INFORMATION SECURITY AND SERVICE DELIVERY IN HEALTH SECTOR: CASE STUDY OF CHOGORIA HOSPITAL

BRENDA NKATHA NYAGA

D61/68687/2011

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER 2016

DECLARATION

I declare that this is my original work and has not been presented for a degree in any other university.

Signature ……………………………… Date ……………………………….

BRENDA NKATHA NYAGA
D61/68687/2011

This research project has been presented for examination with my approval as the university supervisor:

Signature ………………………… Date ……………………………….

DR. J.T. KARIUKI
Lecturer, Department of Management Science
Master of Business Administration
School of Business, University Of Nairobi

ACKNOWLEDGEMENTS

Thanks to Almighty God for giving me strength and ability to learn, understand and complete this project. I greatly appreciate the guidance from my Supervisor Dr. J. T. Kariuki and his tireless support throughout the project process. I also thank my project moderator Mr. Lelei for his unlimited support during the project. My appreciation also goes to the department of Management Science for their support and guidance.

I am heavily indebted to my fellow friends, classmates and colleagues for giving me the moral support and making this endeavor an enjoyable experience. Finally, I appreciate all the respondents at the Chogoria Mission Hospital for creating time to complete the questionnaires making the completion of this study successful.

DEDICATION

I dedicate this project to my family for their prayers and nursing me with affections and love and for their dedicated partnership for success in my life. May God keep you and bless you abundantly.

ABSTRACT

The study focused on investigating the extent of adoption of information security in the health sector and examined its effect on service delivery. The study adopted descriptive survey design to collate, analyze and present data. The study used a sample size of 30% of the target population of 135 Chogoria hospital staff working in various departments in the hospital. Data collection instrument used was a questionnaire. The data collected was analyzed using descriptive statistics, correlation and regression analysis. The study established a strong relationship between information security adoption and service delivery in the health sector. The study established that information security and its elements (confidentiality, integrity and availability) is an important issue in management of information systems in the health sector because patient's information is very sensitive and disclosure to unintended audience could lead to stigma and discrimination, errors in medical information could have grave consequences by leading to wrong diagnosis, adverse drug interactions and may also lead to death due to compromised standards of patient's care. The study therefore recommends adoption of information security strategies, guidelines and policies on health care information to enhance service delivery by ensuring there is optimal patient's care and management. All staff handling patient's information should have proper training on information security.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATION

ALOS	Average Length of Stay
CIA	Confidentiality, Integrity and Availability
DDoS	Distributed Denial-of-Service
EMP	Electromagnetic Pulse
HIPAA	Health Insurance Portability and Accountability Act).
HIS	Health Information systems
ICT	Information Communication Technologies
IEC	International Electrotechnical Commission
IS	Information Security
ISM	Information Security Model
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MIS	Management Information Systems
MOH	Ministry of Health
PCEA	Presbyterian Church of East Africa
PDAs	Personal Digital Assistants
UCISA	Universities and Colleges Information Systems Association
UN	United Nation
WHO	World Health Organization

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Information security in the health sector is an issue of growing importance. The increased adoption of digital patient records, increased regulation, provider consolidation and the increasing need for information exchange between patients, providers and medical insurance companies, all point towards the need for better information security Appari et al (2010). During a patient – physician relationship, patients are required to provide information about their health in order to facilitate accurate diagnosis, management and treatment aimed at avoiding adverse drug interactions. In some cases, the patients may refuse to divulge sensitive information in cases of health issues like psychiatry, HIV or chronic diseases as their disclosure can lead to being discriminated and stigmatized by family members and friends or insurance companies who are reluctant to cover some chronic diseases (Applebaum, 2002). With time, a patient's medical record accumulates significant personal information which includes patient's identity and profile like blood group, age, weight or height, medical images digital renderings, sexual preference, medical diagnosis history, genetic information, treatments history, dietary preference and habits, doctor's subjective assessment of psychological, personality and mental state and employment, income, medication history (Mercuri, 2004).

Information is today regarded as one of the most valuable assets of an organization and with the advent of globalization and ever changing technologies the need for information security is becoming more and more vital. As organizations are becoming dependent on information technology the emphasis on Information Security (IS) is getting more significant. While initially IS was seen as a technology problem that could be addressed via sophisticated hardware and software solutions, increase in number of security breaches proved that this is indeed mostly a people problem (Rudolph et al 2002). In this regard managing information risks brings together the collective judgments of individuals and groups within these organizations responsible for strategic planning, oversight management, and day-to-day operations –providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of these organizations (NIST, 2011). Thus effective risk management requires that organizations operate in highly complex interconnected environments i.e. systems that organizations depend on to accomplish their missions and to conduct important business-related functions (NIST, 2011). It can be argued that since information security is continually evolving, businesses have come to view information as a critical asset, and have increasingly come to depend on public networks to transport sensitive information thus protecting information has become less about technology and more about sustainability of the enterprise itself (ISACA, 2009).

The security of personal information is of paramount importance to all institutions. However, in the health sector the information systems need to be robust with the aim to ensure the confidentiality, integrity, and availability of personal health information is met. Subsequently, this ensures that patients' records are up to date to facilitate easy access and fast tracked delivery of patient care, increase efficiency on administrative processes for example appointments bookings and enable accurate clinical and statistical research.

The study was guided by integrated systems theory and contingency theory. Integrated system theory integrates different perspectives from security policy, risk management, control and auditing management systems. Contingency theory states that there is no optimal way to structure and manage organizations and therefore it recognizes and responds to situational variables in order to attain organizational objectives effectively (Koskosas & Asimopoules, 2011). This study focused on issues relating to adoption of information security and its elements of confidentiality, integrity and availability in information systems at the Chogoria hospital and how they affect service delivery.

1.1.1 Information Security

By definition, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction (Larsen, Pedersen & Andersen, 2006). Confidentiality, integrity and availability, also known as the CIA triad, is a model that provides guidance in policies for information security within an organization. The principles of the CIA triad form the three most important components of information security.

Information confidentiality means that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when information is disclosed either by word of mouth, during transmission of information via e-mail, copying, or creating documents and other data. Patients routinely disclose personal information with health care providers in the cause of treatment. Therefore, confidentiality of this information should be protected at all cost to avoid loss of trust between the patient and the health care provider.

Information integrity refers to authenticity and completeness of information. It ensures that the data being accessed or read, has neither been tampered with, nor been altered or damaged by an individual or through a system error over its entire life-cycle. Information integrity is a key component of information security and is required in order to have a sound security management programme. Although it is not possible to achieve 100 percent information security a reasonable assurance is achievable by using appropriate counter measures which include file permissions and user access controls. Version control can also be used to mitigate against erroneous changes or accidental deletion by authorized users. Other counter measures that can be implemented in case of system errors like an electromagnetic pulse (EMP) or server crash include checksums, certificates, logging and digital signatures to verify integrity. Backups and redundancies must be in place to restore data to its correct state.

Lastly, information availability means that the information systems responsible information collection, processing and storage are easily accessible when required, by those who require them. In health care, the characteristic of health information should be available when and where it is required and should be disclosed only to authorized organizations and individuals to ensure continuity of heath care of a patient.

While the magnitude of threat against healthcare information has grown exponentially, the intention or investment in securing that information has not always followed. Worse still, information security attacks in most organizations never get publicly reported, leading to a false sense of security, and complacency.

