Computer and Information Science; Vol. 16, No. 4; 2023
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Electronic Health System Integration Framework for Secure M-Health Services: A Case of University of Nairobi Hospital

Samuel Nandasaba[1], Gregory Wanyembi[1], & Geoffrey Mariga Wambugu[2]

[1] Mt. Kenya University, Kenya

[2] Murang'a University, Kenya

Correspondence: Samuel Nandasaba, Mt. Kenya University, Kenya.

Received: September 1, 2023 Accepted: October 5, 2023 Online Published: November 20, 2023

doi:10.5539/cis.v16n4p21 URL: https://doi.org/10.5539/cis.v16n4p21

Abstract

The purpose of this article sought to design a secure framework that can be used in M-Health systems development. The researcher used the integrated information theory as a framework for enforcing system security as a holistic approach. To actualize this study, objectives that were meant to guide in carrying out the research were: To evaluate the significance of Confidentiality, Integrity and availability on the security of M-health systems and to develop a framework for secure integration of M-Health systems. The researcher used University of Nairobi Hospital because of ease of accessibility and financial resources available to conduct the research. The study adopted a cross section survey design methodology that included a sample size of 44 ICT personnel and users of University Health System at the University of Nairobi Hospital. Data collection methods were observation, conducting interviews and filling questionnaires that were administered to the target population in the University Hospital. The target population were handed the questionnaires and had them filled. The filled in questionnaires were then picked later from the respondents. SPSS version 23 was used for data analysis, then presented in frequency tables, bar charts, pie charts and standard deviation.

Keywords: availability, confidentiality, integrated information theory, integrity and M-Health

1. Introduction

With the advancement of wireless information technologies and applications, a rapid rise has been recorded in the use of smartphones, tablets, and other electronic gadgets in the health sector. Researchers have developed frameworks such as (Maranda, 2016),

(Gejibo, 2015), (Nkosi, 2014), (Leon et al., 2012), and (Elkhodr, 2012). In addressing the M-health information services, these frameworks are faced with security challenges, the major being confidentiality, availability, and integrity, this is negatively affecting the usage of the frameworks in sorting out the security risks. (Vimalachandran et al., 2018), because of the effects on encouraging good standards of patient care, maintaining CIA data in EHR systems has grown to be a significant issue. This research therefore aims to offer an intervention by proposing an integration framework of EHIS into M-health with much focus on the security aspect to enhance M-health applications security. Iwaya et al (2020), it has become clear that security and privacy are the most difficult parts of healthcare information systems, and it is vital to properly comprehend and handle the security concerns of M-Health.

2. Objectives

Research Objectives

The research was guided by the following objectives:

Main Objective

The main objective of this study was to design a framework for electronic health system Integration for secure M-health services at the university of Nairobi hospital.

Specific Objectives

The following two specific objectives served as the study's guide in order to accomplish the overall goal.

1. To evaluate the significance of a comprehensive information security of M-health systems at the

University of Nairobi Hospital.

2. To develop a framework for secure integration of M-Health systems at the University of Nairobi Hospital.

Research Questions

1. How can comprehensive information security be realized in an M-health system at the University of Nairobi Hospital?
2. How can a secure integration framework of M-Health system at the University of Nairobi Hospital be developed?

2.1 Justification

Cyber security has been a key challenge to computer-based systems in the last few years. It is important to note that systems security should be considered as a part of the system development in any information system and not an implementation requirement. Therefore, the ability to analyze the key security demands of the system and integrate them within the computer-based system as it is being built is critical. Furthermore, for health information systems, preservation of privacy of a patient's health data is one of the key tenets of any health system/facility. Thus, a comprehensive security model must be enforced in any kind of health system for it to be considered effective and beneficial.

The study focuses on the influence of electronic health system integration framework for secure m-health services: a case of university of Nairobi hospital. The study will adopt a cross section survey design.

Mobile Health applications development plays a crucial role in today's lives with the increasing number of tablets and smartphone users. Mobile technology is growing exponentially and therefore organizations and government are making use of their power to collect, collate, transmit and present data in a timely manner hence overcoming limitations that are in manual systems and the University of Nairobi hospital is not an exception.

Fast growth of mobile technology has made it possible for electronic systems to share data more often, therefore providing decision makers with useful information and improving their capacity to have very important decisions about health matters. While mobile phone technology has shown tremendous potential to transform health-care distribution, there is little guidance to keep university of Nairobi hospital developers updated about the development of secure frameworks for M-Health systems.

2.2 Literature Review

2.2.1 Theoretical Framework

This section looked at the various theories that were used to inform the study on security features of an E- health system. The study was founded on one theory, the Integrated Systems Theory. Specifically, literatures pertaining to health system information security in health care systems were reviewed.

