International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 88-94
Published Online November 2019 in IJEAST (http://www.ijeast.com)

A FRAMEWORK FOR EFFECTIVE INFORMATION SYSTEM SECURITY MANAGEMENT IN KATSINA STATE HEALTHCARE ORGANIZATIONS

Attahiru Saminu
Department of Library and Information Science,
Hassan Usman Katsina Polytechnic

Abstract— Information security has significant role in Healthcare organizations. The Electronic Health Record (EHR) and patient's data is considered as very sensitive information in Healthcare environment. This study explored the current countermeasures used and how employers shared their knowledge about the existence of information security countermeasures in order to protect Healthcare Records from possible security threats in healthcare organization. The choice of this study is qualitative research method. It seems too obvious that 'the choice of the research method ought to be determined by the nature of the research problem. The population of the study is made up of 564 staff in the Katsina General Hospital. The researchers have constructed an interview guide that covers eleven relevant questions to four categories of staff which include 5 IT personnel, 15 medical Doctor, 15 nurses and 5 management staff/Administrators in all the three general hospitals located in the study areas were identified as targeted group to meet the requirements for answering the research questions. A conceptual framework was proposed, this framework guides the study of information security countermeasures in healthcare organization in relation to knowledge sharing among employers. The results of the case study shown that, deterrent action, organizational action and preventive action are the countermeasures partially practiced and there is lack of knowledge sharing on the existence of information security countermeasures among employers, some factors were found to be the key resistance factors why employers are not willing to share their knowledge; these include behavior, low security awareness, personality differences, top management commitment and educational background.

Keywords— **Electronic Healthcare Records, Security and Management, Countermeasures, Knowledge Sharing**

I. INTRODUCTION

Information is very vital for the effective management and development of better healthcare services at all levels of the health pyramid. Medical or health information consist of medical history reports, patient discharge summaries and drug information, which form an individual's Protected Health Information (PHI) [1].

Medical and health information is tremendously sensitive and volatile in nature. Security is therefore very important as any interference or compromise, may lead to issues such as erroneous diagnosis or treatment, and in extreme cases, death. Owners and users of medical information expect confidentiality, an act of secrecy and integrity by ensuring the information is honest and true.

The flow of information amongst diverse healthcare practitioners can either be in non-electronic format or electronic format. The flow of information in non-electronic formats involves the exchange of information amongst healthcare practitioners in paper based forms while the flow of information in electronic formats involves the use of Information and Communication Technology (ICT) tools to exchange information. Nevertheless, the flow or exchange of information within a Health Information System is plagued with several challenges especially in developing countries such as Nigeria. This is because data collection is majorly manual. Furthermore, there is significant fragmentation and duplication in data collection and storage. Hence, healthcare organizations find it difficult to effectively manage information as it flows within or across the continuum of care. Therefore, the information exchanged is usually untimely. Consequently, these results in inappropriate decision making and care management, inapt research, inappropriate quality assessment, ineffective planning, increase in medical errors and cost as well as a decline in the quality of patients' care.

There has been limited published academic research to date that specifically focuses on information security counter measures in developing countries. At the same time, the profile of security is increasing due to the recognition in its important role in protecting information. Therefore, the effective management of security risks ultimately requires appropriate implementation of information security management. This research focuses on the Frameworks and counter measures that are used to help in mitigating security challenges in Healthcare organizations.

II. RESEARCH OBJECTIVES

The main objective of this research is to propose a framework that can be used to improve Information Security in Healthcare organizations in Katsina State.
Specific objectives include:

I. To identify the Information System counter measures that healthcare organization use to mitigate security threats.
II. To identify the ways employees share knowledge about information security issues and counter measures.
III. To evaluate the effectiveness of information security counter measures based on the proposed framework from Katsina State Healthcare organizations perspective.

III. RELATED WORK

All According to [2], the application and implementation of Electronic Healthcare Records (EHR) in various healthcare organizations are driven by the needs to facilitate clinical and administrative processes, to reduce medical errors and to reduce health care cost. As identify by [2], an Electronic Healthcare Records (EHR) system allows access to process notes or procedural data, and may support other functions include Computerized Provider Order Entry (CPOE), Picture Archiving Communication System (PACS), and Clinical Decision Support System (CDSS). Tools to support administrative procedures such as billing and scheduling are also becoming common EHR features. The use of EHR can facilitate clinical decision-making and minimize the potential for mistakes due to the inaccuracy and incompleteness of paper records [3].