1.1.2 Service Delivery

In the health sector, service provision or delivery is an immediate product of the inputs such as efficient procurement and supplies channels, investment in infrastructure, and competent human resource into the health system. The increase of resources should lead to improved service delivery and enhanced access to services. Ensuring availability of health services that meet a minimum quality standard and securing access to them are key functions of a health system (WHO, 2008). The delivery of service in health sector has been and continues to draw attention from the external and internal environment. The heath sector has also adopted modern technology in order to improve service delivery (Humphrey, 2010).

Service delivery framework is a set of principles, standards, policies and constraints used to guide the design, development, deployment, operation and retirement of services delivered by a service provider with a view to offering a consistent service experience to a specific user community in a specific business context. Service delivery framework is the context in which a service provider's capabilities are arranged into services (Helmsing, 2005). Helmsing (2005) in his study defines service delivery in an organization as a deliberate obligatory decision by the management to serve or deliver goods and services to the recipients. Customer care involves putting systems in place to maximize customers' satisfaction. It should be a prime consideration for every business sales and profitability depends on keeping your customers happy. It is more directly important in some roles than others. For receptionists, sales staff and other employees in customer-facing roles, customer care should be a core element of their job description and training, and a core criterion when recruiting (Athanassopoulos, 2000).

According to WHO (2008), some of the ideal characteristics desired in an effective health system based on health care are comprehensiveness of health services that are appropriate to the needs of the population which include preventative, curative, palliative and rehabilitative services and health promotion activities; Other characteristics are accessibility to health services whether at home, community, workplace or health facilities. The health service should cover all people regardless of the fact that they are sick or healthy and not based on their social or economic groups. Health services should be person-centered; this means focusing on the person and not the disease to provide a holistic approach to treatment and management. There should be continuity and coordination amongst all health providers. Finally, the health service should be of high quality, focused on the patient’s needs and provided in a timely manner. Well managed service delivery should ensure there is minimal wastage of resources thus being efficient.

1.1.3 Information Security and Service Delivery

Information technology (IT) offers numerous benefits to the healthcare sector. IT enables ease of data collection, information processing and presentation to ensure accurate medical information is more readily available to health sector stakeholders and can improve service quality, improve patient's management and lower the cost of health care. However, the shift of medical records from paper to electronic formats has increased the potential for individuals to access, use and disclose sensitive personal health data which raises concerns about patient's information privacy and security.

Incidents that involve loss of information's confidentiality, integrity or availability can be very costly leading to damage of the hospital's reputation, financial loss, litigation, regulatory enforcement and even death of patients due to medical errors. Therefore there is the emphasis to heath institutions to implement effective information security management processes by continuously monitoring, reviewing and improving the information systems to safeguard patient's information and information technology equipment. One way of achieving this is to implement information security best practice recommendations and guidelines.

1.1.4 PCEA Chogoria Hospital

PCEA Chogoria Hospital was begun in 1922 by Scottish missionaries as a medical outpost in Tharaka Nithi county, Kenya. The hospital is one of the largest mission hospital in Kenya. The outpost grew into the Presbyterian Church of East Africa (PCEA) in l956, when its name changed to PCEA Chogoria Hospital. The hospital runs a system of 32 effort centers; twenty of these facilities are completely overseen by the clinic, 10 by territory wellbeing advisory group individuals with support from the hospital, and one by the Ministry of Health (MOH).

Currently the hospital has a bed capacity of 295, including 52 maternity beds. The normal length of stay (ALOS) for all inpatients is nine days, while that of maternity is five days. The hospital focuses on curative, preventive and promotive health care services covering the greater Meru and as far as Isiolo and Marsabit. It is also a teaching and referral hospital.

The hospital has expanded its network to include a community health department that consist of a maternal child health /family planning clinic and 30 rural community clinics, groups of community volunteers, a nursing schools and other non- health related projects.

1.2 Research Problem

Although information systems investments have grown in health sector, the use and, especially, the effects of it on a larger scale service delivery are still in the early stages and changes are only starting to occur (Grimson et al, 2012). Effective information systems management has emerged as the means by which health sector can participate in the new knowledge landscape for improved service delivery. The investment in more modern information systems, like in any sector, is expected to increase effectiveness without compromising quality. However, an information system alone seldom has a long lasting or sustained effect on effectiveness and quality (Wade & Hulland, 2004).

With the dramatic increases of hacking of websites in Kenya and state of data and information compromised, more effective information security tools and services need to be introduced and implemented. As Rao et al (2012) puts it, with implementation of information security, health centres have improved trust in customer relationships as well as ensuring that organisation reputation is protected. There is decreasing likelihood of violation of privacy, greater confidence when interacting with trading partners. It also enables new and better ways to process electronic transactions thus reducing operational costs by providing predictable outcomes and mitigating risk factors that may interrupt the process. Other benefits include protection from loss of customers and business revenue through loss of employee productivity and inability to meet business requirements. Implementation of information security enables banks to have a competitive advantage over their competitors; however there are various challenges in the implementation. Security of information is therefore of paramount importance especially to the health sector and this forms the motivation behind the study to evaluate the security of information in the PCEA Chogoria hospital.

Muratha (2012), did a study on information security practices in the Kenyan capital market. The results of this research revealed that security is more than just a technological problem as it has been generally recognized. Insights have revealed that the human aspect of the information security has not been given much attention and yet most of the breaches experienced in the last four years are on people and processes. Kiptoo (2013) did a study on adoption of computer-based management information systems on quality service delivery in middle level institutions in Kenya: a case study of ol'lessos technical training institute. The study concluded that institutions understand the need to adopt management information systems (MIS) and have even made attempt to facilitate its adoption. However there exists a gap in the usage of these equipments in the management of information. The study recommends a training assessment on MIS, posting information on shared databases and lastly engaging the services of an IT company with necessary technical capacity at the initial stages of MIS adoption. Nyandiere (2006) surveyed 17 managers in his study on the increasing role of Information Systems in the Management of Higher Educational Institutions (HEIs) in Kenya. The study found out that ICT (Information Communication and Technology) as a tool should be core in all functions at the Strathmore University and that ICT should help organize and increase Strathmore's operations efficiency especially management of admissions, finance, examinations and library resources. The study established that ICT is a tool for operations and management support. The study further revealed that most users were not happy with quality, reliability and accuracy of information provided by the current systems especially in the areas of integration and security features. Although a numerous of studies have been done in the area of information systems / information technology and their relation to service delivery in banks, none has focused on information systems security and service delivery at PCEA Chogoria mission hospital. The research question, therefore, is: what is the level of information security adoption and its effect on service delivery at the PCEA Chogoria mission hospital?

1.3 Objective of the Study

The specific objectives of this study were:

i. To determine the extent of information security adoption at PCEA Chogoria mission hospital.

ii. To examine the relationship between information security and service delivery at PCEA Chogoria mission hospital.

1.4 Value of the Study

The findings of this study will enlighten and increase awareness to all stake holders in the health sector and to the management of PCEA chogoria hospital on the importance of information security and how it affects health service delivery and enable them to formulate appropriate strategies, guidelines and standards to safeguard patient’s information.

The policy makers will use the findings to form a background for development of strong information security strategies, guidelines and standards in Hospitals which can be implemented for better healthcare delivery.