2.2.2 The integrated Systems Theory

This theory was proposed by (Hong et al.,2003), as an interdisciplinary theory dealing with any structure of nature, culture, and multiple empirical disciplines, as well as a paradigm with which a phenomenon can be studied from a systematic perspective (Capra,1997). Integrated System Theory entails enforcement of information security policies, management and assessment of risks, information Auditing and internal controls. Consequently, information security is covered comprehensively in terms of many aspects by integrated system theory. It describes organizational actions in terms of information security management and techniques, as well as including alternatives.

In order to fully comprehend information security management, explain information security management techniques, and anticipate management outcomes, integrated systems theory is crucial for the study. Consequently, the theory offers a solid foundation for evaluating the level of information security controls implemented at the University of Nairobi hospital. Internal control is the prevention, detection, and correlation of system-related activities in order to prevent unauthorized and illegal access.

Controls can also be referred to as administrative, operational, and technical measures that safeguard the system's availability, integrity, and confidentiality.

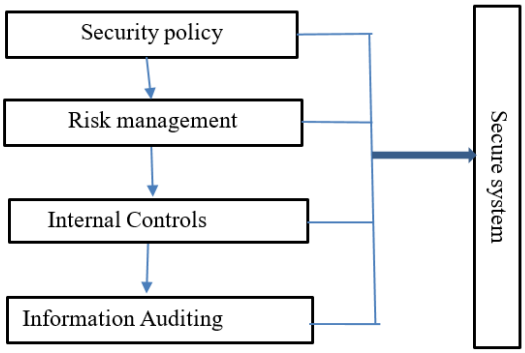


Figure 2. Integrated system Theory (Adapted from Hong et al., 2003)

The nature of this theory makes it difficult to adapt to highly dynamic surroundings, and it also takes a top-down approach that may not be consistent with reality.

We need to consider M-health as a service delivery system; as argued above in Chapter 2, Integrated System Theory entails enforcement of information security policies, management and assessment of risks, information Auditing and internal controls. Consequently, information security is covered comprehensively in terms of many aspects by integrated system theory. It describes organizational actions in terms of information security management and techniques, as well as including alternatives. The relevance of the theory in the management of M-health services is deficient in the fact that the theory fails to holistically look at the overall IT infrastructure holistically but instead lays its overall emphasis on information security management.

The big question that this research needs to ask is therefore, how would a holistic integrated information security delivery system look like? What are the optimal IT infrastructure and what security principles would govern the measures that would be put in place to guarantee the security of services for which the system is built?

According to IBM, IT infrastructure configurations vary based on organizational requirements and objectives, however some objectives apply to all businesses. Business high-performance storage, a low-latency network, security, an efficient wide area network (WAN), virtualization, and zero downtime are all features of the ideal infrastructure. This means that to guarantee the security of services supported by these systems, vulnerabilities to each of the components of these systems must be adequately analyzed and addressed.

In our case, M-health systems are critical not only for provision of accurate medical information on patients, but the preservation of this data and a guarantee that only those with the authority to access it can access it whenever they need it. It therefore implies that the collection, storage and processing functions must be secure.

High-performance storage systems include a data recovery system and data archiving and backup capabilities.

Low-latency networks use enterprise-level infrastructure elements to minimize data flow delays.

Secure infrastructures systems that regulate data availability and information access. Regardless of where the data is kept, it may protect a company from hacks and breaches while maintaining customer trust.

WANs prioritize traffic on the network and adjust the bandwidth allocation for certain applications as necessary.

Virtualization increases uptime, enhances disaster recovery, and saves energy while providing quicker server provisioning.

Zero downtime to keep costs low and earnings high, this strategy tries to minimize system outages and business operations disruptions.

There is therefore need to divide the security of M-health services into two

Information security: (principles include confidentiality, availability, integrity)

MHI security (M-health infrastructure security): mhealth infrastructure includes enterprise servers, data storage servers, Mainframes, mobile devices and software and operating systems

Further, in having a holistic view of secure M-health services, we need to consider that any effective Service Delivery system strategy is comprised of five key components (IBM,2016):

- Service level management
- Financial management for IT services

- Capacity management
- Availability management
- IT service continuity management

Therefore, any effective M-heath system must be able to integrate all these functionalities and requirements into the system and its operations.