"In UK, for example, the Government's effort of building the National database of medical records called the National Health Service (NHS) was driven by a vision to improve the standard and quality of healthcare"[4].Similarly, [5] described the Australia's national integrated Health Records and information System (IHRIS) as a system designed to satisfy the needs of clinicians as well as other users such as planners, administrators, researchers and policy makers.

Electronic Healthcare Record has been adopted by various Nigeria healthcare institutions based on the similar ground. The Nigerian Electronic healthcare system referred to as national health system is decentralized into a three level structure with incumbency at the federal, state and local government levels with currently all three levels being involved to some extent in all major health system functions which includes stewardship, financing and service provision. It is a known fact that the overall health of a nation is highly dependent on the efficient and successful implementation of primary health care services or community level delivery. This integration is expected to deliver healthcare to promote health status of the people. Four pilot projects included in the MSC telemedicine model are Customized Personalized medical Education, Tele-consultation and Lifetime Health plan (LHP) [5].

LHP describes each resident to have a smart card containing a subset of the data in the EHR by which he or she receives "seamless continuous quality care" across a range health facilities and healthcare providers in Nigeria. The objective of this is to achieve the goal of a nation of "health individuals, families and communities" [6].According to [2], the main reason for massive failure of technological infrastructure's implementation is that the implementation process is treated as a technological challenges while the human and organizational issues are not fully treated.

Keeping vital information secure is imperative to all organizations. This is done by practicing information security, and the work must start with a management supporting the co-workers and also by educating end users and organization members in information security (SEMA, 2005). Information security is about protecting information from accidents, breaches or other events that could make it harder to understand the information. Information security is practiced in organizations that tend to rely on information, and a certain lack of information could harm the organization. This mean that information security is important to all businesses as information is very important for businesses.

ICTs will help address concerns for healthcare systems as ICTs have much potential. They can expose inconsistencies and inefficiencies in organizations, promote self-care, facilitate joined-up healthcare provision, make service-providers more accountable and even help coping with workforce shortages if correctly used. These potentials could allow ICTs to redesign the organizational structure of healthcare (Ministry of Health and Social Affairs, 2006). Technological developments will drive patient-focused healthcare to be anywhere anytime and on-demand. Electronic records are destined to become important for the overall information environment in healthcare.

Information Systems effectiveness has been extensively studied over the past years because of their potential importance in the field of Information Technology [7]**.** However there is a lack of understanding and knowledge on how security measures and organizational factors can influence the level of security effectiveness in IT organizations in the current literature [7]. [8] Suggested that IS security administrators consider the following to improve the **IS** security level in their organizations.

- IT organizations should monitor and enforce policy and distribute information about organizational guidelines for acceptable system usage.
- Environmental factors such as the tightness of these security environment and visibility of the security administrators should be taken into consideration to reduce the number of computer abuse incidents.
- **IT** organizations should put it more effort in security issues by expanding the staff hours on IS, security.

Many researchers agreed with the idea that the human mind is composed of rational and emotional components. A few authors state that security behavior depends on a person's attitude and beliefs. Believe is cognitive information without emotional component, but attitude is evaluation or emotional response [9].Some other author's [10] proposed the ABC Model where employee attitude to information security issues is based on rational component (cognition) emotional component (affect) and behavior.

A- Emotional aspect of attitude for example, for example, feeling like grief, pain, fear, guilt.

