International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Assessing Security Mechanisms for Protecting Patient Health Information at the Berekum Holy Family Hospital

Gideon Danso[1], Mr. Daniel K. K. Quansah[2]

[1,2]University of Cape Coast

Abstract

The security and privacy of patient health information remains a major concern for most health facilities in recent times where patient data can easily be shared between institutions. Patient health information is considered by many as one of the most confidential of all types of personal information (Calvillo-Arbizu *et al*, 2014). Protecting this confidentiality is therefore essential if the privacy of subjects of care is to be maintained. Securing patient health information involves security mechanisms versus any party not authorized to access the data. Security and privacy in electronic health records systems can be seriously threatened by hackers, viruses, and worms (Luethi *et al*, 2009). According to studies carried out in several countries, concerns regarding data security and privacy have appeared. A recent study estimated that each year there are 25 million compelled authorizations for the disclosure of health records in the United States (Mark *et al*, 2007). In order to prevent these concerns, organizations such as the Certification Commission for Healthcare Information Technology (CCHIT) offer a certified program which covers a rigorous inspection of, among other things, security aspects based on existing standards, which is relevant for the United States. There is a real concern about both people's and entities' access levels to patient health information.

A patients' health information might be expose and accessible from several networks or devices in the health facility. (by visiting different doctors' offices, departments, providers, etc.) (Fernández-Alemán *et al*, 2013). Security defects in some of these areas could cause the disclosure of information to unauthorized persons or companies. Patient health information therefore need protection against manipulations, unauthorized accesses and abuses, which includes taking into account training on the security techniques, encryption of health information, user-authentication and authorization (Mellado *et al*, 2010). Patient health information might be tempered with to the extent that administrative staff could for example access information without the patient's explicit consent in a financial and billing reviews. According to the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, patients' privacy violations and breaches are becoming more expensive than ever (Jorge *et al*, 2012). Therefore, there is the need to assess the various security mechanisms for protecting patient health information from unauthorized access to improve the quality of care delivery.

Keywords: Security, Security Mechanisms, Patient Health Information

Chapter One

PROBLEM STATEMENT

Threats to the security of patient health information have dramatically increased recently. For instance, during the years 2008 and 2009, just in hospitals, almost 1.5 million names were publicly disclosed due to data breaches (Samy *et al*, 2009). Thus, the safety, privacy, and health of patients are put at risk by the any means of storage of patient health information. Basically, both unintentional incidents and intentional threats pose a serious risk to the security of health information, deterring healthcare professionals from using them in the future (Stasi *et al*, 2008). Theft of patients' health credentials to obtain medical treatment, services may have long term economic and health consequences on patients, since these false changes made to their medical records and histories can remain undiscovered for years (Agaku *et al*, 2014).

According to Appari and Johnson (2010), victims of medical identity theft may receive inappropriate medical treatment (including potentially harmful drug prescription), reduce their health insurance benefits, or fail pre-employment medical screening examinations because of the presence of wrong health diagnosis in their health records. Assessment of potential risks, particularly in the domain of healthcare information systems, is prompted by the absence of effective security measures in maintaining the confidentiality, integrity, and availability aspects. In addition, healthcare organizations in the public and private sectors, need to pay close attention to security measures that are poorly organized and security risk analysis methods that are not sufficiently recognized (Appari *et al*, 2010).

SIGNIFICANCE

According to Shreepee Singh (Member of the World Economic Forum Early Career Program, World Economic Forum), effective security mechanisms will ensure maximum protection of patient health information in the health facility. This helps health workers to work with accurate information about patients' health problems to improve the quality of healthcare. Protection of patient health information by means of secured mechanisms prevent any data leakage which can cause serious harm to the patient.

Scope of the Study

In this Study, one health facilities in Berekum Municipality will be involved. Thus, Berekum Holy Family Hospital. The targeted respondents are strictly Healthcare professionals and the Administrative workers in the above listed hospitals. This will help generate enough data to the support the main objective of this research work.

Main Objective

The main objective of this study is to explore the various security mechanisms in place at the Berekum Holy Family Hospital to the protection of patient health information.

Specific Objectives

1. To find out the physical security mechanisms for protecting patient health information in the health facility.
2. To explore the technical security mechanisms for protecting patient health information in the health facility.
3. To investigate the administrative security measures for protecting patient health information in the health facility.

Research Questions

1. What are the physical security mechanisms for protecting patient health information in the health facility?

2. What are the technical security mechanisms for protecting patient health information in the health facility?
3. What are the administrative security measures for protecting patient health information in the health facility?

Study Organization

This study is in five chapters. Chapter One is the introduction which comprises of the background of the study, problem statement, main objective, specific objectives, research questions, significance of the study, scope and organization. Chapter Two emphasize on the review of various related literature. Chapter Three deals with the research methods such as the research design, population target and sampling procedures and data analysis technique. Chapter Four makes details on results and discussion of the research findings and Chapter Five looks at the conclusion and recommendation of the research work.

CHAPTER TWO
LITERATURE REVIEW

1. The Physical Security Mechanisms for Protecting Patient Health Information

Physical security includes those elements of protective security that are concerned with physical safeguards for the protection of assets (Draper *et al*, 2017).

- **Closed-Circuit Television (CCTV) Cameras**

The protection of patient health information was found to include several actions in addition to the use of CCTV cameras. Hospital's health information department and the IT room were not the only places under CCTV surveillance. It also kept a close watch on the healthcare professionals and the patients (Desai, 2010).