Theoretically, the research will be significant to academicians and researchers since this research will contribute to the existing knowledge on information security and shall provide reference material to scholars.

The research findings will form a basis for further studies on effect of information security on health care service delivery.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature on theoretical foundations of the study, concept of information security and its application in organizations, and the relationships that exists between information security and service delivery in healthcare. The chapter also shows the conceptual framework identified that shows the relationship of the variables.

2.2 Theoretical Basis of Study

This section looked at the various theories that were used to inform the study on the effect of information security adoption on service delivery. The study was founded on two theories that is the Integrated Systems Theory and Contingency Theory. Specifically, literatures pertaining to health system information security and health care service delivery were reviewed.

2.2.1 Integrated Systems Theory

The integrated systems theory was proposed by Hong et al (2003), as an interdisciplinary theory concerned about every system in nature, in society and in many scientific domains as well as a framework with which a phenomena can be investigated from a holistic approach (Capra, 1997). Integrated System Theory covers the importance of enforcing information security policies, assessing and managing risks, internal controls, technical and process controls and information auditing. By doing so, integrated system theory covers information security holistically in terms of different perspectives. It explains organization behavior regarding information security management and strategies and provides alternatives.

Integrated systems theory was significant to the study as it facilitates a comprehensive understanding of information security management; it helps explain information security management strategies, and helps to predict management outcomes. Therefore the theory provides a good basis for estimating and measuring the level of information security adoption, the security awareness and controls implemented at the Chogoria hospital.

2.2.2 Contingency Theory

Contingency Theory is mainly associated with Joan Woodward (1958) which argues that the organization structure is shaped by three contingencies of the environment, size and strategy which it needs to fit them to avoid loss of performance. Contingency theory suggests that there is no optimal strategy for all organizations and posits that the most desirable choice of strategy variables alters according to certain factors, termed contingency factors (Donaldson, 1996). A contingency theory is an organizational theory that claims that there is no single optimal way to organize and manage an organization. Instead, the optimal course of action is contingent (dependent) on environmental conditions both internal and external situation. Contingency approach means that an organization recognizes and responds to situational variables in order to attain organizational objectives effectively (Drazin & VandeVen, 1985).

Contingency approach has been applied in information security management. For instance, Solms et al, (1994) proposed an information security model (ISM) which consists of information security levels: ideal, prescribed, baseline, current and survival. Except for ideal level, all the other levels are dynamic and contingent upon environmental variables such as information security threats, vulnerabilities and impact for an organization.

Most methods for mitigating the organizational information security challenges are unclear since the methods depend upon several situational variables. Contingency theory supported the study in that it highlights the importance of the hospital’s management to determine the effects of the external and internal activities and how they affect the structure of the organization so as to effectively prepare actions for its operation. The theory clearly delineates external environmental variables from the organizational factors, which affect strategy implementation and hence contributing to the study of information security and service delivery in health sector in Chogoria hospital.

2.3 Information Security

Calder et al (2008) states that security of information systems means different things to different people; for example it is limited to products when it comes to vendors of security products. To many directors and managers, it is seen as technical issue that is difficult to understand and its often left to the IT manager to deal with. To many IT equipment users, it tends to mean undesirable restrictions imposed by the management on what they can do on their computers and other IT devices.

Organizations operate in an environment with increasingly powerful ways of manipulating and storing information. This is matched by growing threats to that information. Businesses need to manage their information so that they get the best value from it, and minimise the risks of losing it. Information security is important in ensuring that your organization continues to operate effectively and profitably. ISO/IEC 27001 standard defines the various information security practices that organizations should implement. The practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program. The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. The practices provide a common ground for determining the security of an organization and build confidence when conducting multiorganizational business. Swanson and Guttman (2006) emphasises that organizations should use the practices as a starting point in order to develop additional practices based on their own organizational and system requirements. The common practices should be augmented with additional practices based on each organization's unique needs.

Organizations are vulnerable to uncertainties whose impact may negatively affect the organization in various ways be it operational or financial and it is the role of the IT security professionals to support and help the organizations' management to understand and manage these uncertainties hence attaining the fundamental precept of information security which is to support the organization's mission (Mattrod, 2009). According to Elky (2006), managing and mitigating all risks an organization faces is almost impossible due to ever-changing threats and vulnerabilities as well as limited resources most organizations have that make management of risks a difficult task to accomplish. To this effect, Elky (2006), recommended that IT security professions need to have a toolset that is consistent, repeatable, and cost-effective that would reduce risks to a reasonable level to assist them on sharing commonly understood view with IT and Business managers in regards to the impact of various IT security threats to the organization's mission.

The main goal of any health information system both manual and digital in not just health information collection, but also to facilitate sound decision making to all stakeholders in the healthcare system. Effective information systems should greatly contribute to good healthcare service delivery. Health related information collection, analysis and presentation should be organized in such a way that it helps to identify the most needy groups and individuals. Health information collected is vital and should be safeguarded at all costs.

Health professionals are obligated to maintain confidentiality of patient's information during the course of their relationship. This means, protecting the information created, disclosed or acquired directly or indirectly in the context of the patient and health care provider relationship. All the staff that accesses the information during the process of delivering heath care has a duty to protect the information from unauthorized access. This means computer passwords are put in place, rooms where files and servers are kept are under lock and key to control access, medical information is only handled by qualified personnel and is used only for the intended purpose.

.

Parker (1998) states that integrity means that information meet the accuracy, completeness, and robustness criteria. The concept of integrity ensures that: modifications are not made to data by unauthorized people or processes, and the data is consistent both internally and externally. In the hospital set-up, it is important to have information continuously updated to ensure completeness and reliability. Incorrect information could have adverse effect on patients, or even be fatal. Information integrity means that the information is not and should not be distorted by desired or undesired changes, and that information should be protected against losses. Training of users' with IT skills and create information security awareness prevents intentional and unintentional losses and improves transmission of information amongst different people. In addition, reliable and correct information also means that the information is updated. In the case of paper-based medical record it means that documents about the patient are added to the record and the documents in the record are sorted continuously. Hence outdated documents are removed from the record and replaced with the current records.

Osborne (2006) defines availability as the principle to ensure that our data will be available in a timely manner. Available information means that healthcare professionals should have access to information when needed. In a health environment this is crucial. Without access to relevant, as well as correct, information, there is a risk for the patient's health. Availability of information goal can be achieved by the hospital ensuring that the information system is always up and running, off site back-ups should be often tested to ensure business continuity, the flow of information should be traceable through proper documentation and logging. Electronic and manual medical records should continuously sorted and arranged in a manner that enable easy retrieval. As indicated by McCumber (2005), if data is required for a choice or for some other reason and it is not there, it is basically not accessible. Case medical records should follow the patient to ensure consistency in medical management and reduction in duplication of treatment procedures. Information technology is viewed as an enabler to ensure electronic health records can be made available promptly when required.

Information system security is the application of managerial and administrative procedures and technical and physical safeguards to ensure not only the confidentiality, integrity and availability of information which is processed by an information system, but also of the information system itself, together with its environment. Such procedures and safeguards not only need to deter and delay improper access to information systems, they must also ensure that any improper access is detected; that is, individuals have to be made accountable for their actions.