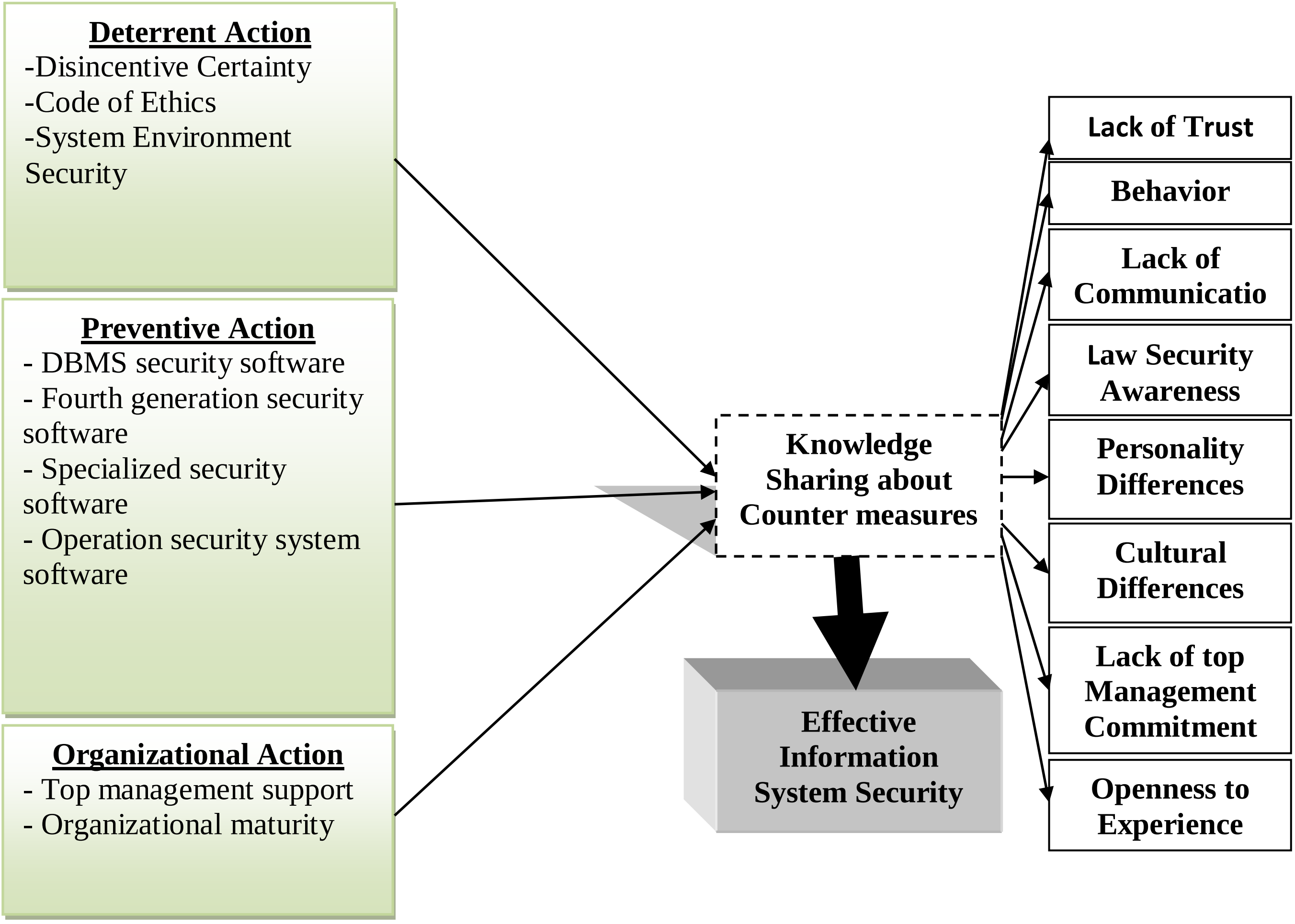
B- Behavior component is derived from fact that our behavior also gives feedback to attitude

C- Cognitive or thoughtful aspect of attitude.

The implementation of health information technology and electronic exchange of patients' information will resulted in privacy violations and security breaches for information security, knowledge sharing is aiming at to make sure that the knowledge can be transfer among employees, disseminate and distribute to make it available to those who require [11]. Meanwhile in [12] , they have identified that knowledge gap and flow as part of knowledge sharing among healthcare providers analysis. [13] Adopted Nonaka's modes of knowledge creation between tacit and explicit knowledge to ensure that knowledge can be created and disseminated, [[11] Identified the key resistance factors in knowledge sharing towards information security culture in healthcare organization, some key resistance factors highlighted are lack of top management commitment, behavior, lack of trust , personality differences, lack of communication, low security awareness, cultural differences, and openness to experience.

The Security, confidentiality and privacy of electronic health care information are the main concerns in healthcare informatics. These aspects are distinct but inextricably linked [14]. Base on the literature reviewed, conceptual framework Information Systems Security (ICT-ISS Model) is developed that mapped Disincentives Certainty, Systems Environment Security Control, Codes of Ethics, Software Security Controls, Top Management Support, Organizational Maturity and Conceptual Model of Knowledge Sharing into a single conceptual framework for information security.

Figure 1: Information and Communication Technology-Information Security System Model (ICT-ISS Model)



IV. RESEACH METHOD

The choice of this study is qualitative research method. For the purpose of this study, the targeted population are all staff of the Katsina State General hospitals that made up of (564) staffs. The researcher engaged both purposive and stratified random sampling. Purposive sampling was used to target those who might be in a privileged position to provide more information while stratified random sampling was used to identify a few members of the general population and solicit their views on the subject.