3. ICT and Healthcare Systems

Patient Care Information Systems (PCIS) deployment in healthcare organizations has not been successful. This has been so because of a number of challenges that may be faced when the systems are being implemented or thereafter (Berg, 2001). Healthcare Information and Communication Technologies (ICT) are complex operational technologies whose applications, purposes, disadvantages, and ramifications are not well defined, nor are the advantages of usage guaranteed. However, there are some compelling theories about how IT can be used in healthcare to increase efficiency, consistency, and connectivity in order to promote acceptance and guide effective deployment of e-healthcare systems. ICT use ideas are discussed among a group of partners that include medical practitioners, representatives of healthcare organisations, legislative and regulatory authorities, as well as ICT suppliers and consultants. This interactions between a group and systems form and decide the consequences of healthcare ICT technologies. As a result, understanding the social development and interpretive mechanisms by which healthcare ICT technologies are created and shared is important for forecasting consequences of ICT implementation and informing policymakers of the threats presented to patient information contained within these digital networks.

Information security.

Information systems (IS) are highly depended on by organizations. Consequently, these firms employ technical controls to lessen information security risks (Gundu & Flowerday, 2013). Risk identification.

This refers to the process where potential risks of a project and their characteristics are listed. The results are usually recorded in a risk register.

3.1 Risk Management.

Risk refers to the possibility of something adverse happening. Risk management is therefore about transforming organizational culture to accept risk and facilitate risk discussion when doing business activities or making any strategic investment on various projects.

3.2 Risk Mitigation

It is a strategy in preparation for and lessen the effects of threats faced by a system.

3.3 Existing Frameworks for M-Health Systems.

There are researches that have been done on the frameworks for M-health and have been published in various referred journals as discussed below.

3.3.1 A Framework for Assessing M-Health Challenges in South Africa.

A qualitative study conducted in South Africa to review the benefits and challenges of M-health in community-based health services. There were four key system dimensions that were identified and assessed. These were;

- Government stewardship
- Organisational
- Technological
- Financial

According to the report, prospects for effective M-health adoption in South Africa include a high prevalence of cell phones, a positive policy framework for M-health, successful use of M-health for community-based health programs in a variety of initiatives, and a well-developed ICT industry. However, there were some shortcomings in other main aspects of the health system, such as corporate culture and potential for using health knowledge for management, as well as a lack of access and usage of ICT in primary health care. The complexities of ensuring interoperability and convergence of information systems, as well as ensuring information safety, is among the technical challenges. There was also the issue of sufficient financing for large-scale M-Health usage in a resource-constrained world. The limitations of this study was that it never dealt on technological Security of

M-health systems.

The framework that was developed is as shown in the figure 3;

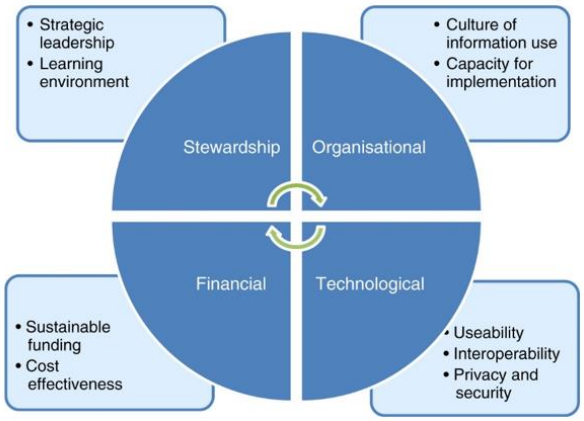


Figure 3. A framework for assessing M-Health challenges in South Africa (Leon et al., 2012)

The figure shows four health systems dimensions that should be addressed when assessing the complexities of scaling up M-Health from a health systems perspective.

3.3.2 M-Health Decision Making Framework for Community Based Services

(Maranda ,2016), the researcher encompassed additional security procedures using encryption, integrity of the data and the security keys. In the encryption perspective, encrypted data was sent to the server .The researcher used built-in libraries for encryption of string data. The messages were transferred in XML format to the server

(Maranda,2016) implemented integrity of the data using Digital signatures. The Digital signature ensured that the message that was sent was exactly what was received. The signature depended on the encryption which assured authentication.

The Digital signature solely relied on a private key algorithm. This meant that the message owner was the only one who knew it but the public key was known. The researcher used checksum algorithms and a checksum function to transform the input and produced a numerical output of smaller size.

He suggested the use of security keys. In this case he used 128bit strings which were delivered to the server before requesting sensitive data. The security keys were encoded with chosen cryptographic algorithm and was unified with entire application but quite independent from the device.