2.4 Service Delivery

Service delivery framework is a set of principles, standards, policies and constraints used to guide the design, development, deployment, operation and retirement of services delivered by a service provider with a view to offering a consistent service experience to a specific user community in a specific business context. Service delivery framework is the context in which a service provider's capabilities are arranged into services (Helmsing, 2011).

According to Oboth (2011), service is a system or arrangement that supplies public needs whereas delivery is periodical performance of a service. Therefore, service delivery is a system or arrangement of periodical performance of supplying public needs. Heskett (1987) defines service delivery as an attitudinal or dispositional sense, referring to the internationalization of even service values and norms. Rajnish et al (2010) notes that delay in delivery of health services is a main factor in dissatisfaction of customers. He further asserts that, service quality means how well the patient's expectation is met or surpassed against their perception. Service quality can be measured in terms of the perception, expectations, satisfaction of the patient.

Bansal (2004) put some of the service delivery satisfactory elements in health care as responsiveness of health professionals to patient's needs, accuracy of diagnoses, knowledge, skills and credentials of health professionals and reputation of the health institution. Other factors on customer satisfaction in health care highlight the importance of convenience, accessibility, minimal waiting time, quality of information given by the doctors, nurses and pharmacists, variety of services, nature of the patient's medical problems, a comfortable environment, and a courteous, patient and caring medical staff.

2.5 Information Security and Service Delivery

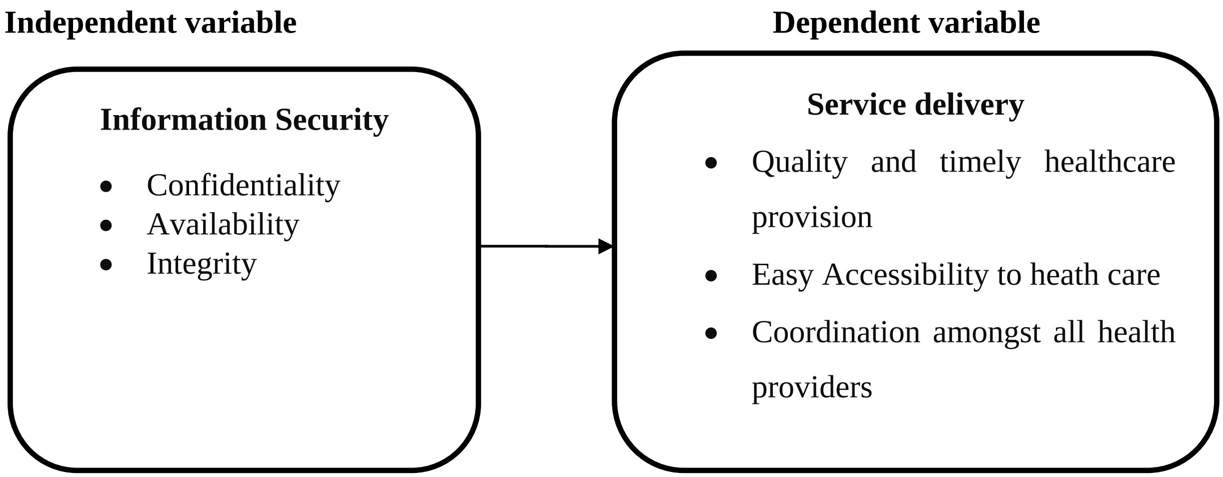
Felicia (2011) in information system security journal remarked that simply checking that operating systems and applications are running the latest patches has obvious security benefits, especially when you take into account that identifying un-patched machines without such tools is both time consuming and prone to manual errors. Areas of potential exposure can be highlighted by being aware who the user of a certain machine is and whether the device is loaded with the software appropriate for the task. This can be reinforced by ensuring that all software used in the organization have the proper licenses and also by paying for the requisite levels of software assurance, patching and supporting all users contribute to minimising risk.

Advances in technology have prompted the consolidation of health records from various sources to a single database which supports researchers interested in improving healthcare methods and service delivery. Information security breaches in the health care sector have financial implications to various stakeholders including patients, payers like insurances and health care providers like hospitals. A research done by FTC on identity theft, pointed out that in 2005 about 3.7% of people were victims of identity theft - 3% comprised of medical thefts where the stolen personal information was used to receive medical services by the perpetrators (FTC 2007).

The main objective on any healthcare sector is to implement the reforms that aim at improving healthcare service delivery and health information system in the starting point to provide information on the quality of service delivered against needs. Therefore the health information systems provide the means of tracking and measuring these parameters. According to (Brundtland, 2001), health care delivery has been noted as one of the service deliveries that demand high consumer involvement in the consumption process (Peprah, 2014). The consumer is involved in the whole process of the service delivery. Information security breaches can lead to medical errors and cause erroneous clinical diagnosis which can lead to grave consequences. In health care management, a bad service delivery has the potential to cause harm to the patient to some extent it could lead to death of the patient. Due to this, patient satisfaction means good service in the health care system.

2.6 Conceptual Framework

The conceptual framework shows the relationship between service delivery and information security.



Independent variable

Information Security

- Confidentiality
- Availability
- Integrity

Dependent variable

Service delivery

- Quality and timely healthcare provision
- Easy Accessibility to heath care
- Coordination amongst all health providers

Figure 2.1: Conceptual Framework

2.7 Summary of Literature Review

The fast paced developments in technology in the health sector industry has driven the need to implement more robust information systems which are designed more on customer experience. Service is the key driver of strong service delivery results in the industry and research has also shown that good knowledge of your customers which yields customer segmentation for specialized service need to be properly addressed. Customer satisfaction as a result of customer experience promotes customer loyalty, which is critical in the health sector industry.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter details how the research was undertaken. It gives an outline of the research design, population of the study, sample size, data collection process and the methods that were used to collect data from respondents participating in the study and the data analysis techniques that were used.

3.2 Research Design

The study adopted descriptive survey design. A descriptive case study seeks to describe a unit in detail in context and holistically (Kombo & Tromp 2006). Where a deep and rich evaluation information is required, the descriptive case study approach has a rich history of success in applied research. This study sought to investigate the impact of information systems security on service delivery in at PCEA Chogoria mission hospital. Shuttleworth (2008) argues that descriptive research design is a scientific method which includes observing and portraying the conduct of a subject without impacting it in any way.

3.3 Study Population

The study population consist of all the staff at the PCEA Chogoria hospital, working in various departments these includes doctors, nurses, pharmacists, clinical officers, information clerks, and laboratory assistants. The hospital has a total of 135 staffs in various departments.

Table 3.1: The study Population

	Target population
Doctors	15
Nurses	65
Pharmacists	8
Clinical officers	20
Information clerks	5
Laboratory assistants	22
Total	**135**

Source (Researcher, 2016)

3.4 Research Sample

The study used 30% of the entire sample which is a good representation of the entire population. The sample population consisted of 41 (30% of target population) respondents drawn from different departments within the hospital. According to Kothari and Kothari (2003), a sample size of 30% of the population is a representative. Mugenda and Mugenda (2003) further recommends that a sample size of more than 30 respondents or at least 10% of the target population as an appropriate for social sciences.