Goldstein (2021) suggested that, in cases where hospital staff restrooms and changing areas are prohibited from being caught on camera by surveillance cameras due to hospital policy and contractual agreements, an advisable, watchful hospital security officer will request clearance or permission from his or her top management and the hospital administration. According to Fennelly L. (2016), CCTV Camera with recording capability serves as a deterrent flexibility of recording, permanent record, reduced insurance rates, deterrent for crime, multiple angles of view, night view and works in low light at the healthcare facility. With this, intruders who illegal access patient health records are easily caught on camera and arrested.

- **Alarm Systems**

Alarm systems for healthcare facilities are essential for the effective, secure, and protection of patient health information (Fennelly, 2016). Alarms are used to alert healthcare professionals to potential deviations from the norm in healthcare services so that healthcare facility management can take the necessary corrective measures. (Goel *et al*, 2017). Alarms are one of the various layers of protection of patient health information that are used for a facility. They serve as an alert system to draw attention to an entry of intruders into the health information department (Sandland-Taylor 2018). In essence, they enhance the detecting process. Alarms, in any case, only work if there is a response. A response to an alarm is required. Without timely response, an alarm system is ineffective. (Fennelly, 2016).

According to Sandland-Taylor (2018), information systems, radiological equipment, and other electrical devices all face problems. The chance of fire is likely to increase as a result of these devices and equipment

and the heavy use of power. The loss of valuable equipment and patient health information might be huge when a fire breaks out. Hence, fire alarm systems help in curbing fore outbreak to protect health information and clinical information systems.

- **RFID (Radio-Frequency Identification) Detectors Installed on the Machine**

Sharon Shea, (Executive Editor of TechTarget) explains RFID as "a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person". The system hardware consists of RFID electronic tickets,

RFID readers, computer terminals, optical networks, computer servers and site controllers (Farooq *et al*, 2014). Electronic ticket contains the S-DES encrypted form of data including scenic region number, scenic spot number, ticket type, ticket date, site number, serial number and check bit. The RFID reader at the site reads the data inside the e-ticket and transmits it to the computer terminal and servers though the network. The data is decrypted at the terminal and its authenticity is verified (Farooq *et al*, 2014).

Turcu and Popa (2009) wrote that RFID-based systems are used in hospitals to provide positive patient identification (PPI). We recommend extending patient identification beyond of hospital and national borders. As a result, the open-loop RFID application that powers our RFID-based software solution will operate with hospitals all around the world. It will be necessary to implement new or common standards (like HL7) for this system. In order to support an international health information infrastructure, particularly for emergency healthcare, standards are required.

RFID is a constantly developing technology that transfers and collects data using radio waves. It can efficiently collect data without user intervention. The next-generation solution for automatic data collection and asset tracking is believed to be RFID (Yao *et al*, 2010).

2. The Technical Security Mechanisms for Protecting Patient Health Information

According to Wilnellys Moore and Sarah Frye, "technical security refers to control of access to computer systems and protection of electronically transmitted Protected Health Information. Technical security addresses who has access to electronic medical records and how a person may access, view and use such records".

- **Access Control Mechanisms (Authentication, Identification and Authorization)**

Andriole, K. P. (2014) explains some access control mechanism as follows;

Identification: Identification asks a user who they are.

Authentication: It is process of verifying the identity of a person by a computer system, or assuring that a computer program is a trusted one. Also authentication verifies the identity of health workers by the Electronic health records or Health information system and can be accomplished using log-ins or usernames and passwords, digital certificates, smartcards.

Authorization controls that restrict system access to authorized users only.

Functions for authentication and authorization are crucial for security. When it comes to electronic health records, they get much more complicated. Role-based authorization has developed into a crucial idea for hospitals to manage security rules (Luethi *et al*, 2009).

There are several ways that may be used to authenticate a healthcare professional in accessing patient health information during healthcare delivery. These include, password, passphrase, dumb card and smart

card. Each health professional has his or her unique user identification of which they can be tracked by the time and type of information they accessed in the electronic health records. (Al-Nayadi *et al*, 2007). This will prevent unauthorized individuals from getting access to the patient health information by accessing the Electronic health records.

- **Biometric Security Systems**

The growth of interconnected health information networks raises several major issues of concern. This include identification of patients and physicians, privacy and confidentiality protection (Flores *et al*, 2010). Due to their capacity to offer a system for the individual identity of a person to be uniquely verified, biometric technologies have been suggested as a potential technological solution to these problems (Flores *et al*, 2010). Biometrics are mostly used in security systems for user identification or verification. Identification is typically the more challenging of the two purposes because a system needs to go through a database of users who have signed up in order to locate a match (a one-to-many search) (Liu *et al*, 2015). Biometrics like face, voice, retina, fingerprint, and iris recognition have shown to be more effective in identifying healthcare professionals in the health facilities. However, breach of confidentiality must be resistant against biometric authentication methods. Additionally, biometric security control offers efficient system security and the implementation of a secure biometric template protection system, particularly for health information systems where a patient's privacy and security are of greatest priority (Abdul *et al*, 2017).

- **Encryption of Patient Health Information**

Encryption protects patient health information in transmission and on mobile devices, and is often a limit on liability for breach purposes under HIPAA (Morse *et al*, 2011). Data encryption is a key component of a healthcare facilities' cyber security technique to protect patient health information and meet HIPAA compliance. Health data encryption occurs when there is a conversion of data into encoded and unreadable text in order to make the information inaccessible without a decryption key. Encryption helps protect patient health information when it's transmitted from one user to another (Chand *et al*, 2021).