The researcher has constructed an interview guide that covers eleven relevant questions to four categories of staff

Which include 5 IT personnel, 15 medical Doctor, 15 nurses and 5 management staff/Administrators in the study area were identified as targeted group to meet the requirements for answering the research questions out of the total population of 564 regarding the Effective used of information security counter measures to prevent Health Records from security threats, risks and the impact of knowledge sharing on these counter measures among employees. In order to ensure the research validity, sample size is carefully identified, so that it can represent the whole group from which it were taken.

V. RESULT AND DISCUSSION

Although Katsina state general hospital was founded almost 22 years ago, information security issues have only been considered in the last 2 to 3 years. Control of patient data, financial loss, inability to deliver medical records and negative publicity are the main reasons to provide information security with the organization, so information security management should be applied to all departments and support processes, as well as counter measures for risk reduction, mitigation or transference should be chosen

A. Counter measures (Effectives of Information Systems Security in Katsina State General Hospitals)

During the interviews with the staff responsible for information security, human resources and technologies some questions were asked to find out the Information system security counter measures used by Katsina State general hospitals to protect Electronic Health records as;

i. How information security counter measures mitigate the security threats of Electronic Medical Records

The interviewees described how they perceived various counter measures that are used for reducing and mitigating internal threat in the organization. The names of interviewees and other demographic information are not provided within the research as anonymity must be provided. Only the length of time of working within the organization was asked, because it reveals when the employment procedure were accomplished, all security related documentation explained and how often training or awareness program activities have been performed. The following counter measure groups were identified with the Katsina state:

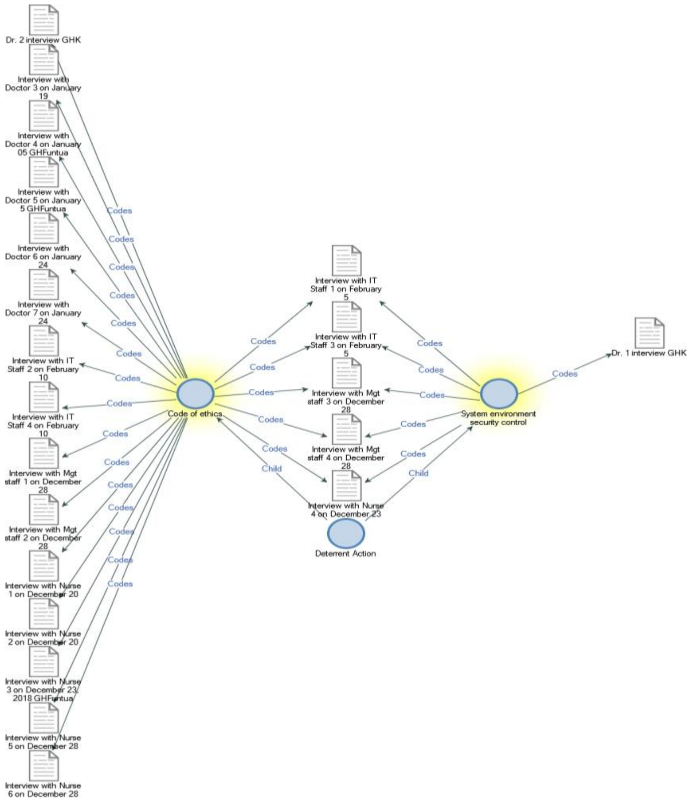
a. Deterrents actions

Majority of interviewees believed that Katsina State health care have sensitive information so there should be high security in order to prevent sensitive information from access of unauthorized users.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. Example of deterrents include computer security awareness training, guidelines, policy statements and minimum set of standards for personnel behavior and company personnel rules that contain specific conditions for the acceptable use of the system. Three main elements in deterrent actions are ***disincentives certainty, systems environment security control*** and ***codes*** of ***ethics.*** Disincentives certainty defines that when the risk of punishment is high and penalties for violation are severe, potential offenders will be inhibited from committing anti-social acts. Systems environment security control talks about the tightness of the security environment and visibility of the security administrators that may correlate negatively with computer abuse. Finally codes of ethics refer to the rules and standards governing the conduct of an individual with others.

It is evident that most of the participants wish for more focus on code of ethics and System environment security control rather than more focus on Disincentive certainty. They argue that, in the long run, it will be safer for patients if information is made available. Of course, proper measures must be carried to ensure that unauthorized access does not occur. We should focus on why people act the way they do. Why do people print electronic records? Something that is mentioned, concerning education and printing, is that this could be solved after newer generations take over totally in healthcare. As Nurse says; control measures is the best. This often requires additional security control in compliance which is to monitor measure and report compliance with security and privacy requirements (see figure 2).