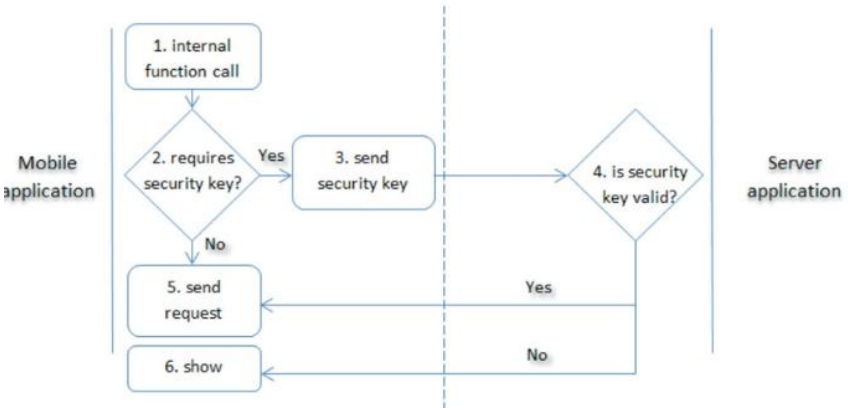


Figure 4. Data transfer using encryption and digital signatures. (Maranda, 2016)

In this study, the researcher introduced three core components that must be taken into account while developing and deploying mobile applications. These components were: data transfer, storage, and access. All these components must be viewed as equally important all through all phases of development. The Secure Development Strategy detailed the assumptions and frameworks that ought to be enforced within the application context to provide mobile protection. The most important feature of Secure Development Strategy is that it embraced all crucial aspects by describing the concepts and grouping them. The geo-location and ADID

(Application Device Identifier) for data access, the encryption of sensitive data in database files, and the encryption of requests transmitted over the internet with digital signatures and security keys were not addressed by the researcher in this study. The Secure Development Strategy's objectives were to limit the number of potential risk points in the program rather than to completely protect it from assault by preventing potential attackers from encrypting important data. With the use of a developed security architecture called iSec, the Secure Development Strategy's pillars were really put into practice.

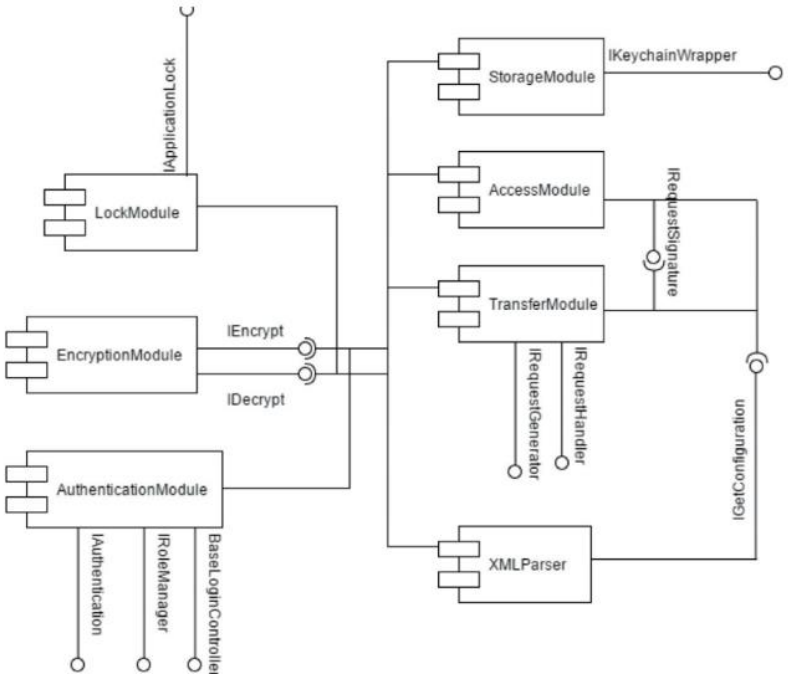


Figure 5. Components of the iSec framework. (Maranda, 2016).

3.3.3 Mobile Application Security System Framework

For mobile application networks, Floyd (2006) developed creative layering of security mechanisms that offered a dispersed security solution. Code signature variation, remote hashing, a mobile application generator, application time to live, resident monitor applications, distributed application monitoring, code obfuscation, and hashing algorithms were all provided by the researcher in a way that maximizes benefits while minimizing overhead. The researcher offered a distributed method that could keep safeguarding even if hosts and programs were deleted, corrupted, or destroyed. The integrity and security of the application system were strengthened by the security measures described in this study.

The limitations of these research is that the researcher didn't address methods for detecting and preventing denial of service (DoS) attacks and a secured interprogram communications. Diverse application kinds must collaborate through interprogram communications in order to carry out an essential task.