Healthcare devices transmit data to the cloud across an insecure public area network. During transmission, an intruder could read and modify the data in the network. However, a specific method for the data protection with wearable device has not yet been established due to the variation, various characteristics, and small size of smart wearable devices. Therefore, an access control system based on encryption was required to preserve the security of patient health data (Khandare *et al*, 2019).

Stine and Dang (2011) suggested that if there is a chance that an unauthorized individual could access any patient health information that has to be kept confidential, it should be encrypted. In the healthcare environment, data at rest must be frequently encrypted. To guarantee data confidentiality, all copies of the medical records and patient data, including those in backup and storage settings, should likewise be encrypted (Stine *et al*, 2011). With the help of proper encryption technique, we can protect the patient health information.

- **Firewalls**

Fennelly L. (2016) suggested that in order to prevent unwanted data traffic from an outside network, routers operate with firewalls. Both hardware and software can be used to configure firewalls. A firewall

should be used to connect security systems to any other networks. Otherwise, the facility won't be secure and neither will the security system. Malicious data is prevented by firewalls.

According to Collier (2014), implementing firewalls to safeguard the information technology system of healthcare businesses was the security measure that was most frequently addressed. Despite the fact that firewalls are known to be expensive and that their cost can vary depending on the size and complexity of the healthcare organization, they have shown to be quite effective at protecting network and the patient health information they store.

To safeguard the organization against a range of threats to the patient health data the network contains, a number of different types of firewalls can be established both internally and outside (Liu *et al*, 2015). A packet filtering firewall is the first form of firewall that can be used by a healthcare organization. A packet filtering firewall system keeps outside feeds from accessing the organization's network by filtering internal electronic feeds (Liu *et al*, 2015). Status inspection firewalls fall under a second category of firewalls. While status inspection firewalls are similar to packet filtering firewalls in that they can verify and establish the correlation between incoming electronic feeds and electronic feeds that have already been filtered, status inspection firewalls are significantly more dynamic than packet filtering firewalls (Liu *et al*, 2015). The application level gateway falls under the third category of firewalls. This kind of firewall prevents outside access to the health organization's internal network by allowing access to external network connections through the gateway. Application level gateways have been successful in keeping hackers from directly accessing EHRs to access patient health information. (Liu *et al*, 2015).

Before implementing any kind of firewall, an organization must perform a thorough strategic assessment, financial analysis, and threat analysis of both internal and external threats. The healthcare institution's information system as a whole and the security of patients' electronic health records may both suffer when it fails to do so (Fennelly, 2016).

3. The Administrative Safeguards for Protecting Patient Health Information

The Security Rule defines administrative safeguards as, “administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

- **Train Employees to Recognize Potential Attacks**

According to Samikshan Sarkar (a technical writer), employees are still adjusting to health care information technology adoption because it is still in its early phases. To protect the security of patient health information, policies and practices must be updated to account for the digitalization of patient records. But without enough training, just implementing new policies is limited. Your employees' decision-making and ability to identify potential security dangers can both benefit from security awareness training. This kind of training can urge users to use the appropriate precautions when handling patient health information and data. It's crucial to instruct both new and experienced personnel on the most recent data security practices.

In addition, there should be periodic retraining to healthcare professionals whenever environmental or operational changes affect the security of electronic protected health information (EPHI). These changes may include a new or updated policies and procedures, new or upgraded software or hardware, new security technology or even changes in the Security Rule (Trinckes *et al*, 2012).

- **Implement Policies and Procedures to Manage Patient Health Information Security**

In order to adhere to national norms and standards, the security of health information must be taken into consideration on a high level. If this were the case, many hospitals may adhere to a standard guideline to increase information security in their facilities (Farzandipour *et al*, 2010). The management and the use of patient medical records within the health information system must comply to defined security regulations. As soon as data is entered at the patient **WPAN**, the policies should work to safeguard its integrity and confidentiality (Misic *et al*, 2007). Also this implemented policies and procedures will help to prevent, detect, contain and correct security violations. Such policies may include procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations. This will prevent exposure of patient health records and other administrative vital document to the public (Farzandipour *et al*, 2010)

- **Perform Annual Risk Assessments**

It is important for a covered healthcare organization to be aware of whether the security policies and practices it employs continue to appropriately safeguard patient health information. Therefore, the administration of the healthcare facility should perform annual risk assessment to predict the risk of new and current healthcare information technology. It will reduce the unintended results of new applications (Yucel *et al*, 2012). This assessment also seeks to enhance the technical quality and transparency of the health data and the ensuing public policy and HIPAA regulation (Faustman *et al*, 2008).
With this, monitoring and evaluation is practiced which ensure the patient health information is protected.

- **Duplication of Critical Hardware**

Healthcare facilities use information systems to access patient health information. These systems have hardware components which might be tempered with. It is a key factor to make duplication of such critical components or functions of a system with the intention of increasing reliability (Trinckes *et al*, 2012).
This is usually in the form of a backup or fail-safe, or to improve actual performance of the system. Hard drives are the most common form of hardware redundancy. A simple set up would have a primary drive copied on a regular basis to a backup drive. If the primary drive fails, the secondary drive containing all the patient information could be slotted in. The only health information or data lost will be anything produced since the last time the files were copied. Hardware redundancy may be the only way to improve the dependability of the health information system (Dubrova, 2013).

CHAPTER THREE
METHODOLOGY

This chapter involves the design of the study, population target, sampling procedures, data analysis, the sampling technique, research instrument, sample size, pretesting and review of questionnaire and the limitations of the study.