Figure 2, the Deterrents actions based on the interviewees response


Dr. 2 interview GHK
Interview with Doctor 3 on January 19
Interview with Doctor 4 on January 05 GHFuntua
Interview with Doctor 5 on January 5 GHFuntua
Interview with Doctor 6 on January 24
Interview with Doctor 7 on January 24
Interview with IT Staff 2 on February 10
Interview with IT Staff 4 on February 10
Interview with Mgt staff 1 on December 28
Interview with Mgt staff 2 on December 28
Interview with Nurse 1 on December 20
Interview with Nurse 2 on December 20
Interview with Nurse 3 on December 23, 2018 GHFuntua
Interview with Nurse 5 on December 28
Interview with Nurse 6 on December 28
Code of ethics
Interview with IT Staff 1 on February 5
Interview with IT Staff 3 on February 5
Interview with Mgt staff 3 on December 28
Interview with Mgt staff 4 on December 28
Interview with Nurse 4 on December 23
Deterrent Action
System environment security control
Dr. 1 interview GHK
Codes
Child

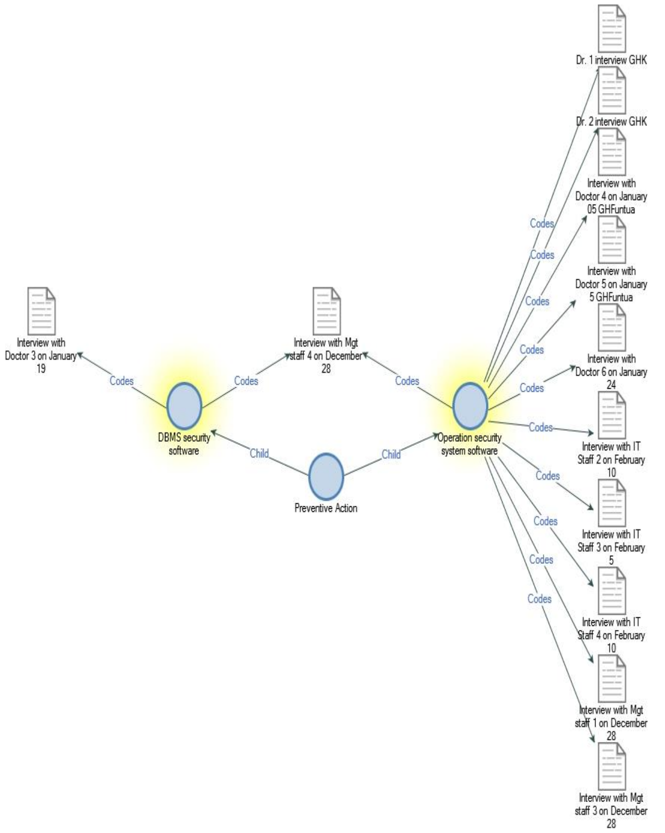
In general, Doctor 2, 3, 4, 5, 6, IT staff 2, 4, Management staff 1, 2 and Nurse 1, 2, 5, and 6 reacted on the use of code of ethics while IT staff 1, 3 Management staff 3, 4 and Nurse 4 responded on the provision of both the code of ethics and system environment security control as shown in appendix 4.1. The findings are also consistent with the findings from Information System Security Counter measures literature [15] pointed the impact of deterrent actions to healthcare organization throughout the medical processes.

a. Prevention actions

Preventive actions enables only authorized users to access a computerized system. There are four main types of security software controls. They are operating system security software control, database management system (DBMS) security software control, fourth generation security software control and specialized security software control. These software controls are intended to insist free use of computing resources thus increase the level of security effectiveness

The interview shows that only Doctor 3 has a view that DBMS security control is provided to protect the EMR from attacked while on the other hand, Doctor 1, 2, 4, 5, 6, IT staff 2, 3, 4 and Management staff 1 and 3 said Operating system software is very available and functioning. Management staff 4 is on the view that, both are provided refer to figure 3.