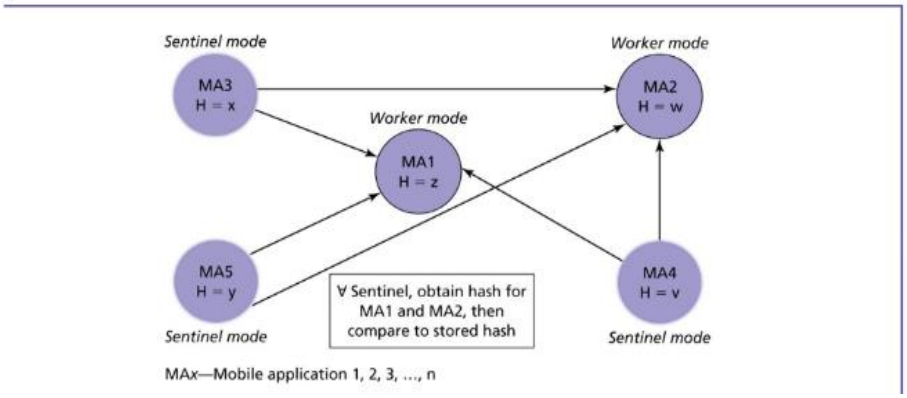


Figure 6. Analyzed hashes obtained for the conflicting parties. (Floyd, 2006)

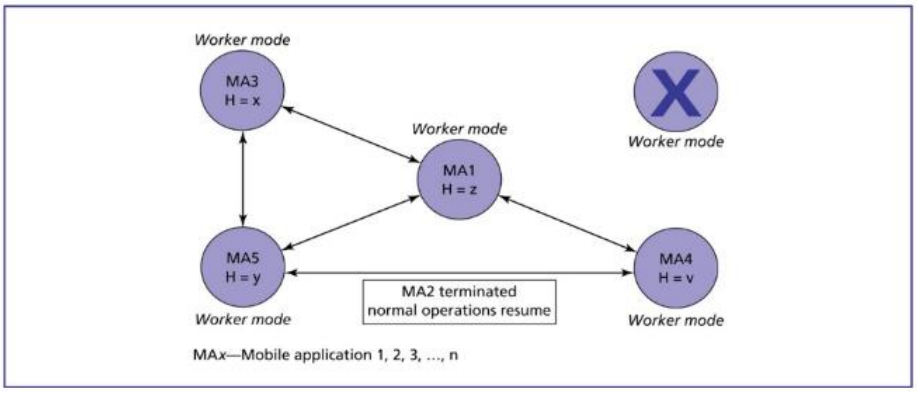


Figure 7. Corrupt application identified by consensus vote (Floyd, 2006)

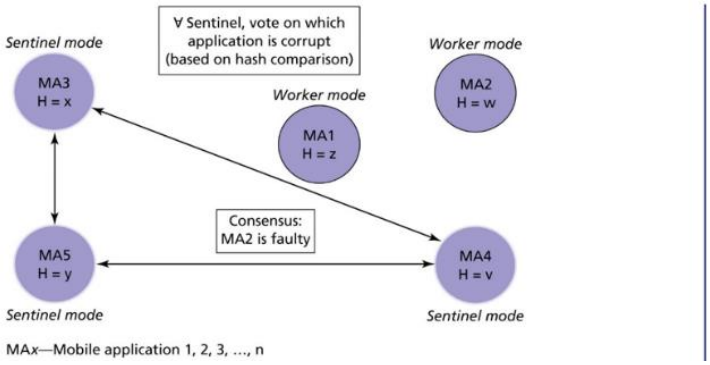


Figure 8. Termination of corrupt application from the network. (Floyd, 2006)

3.3.4 A Framework to Improve Mobile Banking Security

In this case, the researcher recommended providing banking customers with a smartphone device so they could safely access their business or personal accounts from any location at any time.

To resolve these security issues, a confidence negotiation approach was suggested in this report. As the underlying protocol, trust negotiation was paired with Transport Layer Security (TLS). This technological mix aimed to improve the current security of M-banking applications.

The proposed framework verified the requesters and their devices. These gave users the chance to register their mobile devices and provided a mechanism for financial organizations to confirm that the device was being used. By automating the authentication process, this strategy improved two factor authentication.

The limitation of this study is that it did not factor in the location verification method to the m-banking system.

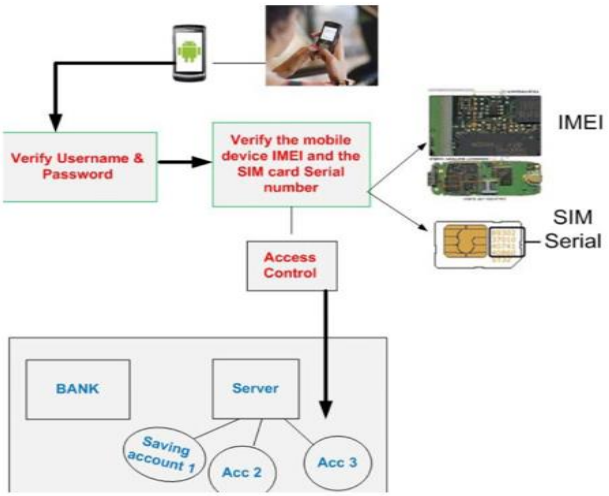


Figure 9. Sec ure M-banking model ((Source, Elkhodr (2012))