Research Design

This study is at the healthcare facility of which data was collected from healthcare professionals. The cross-sectional method was adopted for the study. Data was collected from a cross section of respondents at a single moment in time for an institutional based cross-sectional study. Data from a cross-sectional study conducted at a healthcare facility was utilized to evaluate and detect patterns of relationship among the variables. Data was collected through face-to-face administration of a questionnaires to healthcare

professionals, as well as an observation at the chosen health facility. The respondents' demographics information, such as age, sex, religion and educational level, were collected as part of the study. In addition, details on security mechanisms for protecting patient health information were collected.

Study Site

The Study was carried out at the Berekum Holy Family Hospital at the Bono Region of Ghana. The Berekum Holy Family Hospital has about 323 as the total workforce.

Population of the Study

All the healthcare professionals that work with the patient health information constituted the population of the study.

Sample & Sampling Technique

The study was delimited to only Healthcare professionals in the health facility who work with patient health information due to lack of time and resources. A simple random sampling technique was used to select participants. Each unit of population had an equal chance of inclusion in the sample. The sample for this study was made up of 100 healthcare professionals.

Sample Size Determination

By using the StatCalc function in Epi-Info software version 1.4.3 and at a confidence level of 85%, a sample size of 100 was selected from the population 323 which was obtained from the 2022 profile

Instrument for data collection

A well-organized and structured hardcopy self-completion questionnaires was the instrument for the collection of data.

Data Collection Procedures

The principal investigator personally visited the sample and distributed the questionnaires among the participants. Questions within the self-administered questionnaires were clear, simple yet understandable and protects participants' confidentiality. Difficult terms were first explained and then the participants were asked to give appropriate and exact response without any hesitation and free of bias. A total of 100 questionnaires were distributed and 100 i.e., 100% responses were received. In this way data was collected from the participants.

Reliability and Validity

The study's questionnaire was pre-tested at Berekum Holy Family Hospital. The questionnaire was modified based on Input from the pre-test to guarantee its applicability for the study. To eliminate inconsistencies and biases, it was critical that they were familiar with the questionnaire and the usual style of administering it.

Method of Data Analysis

SPSS statistical software version 22 was used for the entry and the analysis of data. The use of exact numbers, frequency of responses, and percentage was emphasized for a full analysis of the data.

CHAPTER FOUR
RESULTS, ANALYSIS AND DISCUSSION

The main focus of the study was to assess the security mechanisms for protecting patient health information at the hospital. This chapter is categorized into three main sections in accordance with the research questions as well as information sought from respondents. The chapter comprises the presentation of results, analysis and discussion of findings of the study. These are presented according to the three main research questions raised to guide the study. Analysis were done using frequencies and percentages.

Demographic Data

Below is the presentation of the findings based on the objectives set for the study. The table 4.1 below is the socio-demographic attributes of respondents. It contained six questions such as the age, gender, job title, work experience, religion and marital status. Age was coded as (20-24 years = 1, 25-29 years = 2, 30-34 years = 3 and 35 years and above = 4), gender was coded as (Male = 1 and Female = 2), job title was coded as (nurse = 1, midwife = 2, health information officer = 3, dentist = 4, optometrist = 5, anesthetist = 6, nutritionist = 7, dietitian = 8, pediatric doctor = 9 nurse assistance = 10, medical laboratory scientist = 11, clinical pharmacist = 12, sonographer = 13, radiographer = 14, chief health information officer = 15, physician assistant = 16, work experience in years was coded as (less than 5 years = 1, 5-10 years = 2 and above 10 years = 3), religion was coded as (Christian = 1, Muslim = 2 and Others = 3) and marital status was coded as (Single = 1, Married = 2, Divorced = 3, Widowed = 4, Others = 5).

From the table 4.1 below, there was a total of 100 respondents involved in the research, a greater portion of 45 (45%) respondents were within the ages of 20 to 24 years, 34 (34%) of the respondents were within the ages of 25 to 29 years, 11 (11%) of the respondents were within the ages of 30 to 34 years and the remaining 10 (10%) were 35 years and above. 48 (48 %) of the respondents were males and the remaining 52 (52%) were females.

17 respondents representing 17% of the 100 respondents were nurses, 5 (5%) were midwives, 16 (16%) were health information officers, 5 (5%) of the respondents were dentists, 7 (7%) were optometrists, 7 (7%) anesthetists, 5 (5%) were nutritionists, 6 (6%) were dieticians, 5 (5%) were pediatric doctors, 5 (5%) were nurse assistants, 7 (7%) were medical laboratory scientist, 4 (4%) were clinical pharmacist, 5 (5%) were sonographers, 2 (2%) were radiographers, 1 (1%) was chief health information officer and the remaining 3 (3%) were physician assistants. 75 (75%) of the respondents had five or less years (0-5) of work experience, 17 (17%) had six to ten years (6-10) of work experience and the remaining 9 (9%) had more than ten years of work experience.

Also, majority (65%) of the respondents were Christians, 24 (24%) were Muslims and the remaining 1 (1%) were others as in other religion. As for the marital status, 59 (59%) of the respondents were single, 39 (39%) were married and the remaining 2 (2%) were divorced.