Table 3.2: Research Sample

	Target population	**Sample ratio**	**Sample size**
Doctors	15	0.3	5
Nurses	65	0.3	20
Pharmacists	8	0.3	2
Clinical officers	20	0.3	6
Information clerks	5	0.3	2
Laboratory assistants	22	0.3	7
Total	**135**		**41**

Source (Researcher, 2016)

3.5 Data Collection

For the purpose of this study, the main method of data collection used was a questionnaire. The questionnaires were left and picked later at an arranged time by the respondents. Where necessary, there were follow-ups via through email, phone calls and visits to ensure high response rate and to assist in cases where respondents needed clarifications.

3.5 Data Analysis

Data from the filled-in questionnaires was coded and keyed into a computer statistics package. Statistical Package for the Social Sciences (SPSS) version 21.0 was used as a tool to aid in data analysis and presentation of the results.

Data collected under section A was analyzed using percentage and frequency distribution to give the overall picture of the respondent and the healthcare facility. The results were presented in tables. The data collected in section B and C was analyzed using descriptive statistics of mean and standard deviation and frequency distribution.

A linear regression model was used in determining the level of influence the independent variables have on dependent variable as shown below:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

Where;

Y = service delivery

β_0 = Constant Term.

β_1, = Beta coefficients.

X_1= information integrity

X_2= information confidentiality

X_3= information availability

ε = Error Term

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1 Introduction

In this chapter, data collected from the 41 respondents chosen from various departments in Chogoria hospital was analyzed. The study was largely completed by doctors, nurses, lab technicians and information clerks. The questionnaires were given to respondents personally or via email. The overall response rate was 85.3%.

4.2 Demographic Characteristics of Respondents

The study considered gender, education level, position, department and working experience as demographic factors that can influence the effect of information security on service delivery.

4.2.1 Distribution of Respondents by Gender

The study sought to establish the gender of the respondents. Table 4.1 presents the findings.

Table 4.1*:* Distribution of Respondents by Gender

Gender	Frequency	Percent
Male	21	60
Female	14	40
Total	**35**	**100**

Source (Researcher, 2016)

Majority of the respondents in this study were male with 60% while 40% were female.

4.2.2 Distributions of Respondents by Job Position

The study sought to establish the position the respondents held in the hospital. The findings were as in Table 4.2

Table 4.2*:* Distributions of Respondents by Job Position

Position	Frequency	Percent
Doctors	5	14
Nurses	16	46
Pharmacists	2	6
Clinical officers	4	11
Information clerks	2	6
Laboratory assistants	6	17
Total	**35**	**100**

Source (Researcher, 2016)

From the findings 46% of the respondents indicated that they have been working in the organization as nurses, 17% as laboratory assistants, 14% as doctors, 11% as clinical officers, while 6% as pharmacists and information clerks respectively. This depicts that most of the respondents in the organization were nurses and thus higher changes of giving reliable information.

4.2.3 Distribution of Respondents by Level of Education

The study sought to establish the level of education of the respondents. The findings were as in Table 4.3.

Table 4.3: Distribution of Respondents by Level of Education

Academic qualification	Frequency	Percent
Certificate	3	8.6
Under graduate	17	48.6
Diploma	5	14.3
Masters	10	28.6
Total	**35**	**100.0**

Source (Researcher, 2016)

From the study, most of the respondents (48.6%) had undergraduate level of education, 28.6% were educated to master's level, 14.3% were educated to diploma level, while the remaining 8.6% were certificate holders. This depicts that the respondents were well educated and are in a position to answer the questions with ease.

4.2.4 Distribution of Respondents by Department They Work

On the department worked majority of the respondents 34% were in surgery department, 17% were in Laboratory and maternity ward department, 11% were in pediatric ward department, 9% were in casualty department, while 6% were in pharmacy and information technology department. This depicts that the respondents were fairly selected to represent each department. Results are as in Table 4.4.

Table 4.4: Distribution of Respondents by Department they Work

Department	Frequency	Percent
Casualty	3	9
Pharmacy	2	6
Pediatric ward	4	11
Laboratory	6	17
Information Technology	2	6
Surgery	12	34
Maternity ward	6	17
Total	**35**	**100.0**

Source (Researcher, 2016)

4.2.5 Distribution of Respondents by Period of Service

Majority of the respondents had served for 11-15 years, 20% had worked for 5-10 years, 17.1% had worked for 16-20 years, 14.3% had served for Over 20 years while 11.4% had worked for Less than 5 years. This indicates that most of the respondents had worked in the hospital for some time and were in a position to provide reliable information required in this study. Table 4.5 presents the findings.

Table 4.5: Distribution of Respondents by Period of Service

Length of service	Frequency	Percent
Less than 5 years	4	11.4
11-15 years	13	37.1
5-10 years	7	20.0
16-20 years	6	17.1
Over 20 years	5	14.3
Total	**35**	**100.0**

Source (Researcher, 2016)

4.3 Extent of information security adoption

This section analyzed data on the extent of information security adoption by looking at the information integrity, information availability and information confidentiality.

4.3.1 Information Integrity

The respondents were asked to indicate the extent to which information integrity is applied in the hospital's information systems.

Table 4.6: Information Integrity

Statement	**Strongly Disagree**	**Disagree (%)**	**Neutral (%)**	**Agree (%)**	**Strongly Agree**	**Mean**	**Std Deviation**
The hospital ensures that all actors add the medical records as soon as they are with the patient to ensure completeness and reliability	5	13	23	23	37	4.158	0.924
Patients medical records are continuously updated as soon as there are changes to ensure reliability	3	7	4	27	59	4.417	0.730
The hospital ensures accuracy of medical records by protecting the information against losses	5	20	22	17	36	4.217	0.612
The hospital ensures the medical records are protected against distortion when transmitting through electronic media i.e e-mails or fax	6	19	13	21	41	4.196	0.912
The hospital ensures the employees doing data entry have basic IT knowledge to key in accurate data in the system	4	6	10	26	54	4.241	0.844
The hospital has ensured that all employees have knowledge of information security policies and guidelines	13	11	14	41	21	3.655	0.947
Chogoria Hospital ensures that issues of information security are addressed promptly	9	12	16	37	26	4.031	0.840
Average	**6**	**13**	**15**	**27**	**39**	**4.131**	**0.830**

Source (Researcher, 2016)

Based on the study findings the overall aggregate mean score with regard to information integrity in Chogoria hospital was 4.131. The respondents strongly agreed that Patients medical records are continuously updated as soon as there are changes to ensure reliability with a mean of 4.4172. On the other hand, respondents agreed to a moderate extent that the hospital has ensured that all employees have knowledge of information security policies and guidelines with a mean of 3.6552. This indicates that information integrity is used in Chogoria hospital in order to improve service delivery continuously updating the patients' medical records as soon as there are changes to ensure reliability.

4.3.2 Information Confidentiality

The study sought to establish the level of information confidentiality applied in the hospital's information systems. Table 4.7 presents the findings.