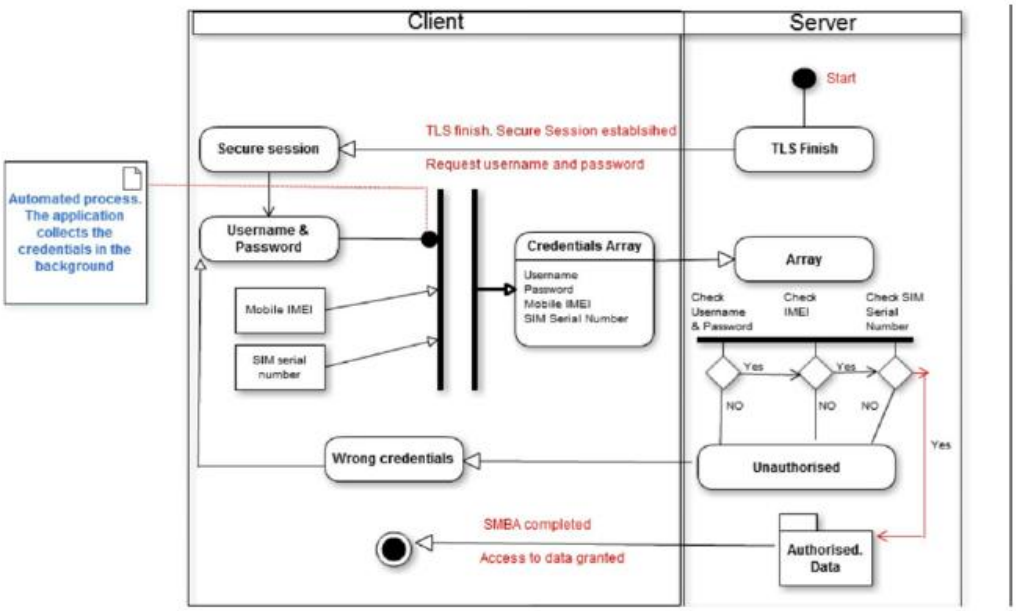


Figure 10. Secure mobile banking approach framework activity diagram. (Elkhodr, 2012)

3.3.5 An Enhanced Mobile Health Applications Cloud Computing Framework

The researcher described the difficulties that mobiles encounter when providing Secure Multimedia-based Health Services due to computation and power supply constraints in this report.

In this case, the researcher postulates that mobile devices are not able to perform complex multimedia and security Algorithms due to the fact that they run on small batteries and also have inadequate computational capacity, as a result, researcher devised a cloud computing platform to support mobile devices while running heavier multimedia and encryption algorithms in the distribution of mobile health services. In this study, the suggested framework makes use of a cloud computing protocol management approach to offer mobile devices security as a service (SaaS) and multimedia sensor data processing. The researcher in this study hypothesized that security and multimedia operations may be carried out in the cloud, enabling mobile health service providers to subscribe and expand the features of their mobile health applications beyond the limitations of currently accessible mobile devices.

In this research, the security of mobile health systems data was not addressed by the researcher hence the need to carry out more research on this topic.

The initials of the diagram

NI- is a non-intrusive sensor that is used to gather the required sensor signals, which are then fed to an embedded digital signal processor (DSP) in a mobile device.

SIPS-is the session initiation protocol signaling

SIP-EP-is the session initiation protocol event packet, this connect the IMS client to the call session control functions (CSFC).

The CSFCs are SIP proxy servers, supporting IMS signaling and session control functions. XDMS- is the database management system which controls and organizes data created by the health monitoring services.

The Application server hosts the ongoing mobile service and sends and receives data from the IMS client. The application server also functions as a branch of the Home Subscriber Server (HSS), which is the primary repository of mobile-related user data. The IMS system monitor acts as the recipient and interpreter of the sensed physiological information and therefore relays back the necessary decision and action to be taken.