Table 4.1 Socio-demographic Characteristics of the respondents

Variable	**Frequency (N=100)**	**Percentage (%)**
Age (Years)		
20 - 24	45	45.0
25 - 29	34	34.0
30 - 34	11	11.0
>= 35	10	10.0
Gender		
Male	48	48.0
Female	52	52.0
Job Title		
Nurse	17	17.0
Midwife	5	5.0
Health Information officer	16	16.0

Dentist	5	5.0
Optometrist	7	7.0
Anesthetist	7	7.0
Nutritionist	5	5.0
Dietitian	6	6.0
Pediatric Doctor	5	6.0
Nurse Assistance	5	5.0
Medical Laboratory Scientist	7	7.0
Pharmacist	4	4.0
Sonographer	5	5.0
Radiographer	2	2.0
Chief Health Information Officer	1	1.0
Physician Assistance	3	3.0
Work Experience in Years		
0 - 5	74	74.0
6 - 10	17	17.0
>10	9	9.0
Religion		
Christian	75	75.0
Muslim	24	24.0
Others	1	1.0
Marital Status		
Single	59	59.0
Married	39	39.0
Divorced	2	2.0

Table 4.2 below illustrates the responses of healthcare professionals on the physical security mechanisms for protecting patient health information. The healthcare professionals responded to five questions. All the questions were presented in Table 4.2. The table below was designed to seek the view of healthcare professionals at Berekum Holy Family Hospital on the physical security mechanisms for protecting patient health information.

Table 4.2 shows 89 respondents representing 89% said yes to the question that the facility have a man guard force, and 11% or 11 respondents said no to the same question. Out of the 100 respondents, 90 respondents representing 90% said yes to the question that the facility deals in staff ID, 10 respondents representing 10% responded negatively to the same question.

The Table 4.2 also reveals that 97 respondents representing 97% responded positively to the question that the guards check healthcare providers' ID, 3 respondents representing 3% responded negatively to the same question. Also, 88 respondents representing 88% said yes to the question that the facility have alarm systems, the remaining 12 respondents representing 12% said no to the same question.

13 respondents representing 13% responded yes to the question that the electronic health record system have RFID (Radio-Frequency Identification) detectors installed on them, the remaining 87% said no to the same question. 88 respondents representing 88% affirmed that locks are changed when keys get lost, 12 respondents representing 12% responded negatively to the same question.
Lastly, 9 out of 100 respondents representing 9% said yes to the question that facility use CCTV cameras at areas housing patient health data and information systems; the remaining 91% or 91 respondents said no to the same question.

Table 4.2: Responses on assessing the physical security mechanisms for protecting patient health information at the Berekum Holy Family Hospital

STATEMENT	YES n (%)	NO n (%)	TOTAL n (%)
7. Does the facility have a Man Guard force?	89 (89.0%)	11 (11.0%)	100 (100.0%)
8. Does the facility deals in staff ID?	90 (90.0%)	10 (10.0%)	100 (100.0%)
9. Do guards check healthcare providers ID?	97 (97.0%)	3 (3.0%)	100 (100.0%)
10. Does the facility have alarm systems?	88 (88.0%)	12 (12.0%)	100 (100.0%)
11. Does the electronic health record system have RFID (Radio-Frequency Identification) detectors installed on them?	13 (13.0%)	87 (87.0%)	100 (100.0%)
12. Are locks changed when keys lost?	88 (88.0%)	12 (12.0%)	100 (100.0%)
13. Does the facility use CCTV cameras at areas housing patient health data and information systems?	9 (9.0%)	91 (91.0%)	100 (100.0%)

From **Table 4.3** below, there was a total of 100 respondents involved in the research, a greater portion, 84 respondents representing (84.0%) of the respondents said yes to the item that they use electronic health record systems in service delivery and 16.0% or 16 respondents said no to the same item.
From the 100 respondents, 14 respondents representing 14.0% said yes to the question that they can access the Electronic health record system during non-working hours, the other 86 respondents representing 86.0% responded to the same question saying they can't access the electronic health record system during non-working hours.
The table 4.3 also reveals that 34 respondents representing 34.0% responded positively to the statement that your firewalls, information systems and security mechanisms are securely configured, 66 respondents disagreed with the same statement.
Lastly, 79 out of 100 respondents representing 79.0% said yes to the question that all sensitive and confidential information stored on your organization's databases, servers and data files encrypted; the remaining 21.0% or 21 respondents also said that all sensitive and confidential information stored on your organization's databases, servers and data files encrypted.

Table 4.3: Responses on assessing the technical security mechanisms for protecting patient health information at the Berekum Holy Family Hospital

STATEMENT	YES n (%)	NO n (%)	TOTAL n (%)
14. Do you use Electronic health record system in service delivery?	84 (84.0%)	16 (16.0%)	100 (100.0%)

15. Do you log into the system with a unique Authentication (User-Password or Passphrase)?	84 (84.0%)	16 (16.0%)	100 (100.0%)
16. Can you access the Electronic health record system during non-working hours?	15 (15.0%)	85 (85.0%)	100 (100.0%)
17. Are your firewalls, information systems and security mechanisms securely configured? Tick "No", if your systems are configured using factory default settings.	34 (34.0%)	66 (66.0%)	100 (100.0%)
18. Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted?	79 (79.0%)	21 (21.0%)	100 (100.0%)

The **Tables,** charts and graphs below illustrates the responses of healthcare professionals on the administrative security measures for protecting patient health information in the health facility. The healthcare professionals responded to six questions. All the questions are presented in a table as well as in graphs or charts.

The table 4.4 shows that 65 respondents representing 65.0% strongly agree to the item that Employees should be given security awareness training on a regular basis and 35% or 35 respondents agreed to the same item. Meanwhile no respondent was neutral, disagreed or strongly disagreed with the same item. From the pattern of responses provided one can say that most of the healthcare professionals want to be given a security mechanism awareness training on a regular basis.