Figure 3, the Prevention actions based on the interviewee's responses


Dr. 1 interview GHK
Dr. 2 interview GHK
Interview with Doctor 4 on January 05 GHFuntua
Interview with Doctor 5 on January 5 GHFuntua
Interview with Doctor 6 on January 24
Interview with Doctor 3 on January 19
Codes
DBMS security software
Codes
Interview with Mgt staff 4 on December 28
Codes
Operation security system software
Child
Preventive Action
Child
Codes
Interview with IT Staff 2 on February 10
Interview with IT Staff 3 on February 5
Interview with IT Staff 4 on February 10
Interview with Mgt staff 1 on December 28
Interview with Mgt staff 3 on December 28

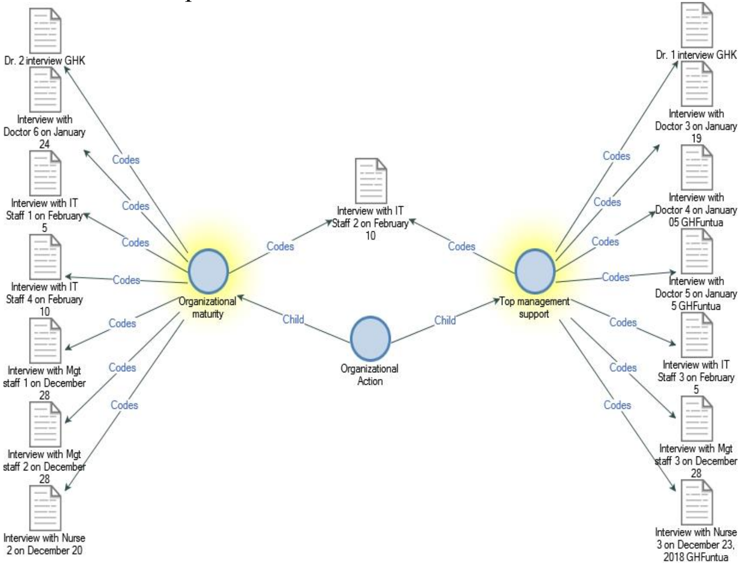
Preventive actions enables only authorized users to access a computerized system [11]. The study investigated four types of preventive actions: the DBMS security software, fourth generation security software, specialized security software and operation system security software. Where found the partial application of DBMS security software and Operation System software by IT staff, Doctors and Management staff, preventive actions is very important full application of it will provide security to entire systems.

a. Organizational actions

Organizational actions include top management support and organizational maturity. Top management support in decision making, monitoring security measures encourages employees to comply with security rules and procedures. Mature organizations are those with formalized business procedures and guidelines, high **use** of performance measurements and availability of decision related data. It is quite logic that mature organizations have proper guidelines and codes of ethics that will stress on the proper and improper usage of Information Systems thus increase the level of security effectiveness.

Doctor 1, 2, IT engineer 1, IT engineer 2, management 1 and Nurse 2 are on the opinion that top management is doing well to protect the Medical Records of Katsina State General Hospitals through the provision of policies, a lot of rules and regulations and laws that upper management authorities. Also many strategies from political authorities for sensitive information is now adopted and implemented to ensure adequate security see also figure 4.

Figure 4, the Organizational actions based on the interviewee's response


Dr. 2 interview GHK
Interview with Doctor 6 on January 24
Interview with IT Staff 1 on February 5
Interview with IT Staff 4 on February 10
Interview with Mgt staff 1 on December 28
Interview with Mgt staff 2 on December 28
Interview with Nurse 2 on December 20
Codes
Organizational maturity
Interview with IT Staff 2 on February 10
Child
Organizational Action
Child
Top management support
Dr. 1 interview GHK
Interview with Doctor 3 on January 19
Interview with Doctor 4 on January 05 GHFuntua
Interview with Doctor 5 on January 5 GHFuntua
Interview with IT Staff 3 on February 5
Interview with Mgt staff 3 on December 28
Interview with Nurse 3 on December 23, 2018 GHFuntua

Base on the interviews conducted with stake holders, it was found that IS security issues are not the main concern because until now there is no serious IS security violation offences committed by the employees. Being a pioneer in the healthcare, Katsina State General Hospitals is a well-known organization for its rules and procedures that are systematically formalized. With an experience for more than 25 years, Katsina State General Hospitals could focus on how to apply, preserve and develop enhanced security measures. Figure 4 indicates the choices of interviewees on organizational actions. Therefore, it is evident that a mature organization like Katsina State General Hospitals plays a part in achieving higher level of security effectiveness. As said by management staff 1. These findings also are in line with "Healthcare organization that aimed to apply KM strategy and integrated with knowledge sharing needs to focus more relationship between managers and employee. These may help to improve the organization's current security knowledge and requirements among healthcare practitioners in cultivating information security culture." [5].

