	There is a strong probability that EMR privacy breaches may lead to privacy issues					
21	The use of EMR is likely to cause privacy problems					
	Perceived Severity					
22	Having EMR privacy breaches is a severe problem for me					
23	Losing EMR data is a severe problem for me					
	Perceived benefits					
24	Complying with the privacy policy prevents future EMR privacy breaches					
25	The privacy policy can ensure EMR privacy					
26	I am less anxious about EMR privacy breaches if I can comply with the privacy policy					
	Perceived Barriers					
27	Complying with the privacy policy may interfere with many work activities					
28	Complying with the privacy policy is difficult					
	Self – Efficacy					

29	I am confident that I can comply with the privacy policy	1	2	3	4	5
30	I am confident that I can recognise the potential problems of violating EMR privacy					
31	I am confident that I can comply with the privacy policy even if there is no one around to help me					
	Cues to Action					
32	My hospital regularly distributes newsletters or articles concerning the protection of EMR privacy					
33	My hospital regularly organizes talks on EMR privacy					
36	My hospital regularly sends out alert messages regarding EMR privacy					
	Sanction Severity					
37	My hospital disciplines employees who break EMR privacy rules					
38	My hospital terminates employees who repeatedly break EMR privacy rules					
	Sanction Certainty					
39	If I don't follow EMR privacy policies, I will be penalised					
40	I would be formally reprimanded if management learned that I had violated EMR privacy policy					
	Compliance to Protect EMR Privacy					
41	I follow privacy policies of the hospital					
42	I continue to protect EMR privacy					
43	I am certain that I follow the hospital EMR policies					

Thank you