Also for the item, health information security policies and procedures must be made available to all healthcare providers as per facility's best practices, 60 (60.0%) strongly agreed and 37 (37.0%) respondents replied that they agreed with the item. At the same, 2 (2.0%) were not taking sides, that is, they were neutral, 1 respondent representing 1.0% replied that they disagreed with the item and no respondents representing 0.0% strongly disagreed with the item that health information security policies and procedures must be made available to all healthcare providers as per facility's best practices.

The table reveals that 49 (49.0%) and 39 (39.0%) respondents strongly agreed and disagreed respectively with the item that there must be a reporting mechanism which allows employees to report breach of confidentiality while 6 (6.0%) were neutral to the same item. 3 (3%) respondents disagreed and 3 (3.0%) strongly disagreed with the statement that there must be a reporting mechanism which allows employees to report breach of confidentiality. Majority of the respondents in Berekum Holy Family Hospital strongly agree and agree that there must be a reporting mechanism which allows employees to report breach of confidentiality.

Furthermore, 55 or 55.0% respondents and 41 or 41.0% strongly agree or agree respectively, that A formal disciplinary or sanction policy must be enforced for healthcare providers who have violated security policies and procedures. However, 4 (4.0%) respondents were not taking sides (neutral) to this item and no respondent disagreed or strongly disagreed to the same item. This response outcome proves that most of the healthcare professionals agree that a formal disciplinary or sanction policy must be enforced for healthcare providers who have violated security policies and procedures.

From the responses given to the fifth statement in Table 4.4, 45 respondents representing 45.0% strongly agreed to the statement that the healthcare facility is to provide additional hardware of the information systems for backup or redundancy mechanisms and 40 respondents representing 40.0% agreed to the same statement. More so, 14 or 14.0% respondents were neutral to this statement and 1 or 1.0% respondent this

disagreed with the same statement. No respondent strongly disagreed with the statement that the healthcare facility is to provide additional hardware of the information systems for backup or redundancy mechanisms.

From the responses given to the last statement in Table 4.4, 43 respondents representing 24.0% strongly agreed as compared to 0 respondent who strongly disagreed with the statement that the healthcare administration is to perform at minimum, annual risk assessment and reviews to the privacy and security policies. 50 (50.0%) respondents agreed to this statement. More so, 6 (6.0%) respondents were neutral to the statement and 1 respondent representing 1.0% disagree with the statement. We can conclude that majority of the healthcare professionals at the Berekum Holy Family Hospital agree that healthcare administration is to perform at minimum, annual risk assessment and reviews to the privacy and security policies.

Table 4.4: Responses on assessing the administrative security measures for protecting patient health information at the Berekum Holy Family Hospital

STATEMENT	STRONGLY AGREE n (%)	AGREE n (%)	NEUTRAL n (%)	DISAGREE n (%)	STRONGLY DISAGREE n (%)
19. Employees should be given security awareness training on a regular basis	65 (65.0%)	35 (35.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
20. Health information security policies and procedures must be made available to all healthcare providers as per facility's best practices	60 (60.0%)	37 (37.0%)	2 (2.0%)	1 (1.0%)	0 (0.0%)
21. There must be a reporting mechanism which allows employees to report breach of confidentiality	49 (49.0%)	39 (39.0%)	6 (6.0%)	3 (3.0%)	3 (3.0%)
22. A formal disciplinary or sanction policy must be enforced for healthcare providers who have violated security policies and procedures	55 (55.0%)	41 (41.0%)	4 (4.0%)	0 (0.0%)	0 (0.0%)
23. The healthcare facility is to provide additional hardware of the information systems for backup or redundancy mechanisms	45 (45.0%)	40 (40.0%)	14 (14.0%)	1 (1.0%)	0 (0.0%)
24. The healthcare administration is to perform	43 (43.0%)	50 (50.0%)	6 (6.0%)	1 (1.0%)	0 (0.0%)

at minimum, annual risk assessment and reviews to the privacy and security policies					

DISCUSSION

Research Question One: What are the physical security mechanisms for protecting patient health information at the health facility?

The success of quality healthcare depends on a secured patient health information which is protected by the various security mechanisms in the healthcare facility. This survey was an attempt to assess the security mechanism for protecting patient health information. The first question sought to find out the physical security mechanism used to protect patient health information. From the results, it was identified most of the healthcare professionals are aware of the various physical security mechanisms for protecting health information in the health facility. The response rate to "Does the facility have a Man Guard force?" is 89 Yes against 11 No; this could be due to the fact that some of the healthcare professionals are newly transferred or employed worker in the facilty and so have not come across the Man Guards yet.

In addition, the results show 90 among the 100 respondents responded positive to the statement, does the facility deals in staff ID. This could be that the other 10 respondents who responded negative to the statement does the facility deals in staff ID are newly enrolled staff nurse or healthcare professionals and so have not been given their staff ID yet.

Also, the responses on the statement does the electronic health record system have RFID (Radio-Frequency Identification) detectors installed on them are 51.0% positive and 49.0% which clearly shows not all the computers the healthcare professionals used to access patient health information has Radio-Frequency Identification detectors installed on them.

Research Question Two: What are the technical security mechanisms for protecting patient health information at the health facility?

From the study, health care professionals in the healthcare facility have an experience in the technical aspect of protecting patient health information.

The result of this study highlighted that 84 respondents was positive on the statement do you use Electronic health record system in service delivery. This shows that the rest of the respondents, thus 16 healthcare professionals directly work with the paper or manual health records containing patient health information. Moreover, majority of the respondents representing 85.0% responded negatively to the statement can you access the Electronic health record system during non-working hours. This explains that the remaining 15.0% representing 15 respondents can access the electronic health records during non-working hours. This might be the decision of the management under the regulations of the health facility under special healthcare service.