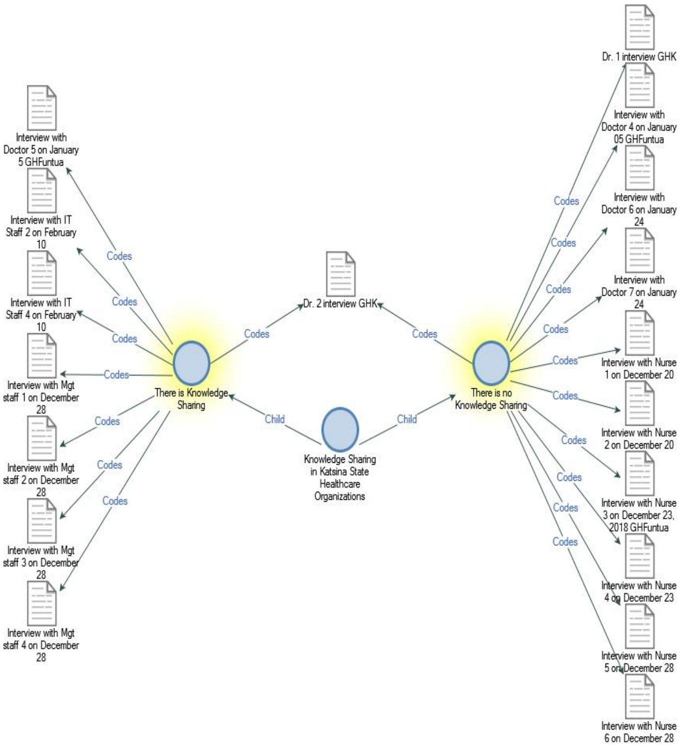
B. Knowledge Sharing Towards Information Security Culture in Katsina State General Hospitals

Knowledge sharing plays a determining role in improving organizational performance. Indeed, generating knowledge, and sharing it, provides information that supports care quality and decision-making. It can also engender new ideas, which create business value. Knowledge sharing (KS) is an act of making knowledge available to others within the organization. Knowledge sharing between individuals is the process by which knowledge held by an individual is converted into a form that can be understood, absorbed, and used by other individuals.

According to interviewees 'answers, every person participates differently on knowledge sharing in Katsina State General Hospitals. It is supported by one interviewee that when an error occurs, the employee responsible is informed orally for the right administration and so this process is done. Some questions were raised to find out the state of knowledge sharing with regards the counter measures taken to prevent electronic medical records in Katsina State General Hospitals as;

The detailed of the interviews' responses were compared from those that viewed that they share knowledge on Medical Record security counter measures and those that said there is no knowledge sharing in Katsina State General Hospitals was explored in figure 5.

Figure 5, Shows the comparison between there is and there is no knowledge sharing


Interview with Doctor 5 on January 5 GHFuntua
Interview with IT Staff 2 on February 10
Interview with IT Staff 4 on February 10
Interview with Mgt staff 1 on December 28
Interview with Mgt staff 2 on December 28
Interview with Mgt staff 3 on December 28
Interview with Mgt staff 4 on December 28
Codes
Codes
Codes
Codes
Codes
Codes
Codes
There is Knowledge Sharing
Codes
Dr. 2 interview GHK
Codes
Child
Knowledge Sharing in Katsina State Healthcare Organizations
Child
There is no Knowledge Sharing
Codes
Codes
Codes
Codes
Codes
Codes
Codes
Codes
Codes
Codes
Dr. 1 interview GHK
Interview with Doctor 4 on January 05 GHFuntua
Interview with Doctor 6 on January 24
Interview with Doctor 7 on January 24
Interview with Nurse 1 on December 20
Interview with Nurse 2 on December 20
Interview with Nurse 3 on December 23, 2018 GHFuntua
Interview with Nurse 4 on December 23
Interview with Nurse 5 on December 28
Interview with Nurse 6 on December 28

This findings is also in line with (M.D. Singh and R. Kant, 2007) "The key resistance factors identified are behavior, lack of top management, lack of communication, low security awareness, personality differences, cultural differences commitment, , lack of trust and openness to experience, and they become the resistance factors for the healthcare practitioners to adopt information security practice."

In general, the findings obtained revealed that respondents are on the same view of code of ethics, System environment security control, DBMS security software, Operating system software, Top management support and Organizational maturity are the counter measures widely used in Katsina State General Hospitals as summarized in Table 5 below, similarly, other counter measures like Disincentive certainty , Fourth generation security software and Specialized security software were neglected in Katsina State General Hospitals.