Table 4.7: Information Confidentiality

Indicator	Very Little Extent (%)	Little Extent (%)	Neutral (%)	High Extent (%)	Very High Extent (%)	Mean	Std Deviation
Passwords have been put in computers for protection of data	4	6	6	27	57	4.7442	0.48961
The hospital has ensured that rooms with patients' information are under lock and key to avoid unauthorized entry	16	6	8	26	44	4.4419	0.33356
The hospital ensures sensitive information is protected and only authorized individuals can have access	9	14	11	19	47	4.6628	0.47372
Medical records are handled by qualified personnel only	11	8	16	22	43	4.546	0.34548
The hospital ensures they provide the user with only the necessary information	13	18	13	21	35	3.930	0.43269
The organization ensures healthcare providers only discuss a patient in need of care	3	12	16	43	26	3.879	0.67739
Average	**9**	**11**	**12**	**26**	**42**	**4.367**	**0.45874**

Source (Researcher, 2016)

According to the study findings the overall aggregate mean score with regard to level of information confidentiality in Chogoria hospital was 4.367. To a very large extent, respondents were on the view that passwords have been put in computers for protection of data with a mean of 4.7442. On the other hand, respondents agreed to a moderate extent that the organization ensures healthcare providers only discuss a patient in need of care with a mean of 3.8793. This indicates that Chogoria hospital has put security measures like use of passwords to protect data and ensure patients' information is confidential.

4.3.3 Information Availability

The study sought to establish the level of information availability applied in the hospital's information systems. The findings are as in Table 4.8.

Table 4.8: Information Availability

Indicator	**Very Little Extent (%)**	**Little Extent (%)**	**Neutral (%)**	**High extent (%)**	**Very High extent (%)**	**Mean**	**Std Deviation**
The Hospital ensures that the information system is always up and running	15	5	10	24	46	4.1001	0.386
Chogoria hospital ensures that the flow of information in the information system is traceable through logging and documentation	5	10	5	24	56	4.3409	0.2959
The hospital ensures that there is off-site backup of patients' information	3	4	36	41	16	3.5628	0.4772
The organization ensures that the case record follows the patient in the organization	12	20	31	9	28	3.2372	0.3797
Healthcare professionals have access to patient's information when needed	10	11	7	14	58	4.4425	0.4861
Medical records are sorted continuously for ease of retrieval	11	12	6	23	48	4.1419	0.3356
Average	**9**	**10**	**16**	**23**	**42**	**3.971**	**0.393**

Respondents agreed to a very high extent that providers of health services can access patient's information whenever they require it with a mean of 4.4425. However, respondents were neutral on the statement that the respondents moderately agreed that the organization ensures that the case record follows the patient in the organization with a mean of 3.2372. This indicates that information is readily available in Chogoria hospital in order to improve service delivery.

4.3.4 Service Delivery

The respondents were asked to indicate the extent to which information security affects service delivery in the hospital. The findings are as in Table 4.9.

Table 4.9: Service Delivery

Statement	**Very Little Extent (%)**	**Little Extent (%)**	**Neutral (%)**	**High extent (%)**	**Very High extent (%)**	**Mean**	**Std Deviation**
Patients' medical records are easily retrieved from the information systems when needed	12	20	9	31	28	3.8302	0.4369
Patients take shorter time in queues to get served	16	12	12	20	40	4.231	0.388
There is better patients' medication management due to availability of information	0	12	28	28	32	4.0419	0.2989
There is improved and accurate clinical decisions	12	12	16	22	38	4.1628	0.4772
Medical history information is available to avoid duplication of diagnostic imaging and testing	4	12	20	44	20	3.7355	0.3797
There is effectiveness and efficiency of healthcare services delivery	8	16	4	30	42	4.4442	0.4861
Average	**9**	**14**	**15**	**29**	**33**	**4.074**	**0.411**

Source (Researcher, 2016)

The findings revealed that service delivery at the hospital was satisfactory with an average mean score of 4.074. The highest mean score was reported with regards to the effectiveness and efficiency of healthcare services delivery as shown by a mean of 4.4442 while the lowest mean score was reported with regard to the statement that medical history information is available to avoid duplication of diagnostic imaging and testing as indicated with a mean of 3.7355. This implies that most patients are given satisfactory medical care.

4.4 Relationship between Information Security on Service Delivery

4.4.1 Correlation Analysis

In order to examine the level at which the variables under study were related, Karl Pearson's as a measure of coefficient of correlation was used. The Pearson product-moment correlation coefficient denoted as *r* is primarily used to gauge the level of association between two variables and ranges from +1 to -1. Lack of relationship between variables is denoted by zero value. Where there is a positive relationship, a figure greater than zero is in indicated whereas a negative relationship is indicated by a figure less than zero. The findings are as at Table 4:10

Table 4. 10: Correlation Analysis

	Service Delivery	Information Integrity	Information Confidentiality	Information Availability
Service delivery(r)	1.000			
(p) Sig. (2 tailed)				
Information integrity (r)	0.679	1.000		
(p) (2 tailed)	0.009			
information confidentiality (r)	0.612	0.326	1.000	
	0.013	0.021		
Information availability (r)	0.574	0.254	0.076	1.000
(p) Sig. (2 tailed)	0.026	0.123	0.046	

The findings reveals that there is a significant positive relationship between Information integrity and service delivery (r = .679, P-value < 0.009). This implies that Information integrity influences service delivery in Chogoria hospital. The findings also disclosed a significant positive relationship between information confidentiality and service delivery (r = .612, P-value < 0.013). Thus, implying that information confidentiality influences service delivery in Chogoria hospital.

The findings indicated a significant positive relationship between information availability and service delivery (r = .574, P-value < 0.0426) thus, depicting that information availability influences service delivery in Chogoria hospital.

4.4.2 Regression Analysis

A multiple regression analysis was undertaken to further gauge the association among the independent variables on service delivery in Chogoria hospital. To aid this, statistical package for social sciences (SPSS V 21.0) was used to facilitate the outcomes of the multiple regressions for the study.

The extent to which changes in the dependent variable (service delivery) is influenced by all the three independent variables (Information integrity, information confidentiality, and information availability) is explained by the coefficient of determination.

Table 4.11: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	. 896[a]	.802	.775	0.0131

a. Predictors: (Constant), Information integrity, information confidentiality, and information availability

b. Dependent Variable: Service Delivery

Table 4.11 shows model summary of regressed variable of the study. The three independent variables in the study explain 80% effect of level of information security as applied by the hospital and how it affects service delivery as represented by R Squared (Coefficient of determinant). This therefore means 20% are other factors not studied in this research that influence service delivery.

Table 4.12: ANOVA (Analysis of Variance)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.942	3	2.314	6.51	.001[a]
	Residual	11.005	31	0.355		
	Total	17.947	34			

a. Predictors: (Constant), Information integrity, information confidentiality, and information availability

b. Dependent Variable: Service Delivery

The model summary also indicates that the regression model predicts the dependent variable significantly well. The F test indicates the statistical significance of the regression model that was used. The P=0.001, which is less than 0.05 indicates that, overall the regression model statistically and significantly predicts the outcome variable that is good fit for the data.

Table 4.13: Coefficient of Determination

	Unstandardized Coefficients			**Standardized Coefficients**	
	B	**Std. Error**	**Beta**	**t**	**Sig.**
(Constant)	7.232	0.451		16.035	0
Information integrity	0.802	0.243	0.126	3.3	0.0011
information confidentiality	0.769	0.261	0.146	2.946	0.0036
information availability	0.473	0.213	0.045	2.22	0.0274

The overall equation model for service delivery, Information integrity, information confidentiality, and information availability was as follows:

$Y_{bt} = 7.232 + 0.802X_1 + 0.769X_2 + 0.473X_3$

From the model, in any given time, the service delivery will be 7.232 when all the predictor values are zero. The model indicates that when the value processed through information integrity changes by one unit the service delivery will increase by 0.802. In addition, if information confidentiality changes by one unit the service delivery increases by 0.769. Further, the study findings revealed that when the information availability changes by one unit the service delivery will increase by 0.473.