The results for the statement, are your firewalls, information systems and security mechanisms securely configured; Tick "No", if your systems are configured using factory default settings; depicted 66.0% of the respondents choosing No and 34.0% out of the 100 respondents choosing Yes. These figures might be the case that the 34.0% who responded negatively to the statement might have no idea on the ways the health facility's information systems are configured.

CHAPTER FIVE
CONCLUSION AND RECOMMENDATION

The hospital's healthcare professionals have secured ways to access patient health information to help in service delivery. Such includes a unique password or passphrase for each healthcare professional with the hospital's staff ID. With this, there is an effective security mechanism in protecting fraudsters and hackers from accessing patient records through the hospitals electronic health record systems. Also manipulation of patient health information is limited which will ensure the quality of care to patient and assess the physicians and other healthcare professionals' competency through their diagnosis, treatment and prescriptions. The hospital's departments are well secured with modern locks and Man Guard force at the various vulnerable points including the two entrances of the hospitals and the Out Patient Department entrance for some physical security checks.

Moreover, the study discovered that, the healthcare professionals made some suggestions and agree on the fact that the hospitals administration should provide the necessary security awareness and training on a regular basis for them. Also, must perform at minimum, annual risk assessment and reviews to the privacy and security policies. This can improve the healthcare professionals' ability to avoid intentional and unintentional security breach of patient health information privacy. The risk assessment and reviews to the privacy and security creates quality standard for identifying the minor and major breaches of security and privacy so as to curb them.

RECOMMENDATION

- Healthcare professionals who are not working in the hospital again as a results of employee's turnover, transfer or retired healthcare professionals' details should be cleared from the hospital's database to prevent them from accessing clinical or patient health information.
- Discussion of the appropriate and other alternate methods for protecting patient health information such as adherence to policies and procedures and conforming to the code of conduct for health care professionals should be provided by health educators and the hospital's board of directors to bridge the knowledge gap relating to the breach of confidentiality, security and privacy of patient health information.

REFERENCES

1. Abdul, W., Alzamil, A., Masri, H., Ghouzali, S., Hussain, M., & AlZuair, M. (2017). Fingerprint and iris template protection for health information system access and security. *Journal of Medical Imaging and Health Informatics*, *7*(6), 1302-1308.
2. Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*, *21*(2), 374-378.
3. Al-Nayadi, F., & Abawajy, J. H. (2007, December). An authentication framework for e-Health systems. In *2007 IEEE International Symposium on Signal Processing and Information Technology* (pp. 616-620). IEEE.
4. Andriole, K. P. (2014). Security of electronic medical information and patient privacy: what you need to know. *Journal of the American College of Radiology*, *11*(12), 1212-1216.

5. Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.
6. Calvillo-Arbizu, J., Román-Martínez, I., & Roa-Romero, L. M. (2014, June). Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems. In *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (pp. 539-542). IEEE.
7. Chand, N., Bhattacharyya, S., & Sarkar, A. (2021). A Novel Encryption Technique to Protect Patient Health Information Electronically Using Playfair Cipher 15 by 14 Matrix. In *Advances in Medical Physics and Healthcare Engineering* (pp. 423-431). Springer, Singapore.
8. Collier, R. (2014). New tools to improve safety of electronic health records. *CMAJ*. 186(4):251–251.
9. Desai, S. (2010). Violence and surveillance: Some unintended consequences of CCTV monitoring within mental health hospital wards. *Surveillance & Society*, *8*(1), 84-92.
10. Draper, R., Ritchie, J., Wilson, E., & Prenzler, T. (2017). Best practice in physical security and people management. In *Understanding crime prevention: The case study approach* (pp. 151-165). Samford Valley, Qld: Australian Academic Press.
11. Dubrova, E. (2013). Hardware redundancy. In *Fault-Tolerant Design* (pp. 55-86). Springer, New York, NY.
12. Farooq, U., ul Hasan, M., Amar, M., Hanif, A., & Asad, M. U. (2014). RFID based security and access control system. *International Journal of Engineering and Technology*, *6*(4), 309.
13. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. *J Med Sys*, 34(4):629–42.
14. Faustman, E. M., & Omenn, G. S. (2008). Risk assessment. *Casarett and Doull's toxicology: The basic science of poisons*, 107-128.
15. Fennelly, L. (Ed.). (2016). *Effective physical security*. Butterworth-Heinemann.
16. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. (2013, June). Security and privacy in electronic health records: a systematic literature review. J Biomed Inform. 46(3):541-62. doi: 10.1016/j.jbi.2012.12.003. Epub 2013 Jan 8. PMID: 23305810
17. Flores Zuniga, A. E., Win, K. T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of medical systems*, *34*(5), 975-983.
18. Goel, P., Datta, A., & Mannan, M. S. (2017). Industrial alarm systems: Challenges and opportunities. *Journal of Loss Prevention in the Process Industries*, *50*, 23-36.
19. Goldstein, E. (2021). CCTV Helps Both Patients And Staff.
20. Jorge Rey, C. I. S. A., CISM, C., & Douglass, K. (2012). Keys to securing data as a practitioner. *The Journal of medical practice management: MPM*, *27*(4), 203.
21. Khandare, L., Sreekantha, D. K., & Sairam, K. V. S. S. S. S. (2019, March). A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems. In *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)* (Vol. 1, pp. 1-5). IEEE.
22. Liu, V., Musen, M.A., and Chou, T. (2015). Data breaches of protected health information in the United States. *J. Am. Med. Assoc.* 313(14):1471–1473. doi:10.1001/jama.2015.2252
23. Luethi, M., & Knolmayer, G. F. (2009, January). Security in health information systems: an exploratory comparison of US and Swiss hospitals. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