As for Knowledge Sharing on the Medical Record Security Counter measures, generally, the findings obtained reveled that knowledge sharing is limited to the employees even if there is some, as ten respondents confirmed that there is no any knowledge sharing on Medical Record security countermeasure. It is only the Management and IT staff maintained that there is knowledge sharing. Based on the above evaluation and comparison of the proposed framework and the result found a new framework was analysed.

VI. CONCLUSION

Information is a very vital component of any healthcare system. This is because information is useful for decision making, policy formation, research purposes as well as administrative and clinical purposes. However, most healthcare organizations in Nigeria store information in silos of paper based systems. Consequently, healthcare information is fragmented and broken and thus the flow and exchange of information in Nigeria healthcare becomes a challenge. Consequently, the Nigeria Healthcare System is fraught with medical errors, rising cost, lack of interoperability as well as poor feedback mechanism.

Furthermore, the state of information security in Katsina State General Hospitals is beneath minimum standard required by international information security standards and other dependable information security organizations and authors. In effect, information resources in Katsina State General Hospitals are somewhat vulnerable. The healthcare environment needs to play an important role due to its openness, and diversity of users and their needs. The main challenges to information security have been identified as follows:

- Lack of strong policies/strategies/framework/standards
- Law top management commitment towards effective information security measures
- Law security awareness/knowledge sharing on the existence of information security counter measures among employees
- Inadequate qualified and IT skilled staff
- Ineffective information security counter measures to tackle security threats to Medical Records

VII. RECOMMENDATIONS

The research recommends that:

- The deployment of electronic healthcare system and building human capacity in healthcare,
- Provision of policies that facilitate the implementation of e-health systems,
- The provision of a unified standard for health information exchange as well as;
- The integration of private healthcare organizations with the Government owned healthcare organizations are some of the strategies for managing information flow within the context of Nigeria Healthcare System.

VIII. ACKNOWLEDGEMENTS

This work is sponsored and supported by **Tetfund Nigeria(Tetfund Nigeria IBR Grant 2016)**

IX. REFERENCE

[1] Lippeveld, T, (2016). Routine Health Information Systems: The Glue of a Unified Health System. KeynoteAddress at the Workshop on Issues and Innovation in Routine Health Information in Developing Countries, Potomac

[2] Carayon et al. (2009). "Implementaiontion of an elctronic health rsecords system in a small clinic: the viewpoint of clinic of of staff'. *Behavioural & Information Technology*, 28:1,55-20

[3] Thompson et al. (2004). The Decade of Health Information Technology: Delivering Consumer-centric and information-rich Health care Framework for Strategic Action.

[4] Mount et al. (2000). An integrated electronic health record and informationsystem for Australia. *Medical journal of Autralia*, 172;25-27.

[5] Booth N. (2003). Sharing patient information electronically througjh the NHS. *Britsh Medical jounal*, 327(7407:114-115

[6] Mohan et al. (2994). The Malaysian Telehealth Flagship Application: a national approach to health data protection and utilisation and consumer right. *international jouranal of medical informaticss Volume 73, issue 3*,, 217-227.

[7] Wise, et al. (2012). "Informalion systems failure analysis,". *IEEE journal*, 318-319.www.edu.plymouth.ac.uk/.../qualitative%20methods%202/qualrshm.htm. (n.d.) retrieved on 2nd Febuary, 2019

[8] Al-Salihy et al. (2003). Effective of Information Systems Security in IT Organizations in Malaysia. *9th Asia Pasific Conference on Communications APCC*, 5.

.[9] Kabay, M. E. (2002). *Using social psychology to implement security policies, Computer Security Handbook.* www.mekabay.com/infosecmgmt/Soc Psych INFOSEC pdf

[10] Tipton, H. F. & Krause M. (2006). Cultivating an organizational information security culture. *Computer Fraud & Securiyty*, 7-11.

[11] Hassan N, et al. (2013). A Conceptual Model for Knowledge Sharing Towads Information Security Culture in Healthcare Organization. *IEEE 3rd International conference on research and innovation systems (ICRIIS'13)*, 5.

[12] Lupiana. (2008). *" Development of A Framework To Leverage Knowledge Management Systems to Improve Security Awareness".* Dublin: Dublin Institute of Technology

[13] Eloff et al. (2003). Information security management: a new paradigm. *ACM: Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* .

[14] Emil Walin. (2010). Managing Information Security in Healthcare. In Y. Xu, *Managing Information Security in Healthcare* (p. 73).

.
.