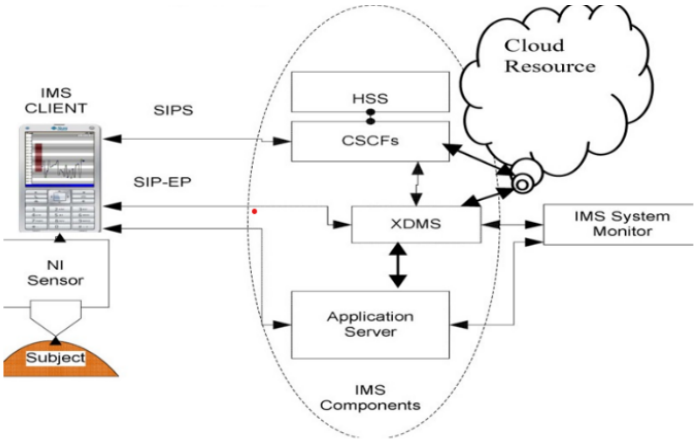


Figure 11. A framework of IP multimedia subsystem standard –based mobile health monitoring with cloud support. (Nkosi&Mekuria, 2010)

3.3.6 Secure Mobile Data Collection System Framework

Gejibo (2015) developed a secure mobile data collection system framework with a set of modular security features that were built to meet MDCS standards and design criteria. The framework included simple interaction interfaces. The framework was created to be flexible, scalable, and adaptable to various MDCS security settings while simultaneously being secure by default. The framework's primary goal was to offer an all-encompassing safe solution for user identification, secure mobile and cloud storage, and secure communication.

Authenticator: a security module that dealt with account recovery, remote server authentication, and user authentication on mobile devices. With a default concrete implementation, it offered the authentication services through straightforward interfaces.

This particular module received the user authentication delegation from the MDCS client. As a result, whenever an attempt was made to access the MDCS (mobile data collection systems) client, the Authenticator module was invoked. The Authenticator is adaptable and may be set up to offer further capabilities like single sign-on and device authentication. The requirement that a phone may be shared by several collectors who should not have access to each other's acquired data was the major justification for the module's existence.

2. Secure Storage: Security module in charge of managing and protecting the mobile device's MDCS application resources. With a default concrete implementation that handles encryption, decryption, cleaning up leftover data once the user logs out, and a recovery strategy in case the application crashes or the battery runs out, the secure storage is available via straightforward APIs.

3. Secure Communication: is a security component in charge of creating a secure tunnel between the client and the server. A popular protocol for protecting HTTP messages is Hypertext Transfer Protocol Secure (HTTPS).

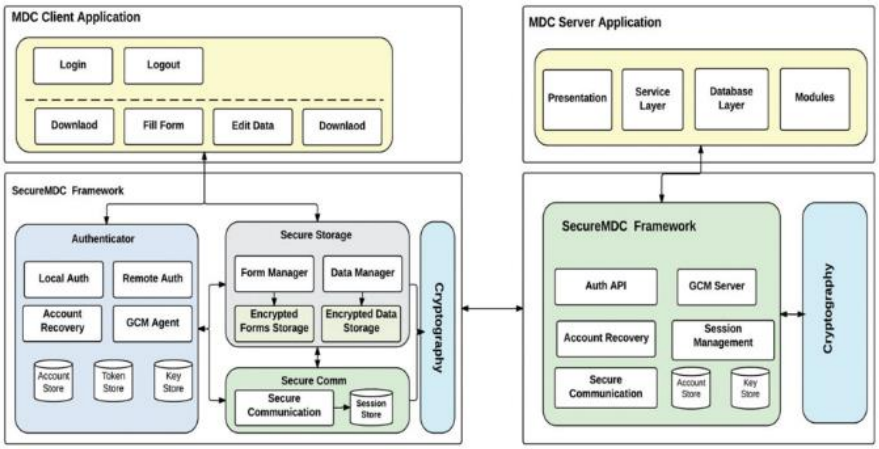


Figure 12. showing the modules and the explanation(Gejibo,2015)

3.3.7 SecourHealth Framework

Simplicio etal (2015) in his SecourHealth, developed a minimal security framework with a focus on very sensitive data collection systems. In this he identified various pillars which included:

I. Lack of connectivity and tolerance delays- Users were able to function offline when necessary and authenticate themselves on any device they had previously registered.

II. Loss or theft device protection- When a device is stolen while a legitimate user's session is still active, this module has a method that restricts the attacker's ability to receive information from the server.

III. Data transfer between a mobile device and sever in secure manner- In this module, even in the absence of an underlying secure connection, all data sent between a server and a mobile device was encrypted and authorized.

IV. By incorporating this security framework into the GeoHealth system and the Android-based "Family Health Program" application, which were both used by the government to collect health data in Sao Paulo city, Marcos (2015) put this security architecture into action.

3.4 Conceptual Framework

Figure 12 shows the conceptual framework for this research. In order to assess your electronic health record security, credibility, and availability requirements, you must first thoroughly consider your practice's health IT climate. This could include the technology your profession uses for both therapeutic and institutional purposes, as well as when and how those technologies are physically used and located within your practice. Consider the circumstances that could result in unwanted entry, use, leak, interruption, alteration, or loss of electronic health records as you assess the health IT climate. These circumstances are likely to be specific to the practice and can take the form of technology problems (e.g., a lack of securely installed computing equipment), procedural issues (e.g., a lack of a security incident management plan), or staff issues (e.g., lack of comprehensive information security training).