To test the significance of each individual variable which was based at 0.05 the t-test was carried out. The result indicates the information confidentiality and information availability have a value of 0.0036 and 0.0274 against the service delivery in the model respectively. This shows that the relationship between service delivery, information confidentiality and information availability is significant. The relationship between service delivery and Information integrity recorded at rate of 0.0011 which is significant since it's less than p-value (P.0.05).

4.5 Discussion of Findings

The result indicates the information confidentiality and information availability have a value of 0.0036 and 0.0274 against the service delivery in the model respectively. This shows that the relationship between service delivery, information confidentiality and information availability is significant. The relationship between service delivery and Information integrity recorded at rate of 0.0011 which is significant since it's less than p-value (P.0.05). Similar to the study findings, Brundtland, (2001) noted that health care delivery has been noted as one of the services deliveries that require high involvement of the consumer in the consumption process (Peprah, 2014). The consumer is involved in the whole process of the service delivery. Information security breaches can lead to medical errors and cause erroneous clinical diagnosis which can lead to grave consequences.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the study findings, conclusion and recommendations drawn from the study findings.

5.2 Summary of the Findings

The study sought to establish the level of information security adoption at PCEA Chogoria mission hospital and to examine the relationship between information security and service delivery in PCEA Chogoria mission hospital. The study revealed that to a very high extent, information confidentiality enhances service delivery. Most respondent agreed to a large extend that passwords have been put to protect.

Further, the study revealed that to a higher extent that patients' information was readily available to health providers and this enhanced service delivery in Chogoria hospital. It was also evident to a very high extent that healthcare providers had accessibility to patient's information when needed. However, respondents moderately agreed that the organization ensures that the case record follows the patient in the organization.

The study also reveals that to a high extent the level of information security implementation affected service delivery at Chogoria hospital. From the regression model, the results indicated that in any given time, the service delivery will be 7.232 when all the predictor values are zero. The model indicates that when the value processed through information integrity changes by one unit the service delivery will increase by 0.802. In addition, if information confidentiality changes by one unit the service delivery increases by 0.769. Further, the study findings revealed that when the information availability changes by one unit the service delivery will increase by 0.473. This implies that changes in level of information security affects service delivery.

To test the significance of each individual variable which was based at 0.05 the t-test was carried out. The result indicates the information confidentiality and information availability have a value of 0.0036 and 0.0274 against the service delivery in the model respectively. This shows that the relationship between service delivery, information confidentiality and information availability is significant. The relationship between service delivery and Information integrity recorded at rate of 0.0011 which is significant since it’s less than p-value (P.0.05).

5.3 Conclusion

Based on the study findings, the study concludes that information integrity is used in Chogoria hospital in order to improve service delivery continuously updating the patients’ medical records as soon as there are changes to ensure reliability. In addition, the study concludes that information security in the health sector entails protection of patients’ information to ensure that its available, it has integrity and its accorded confidentiality it deserves during a patient’s treatment and management. The study shows there is a positive relationship between the level of adoption of information security and service delivery in the health sector. Also, the study concludes that information confidentiality is used in Chogoria hospital in order to improve service delivery as passwords have been put in computers for protection of data, the hospital ensures sensitive information is protected and only authorized individuals can have access, and that medical records are handled by qualified personnel only.

The study also concludes that while new technologies emerge for managing health information, the adoption of it comes with great threats and challenges to information’s security. The management should therefore increase information security awareness by training staff on the risks, threats, policies and guidelines this will greatly reduce information confidentiality, integrity and availability breaches. Other measures that can be employed to mitigate information security risks are use of access controls, giving file permissions, use of encryption, biometrics to ensure that data integrity is attained. To ensure availability of information to all health care providers, the information system should always be up and running, the software and hardware should be updated with latest version, there should be a disaster recovery program in place and physical protection of information by use of lockable doors and windows in rooms where computers, servers, files are stores to ensure they are fire proof, water proof and burglar proof.

The study further concludes that information availability is used in Chogoria hospital in order to improve service delivery, Healthcare professionals have access to patient's information when needed, and that Chogoria hospital ensures that the flow of information in the information system is traceable through logging and documentation

5.4 Study Limitations

The study findings were limited to Chogoria hospital and did not cover other health care institutions in the country and therefore the results cannot be generalized to indicate that information security affects service delivery in all heath care facilities. There were limited finances and inadequate time to carry out an extensive study on level of adoption of information security and service delivery in the health sector.

5.5 Recommendations

The study findings suggest that information security has a positive relationship on service delivery in the health sector. The study recommends that information being a key asset in any healthcare facility needs to be adequately protected. Therefore there is need to develop guidelines and standards that enable adoption of best information security practices and an adequate and acceptable level of security is achieved.

The study reveals that information security measures affect service delivery and therefore the top management should invest more resources in information systems and come up with effective guidelines and policies to ensure accountability to patient's information that is handled. The study recommends all employees be trained on information security policies and guidelines to create more awareness on the importance of securing the health information systems.

5.6 Suggestions for Further Studies

A similar study can be carried out to cover other health care institutions in Kenya to determine whether the findings will be similar. Moreover, the study can include a larger sample size to include hospitals in various counties. This would enable further analysis that establish more variables of the level of adoption of information security that may affect service delivery in the health sector in Kenya.

REFERENCES

Appari, A. & Eric Johnson, M. (2010). Information security and privacy in healthcare: current state of research, *Int. J. Internet and Enterprise Management*, Vol. 6, No. 4, pp.279–314

Applebaum, P.S. (2002). 'Privacy in psychiatric treatment: Threats and response', American Journal of Psychiatry, Vol. 159, pp.1809–1818.

Athanassopoulos A.D.,(2010) Customer satisfaction cues to support market segmentation and explain switching behaviour, Journal of Business Research. Volume 47, Issue 3, Pages 191-207, 2000

Bansal, M.K. (2004). Optimising value and quality in general practice within the primary health care sector through relationship marketing: a conceptual framework. *International Journal of Health Care Quality Assurance, 17*(4),180-188.

Brundtland G. H. (2001). *Improving health systems' performance, OECD.*

Calder, A. & Watkins, S. (2008). IT Governance: A Manager's guide to Data Security and ISO27001/ISO 27002, 4th Edition. London: Kogan Page Limited.

Capra, F. (1997). *The web of life.* New York: Doubleday-Anchor Book

Donaldson, L. (1996). The normal science of structural contingency theory'in The handbook of organization studies. SR Clegg, C. Hardy, and W. Nord (eds), Ch. 1.2.

Drazin R., & Van de Ven, A. H., (1985). The concept of fit in contingency theory. B. M. Staw, L. L. Cummings, eds. *Research in Organizational Behavior,* Vol. 7. JAI Press, Greenwich, CT, 333–365.

Elky, S. (2006). An introduction to information systems risk management.

Felicia (2011) IADIS Information Systems.

FTC – Federal Trade Commission (2007) ―2006 Identity Theft Report,‖ last accessed on June18,2008, ttp://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Grimson, J., Grimson, W., & Hasselbring, W. (2000). The SI challenge in health care. *Communications of the ACM*, *43*(6), 48-55.