24. Mark A. Rothstein & Meghan K. Talbott (2007). Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications, The American Journal of Bioethics, 7:3, 38-45, DOI: 10.1080/15265160601171887
25. Mellado, D., Fernández-Medina, E., & Piattini, M. (2010). Security requirements engineering framework for software product lines. *Information and Software Technology*, *52*(10), 1094-1117.
26. Misic J, Misic V. (2007). Implementation of security policy for clinical information systems over wireless sensor networks. *Ad Hoc Networks*;5(1):134–44.
27. Morse, R. E., Nadkarni, P., Schoenfeld, D. A., & Finkelstein, D. M. (2011). Web-browser encryption of personal health information. *BMC medical informatics and decision making*, *11*(1), 1-9.
28. Samy, G. N., Ahmad, R., & Ismail, Z. (2009, August). Threats to health information security. In *2009 Fifth International Conference on Information Assurance and Security* (Vol. 2, pp. 540-543). IEEE.
29. Sandland-Taylor, S. (2018). No cause for alarm. *Building Surveying Journal*, 12-13.
30. Stasia Kahn, and Vikram Sheshadri, (March/April 2008). "Medical record privacy and security in a digital environment", IT Pro, IEEE Computer Society.
31. Stine, K., & Dang, Q. (2011). Encryption basics. *Journal of AHIMA*, *82*(5), 44-46.
32. Trinckes Jr, J. J. (2012). *The definitive guide to complying with the HIPAA/HITECH privacy and security rules*. CRC Press.
33. Turcu, C. E., Turcu, C., & Popa, V. (2009, May). An RFID-based system for emergency health care services. In *2009 International Conference on Advanced Information Networking and Applications Workshops* (pp. 624-629). IEEE.
34. Yao, W., Chu, C. H., & Li, Z. (2010, June). The use of RFID in healthcare: Benefits and barriers. In *2010 IEEE International Conference on RFID-Technology and Applications* (pp. 128-134). IEEE.
35. Yucel, G., Cebi, S., Hoege, B., & Ozok, A. F. (2012). A fuzzy risk assessment model for hospital information system implementation. *Expert Systems with Applications*, *39*(1), 1211-1218.

APPENDIX A: QUESTIONNAIRES

QUESTIONNAIRE

ASSESSING SECURITY MECHANISMS FOR PROTECTING PATIENT HEALTH INFORMATION AT THE BEREKUM HOLY FAMILY HOSPITAL

Dear respondent,

This questionnaire is based on an ongoing research project about assessing security mechanisms for protecting patient health information at the Berekum Holy Family Hospital. To this end, I kindly request that you complete the following questionnaire regarding your experience on the security mechanisms. Your response is of utmost importance. It should take no longer than 10 minutes of your time. **Please note that the confidentiality of your response is assured**.

Select the appropriate options for the questions below.

SECTION A: DEMOGRAPHIC OF RESPONDENT

1. **Age:** [ ] 20 - 24 [ ] 25 - 29 [ ] 30 - 34 [ ] >= 35
2. **Gender:** [ ] Male [ ] Female
3. **Job Title:**……
4. **Work experience in years:** [ ] 0 - 5 [ ] 6 - 10 [ ] > 10
5. **Religion:** [ ] Christian [ ] Muslim [ ] Others
6. **Marital Status:** [ ] Single [ ] Married [ ] Divorced

SECTION B: THE PHYSICAL SECURITY MECHANISMS FOR PROTECTING PATIENT HEALTH INFORMATION

Please tick ( ) the response as applicable to you.

QUESTIONS	1 YES	2 NO
7. Does the facility have a Man Guard force?		
8. Does the facility deals in staff ID?		
9. Do guards check healthcare providers ID?		
10. Does the facility have alarm systems?		
11. Does the electronic health record system have RFID (Radio-Frequency Identification) detectors installed on them?		
12. Are locks changed when keys lost?		
13. Does the facility use CCTV cameras at areas housing patient health data and information systems?		

SECTION C: THE TECHNICAL SECURITY MECHANISMS FOR PROTECTING PATIENT HEALTH INFORMATION

Please tick ( ) the response as applicable to you.

QUESTIONS	1 YES	2 NO
14. Do you use Electronic health record system in service delivery?		
15. Do you log into the system with a unique Authentication (User-Password or Passphrase)?		
16. Can you access the Electronic health record system during non-working hours?		
17. Are your firewalls, information systems and security mechanisms securely configured? Tick “No”, if your systems are configured using factory default settings.		
18. Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted?		

SECTION D: THE ADMINISTRATIVE SECURITY MEASURES FOR PROTECTING PATIENT HEALTH INFORMATION

In this section, the response to each question has been rated on a scale of 1,2,3,4 and 5. Please tick ( ) the response as applicable to you.

QUESTIONS	1 STRONGLY AGREE	2 AGREE	3 NEUTRAL	4 DISAGREE	5 STRONGLY DISAGREE
19. Employees should be given security awareness training on a regular basis.					

20. Health information security policies and procedures must be made available to all healthcare providers as per facility's best practices.					
21. There must be a reporting mechanism which allows employees to report breach of confidentiality					
22. A formal disciplinary or sanction policy must be enforced for healthcare providers who have violated security policies and procedures.					
23. The healthcare facility is to provide additional hardware of the information systems for backup or redundancy mechanisms.					
24. The healthcare administration is to perform, at minimum, annual risk assessment and reviews to the privacy and security policies.					