Helmsing, A. H. J. (2005). Local Government Central Finance. An Introduction: New York USA.

Heskett, C. (1987). A service quality model and its marketing implications, *European Journal o f Marketing,* Vol. 18, Number 4, p.36-44.

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248.

Humphrey, W. (2010) A Discipline for Software Engineering, Addison-Wesley, Reading, MA. IETF. The Internet Engineering Task Force. http://www.ietf.org/

ISACA, A. (2009). Introduction to the Business Model for Information Security.

ISO/IEC (2002) *for structuring comprehensive information technology for management in organizations*". ISSN 2237-4558.

Kiptoo, T. (2013). *Adoption of computer-based management information systems on quality service delivery in middle level institutions in Kenya: a case study of Ol'lessos technical training institute.* (Doctoral dissertation).

Kombo D & Tromp D (2006). Proposal and Thesis writing – An introduction: Paulines publications, Africa. Nairobi

Koskosas, J.V & Asimopoules. N (2011*).* "Information system security goals". *International Journal of Advanced Science and Technology*. Vol. 27

Kothari, C. R. (2003). *Research methodology: Methods and techniques*. New Age International.

Larsen, .H.M, Pedersen .K. M & Andersen K. V. (2006). "IT governance *reviewing 17 IT governance tools and analysing The Case of Novozymes A/S"* .Proceedings of the 39th Hawaii International Conference on Systems Science.

Marczyk, G., DeMatteo, D. & Festinger, D. (2005). *Essentials of research design and methodology. New Jersey: John Wiley & Sons, Inc.*

Mattrod, K. (2009). Identifying Best Practices for Security in Patient Health Information Systems (E-health Solutions) in Resource Limited Setting: Malawi Case on Establishment of National Health Data Repository Centre.

McCumber, J. (2005). *Assessing and Managing Security Risks in IT Systems*, Auerbach Publications.

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, *47*(7), 25-28.

Mugenda, O. M. (1999). *Research methods: Quantitative and qualitative approaches*. African Centre for Technology Studies.

Muratha, R. K. (2012). *Information security practices in the Kenyan Capital Market* (Doctoral dissertation).

NIST (2011). Handbook, *Special Publication 800-12 [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*.

Nyandiere, C. (2006). Increasing role of computer-based information systems in the management of higher education institutions. In *Proceedings of the Annual Strathmore University ICT Conference*.

Oboth, J. (2011). Decentralization and service delivery: *Constraints and Controversies.* Kampala: Makerere University Library

Osborne, M. (2006). *How to cheat at managing information security*. Syngress.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37-49.

Peprah, A. A. (2014). Determinants of patients' satisfaction at Sunyani regional hospital, Ghana. *International Journal of Business and Social Research*, *4*(1), 96-108.

Rajnish, K., Sharma, S., & Negi, J. (2010). *Proceedings of the 2010 International Conference on Industrial Engineering and Operations Management.* Dhaka, Bangladesh: s.n.

Rao, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA privacy rule compliance: an interpretive study using Norman's action theory. *Computers & security*, *31*(2), 206-220.

Rudolph, K., Warshawsky, G. and Numkin, L. (2002). *Computer Security Handbook*, 4th ed. New York: John Wiley & Sons, Inc.

Shuttleworth, M. (2008). Descriptive Research Design-Observing a Phenomenon. *url: http://explorable. com/descriptive-research-design, date retrieved: February*, *10*, 2013.

Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Swanson, M., & Guttman, B. (2006). *Generally accepted principles and practices for securing information technology systems* (pp. 800-14). National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Wade, M., & Hulland, J. (2004). Review: The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS quarterly*, *28*(1), 107-142.

World Health Organization. (2008). The world health report 2008: primary health care now more than ever. Geneva; 2008.

Appendix I: Questionnaire

INFORMATION SECURITY AND SERVICE DELIVERY IN THE HEALTH SECTOR

Instructions

This questionnaire is purely for academic project and the information you will give shall be treated with high level of confidentiality.

Section A: General Information

1. Please indicate your position in the hospital (Optional)

   ____

2. Please indicate your gender? Male [ ] Female [ ]
3. Please indicate which department you work in?

   Casualty [ ] Laboratory [ ]

   Finance [ ] Information Technology [ ]

   Pharmacy [ ] Surgery [ ]

   Pediatric ward [ ] Maternity ward [ ]

   Other (Specify)________________________

4. How long have you worked in this organization?

   Less than 5 years [ ] 5-10 years [ ]

   11-15 years [ ] 16-20 years [ ]

   Over 20 years [ ]

5. What is your highest academic qualification?

   Certificate [ ] Diploma [ ]

   Graduate [ ] Masters [ ]

   Other (Specify)________________

Section B: Information Integrity

6. In a 5-point scale where: 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=strongly agree, tick to indicate the extent to which information integrity is applied in the hospital's information systems.

Indicator	**1**	**2**	**3**	**4**	**5**
The hospital ensures that all actors add the medical records as soon as they are with the patient to ensure completeness and reliability					
Patients medical records are continuously updated as soon as there are					

changes to ensure reliability					
The hospital ensures accuracy of medical records by protecting the information against losses					
The hospital ensures the medical records are protected against distortion when transmitting through electronic media i.e e-mails or fax					
The hospital ensures the employees doing data entry have basic IT knowledge to key in accurate data in the system					
The hospital has ensured that all employees have knowledge of information security policies and guidelines					
Chogoria Hospital ensures that issues of information security are addressed promptly					

Information Confidentiality

7. In a 5-point scale where: 1= very little extent, 2=little extent, 3= neutral, 4= high extent, 5=very high extent, tick to indicate the extent to which Patients' information confidentiality is applied in your organization's information systems.

Indicator	**1**	**2**	**3**	**4**	**5**
Passwords have been put in computers for protection of data					
The hospital has ensured that rooms with patients' information are under lock and key to avoid unauthorized entry					
The hospital ensures sensitive information is protected and only authorized individuals can have access					
Medical records are handled by qualified personnel only					
The hospital ensures they provide the user with only the necessary information					
The organization ensures healthcare providers only discuss a patient in need of care					

Information Availability

8. In a 5-point scale where: 1= very little extent, 2=little extent, 3= neutral, 4= high extent, 5=very high extent, tick to indicate the extent to which Patients' information is available in your organization's information systems

Indicator	**1**	**2**	**3**	**4**	**5**
The Hospital ensures that the information system is always up and running					
Chogoria hospital ensures that the flow of information in the information system is traceable through logging and documentation					
The hospital ensures that there is off-site backup of patients' information					
The organization ensures that the case record follows the patient in the organization					
Healthcare professionals have access to patient's information when needed					
Medical records are sorted continuously for ease of retrieval					

Section c: Service delivery

9. Kindly indicate the extent to which application of information security strategies has impacted service delivery in the hospital. 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=strongly agree

Indicator	**1**	**2**	**3**	**4**	**5**
Patients' medical records are easily retrieved from the information systems when needed					
Patients take shorter time in queues to get served					
There is better patients' medication management due to availability of information					
There is improved and accurate clinical decisions					
Medical history information is available to avoid duplication of diagnostic imaging and testing					
There is effectiveness and efficiency of healthcare services delivery					

THANK YOU FOR YOUR PARTICIPATION