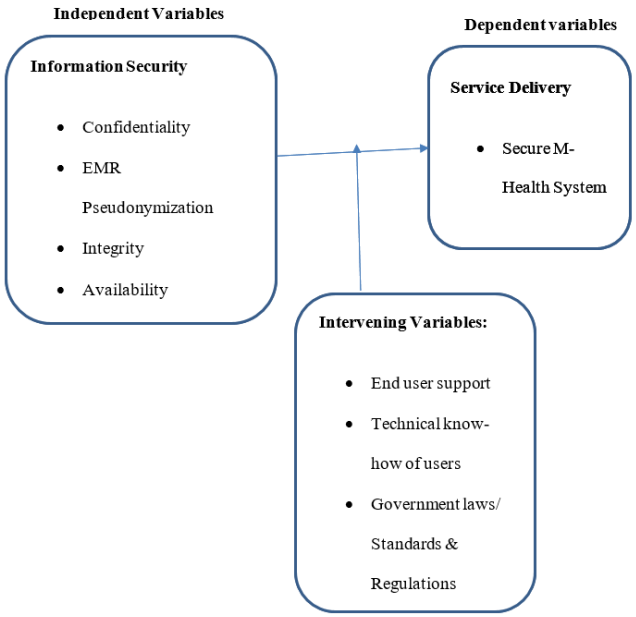


Figure 13. Conceptual framework, (Researcher, 2023)

3.4.1 Confidentiality

The security of information contained inside networks from unwanted or unintended access is referred to as confidentiality.

“Privacy is an individual's right to choose when, how, and to what degree knowledge about them is transmitted to others” (Brands, 2003, pp2). Privacy involves the right of the individual to be left alone, to withdraw from the influence of his environment (Innab, 2018). Additionally confidentiality relates to disclosure or nondisclosure of information.

Patients agree that with their permission their medical data can be shared with other institutions such as insurance companies to facilitate the payment of their dues. Therefore, the patients only understand that the shared individual medical data can only be used for the intended purpose.

Furthermore, outside the hospital, patients have expectations that individuals will not be given access to confidential information or institutions not permitted to keep such content. The content's genuine users won't abuse this access for uses other than those for which it was intended in the first place.

3.4.2 Integrity

The property whose electronic health records has not been tampered with or lost in an improper way is referred to as integrity. It refers to the accuracy and continuity of data stored about a person, entity, or event, in this case, the patient (Charitoudi & Blyth, 2013). Integrity of data encompasses documentation accuracy throughout the entire health record. It entails patient identification, information governance, record correction and validation of authorship. Additionally, the accuracy of the data provided at the time of capture has a significant impact on the quality of the data in the EHR.

The quality of a patient's healthcare may be significantly impacted by inaccurate health information. As health information becomes more computerized and the extent of organizational interchange of health information expands into Health Information Exchanges, maintaining the accuracy and completeness of health data is essential (HIEs) (Kellerman & Spencer, 2013).

(Lucas, 2013) postulates that the accuracy, reliability, and completeness of the demographic information related to or associated with a specific patient is known as patient identity integrity.

Availability

Availability refers to the property where electronic health information can be accessed and used when demanded by an authorized person. System availability looks at the period of up-time for operations and is a measure of how often the system is alive and well. It is always denoted as (up-time)/(up-time + downtime) with numerous variants (Ahmed & Mousa, 2016). Up-time and downtime refer to dichotomized conditions. (Charitoudi & Blyth, 2013) states that Up-time is the ability to perform assigned duty as downtime denotes not being able to perform the given task.

When a system is up and running and ready for use, it is said to be available. A system may go offline for a variety of reasons, ranging from scheduled maintenance downtime to catastrophic failure (Innab, 2018). The goal of high availability solutions is to reduce this downtime and/or the amount of time it takes to recover from an outage (Zdravkova, 2015). How much downtime may be permitted will influence the solution's comprehensiveness, complexity, and cost.

On the extreme end of the scale, high availability can literally refer to a disaster response plan that can get an organization back up and running as soon as possible. For small systems, this may be as straightforward as an uninterruptible power source and a strict backup strategy. The peak of consistent availability, exemplified by comprehensive workload-sharing solutions distributed across several sites, is at the other end of the spectrum. There are differing degrees of availability between these two extremes (Nganji & Nggada, 2011). Computing systems availability has been described using various concepts: high availability computing; fault tolerant systems; system redundancy (Lizasoain et al., 2015). The idea behind all this is to ensure that no matter what happens,

users must be able to access the systems for the data and information that they require. In the case of e-health, system failure can be initiated at five levels.

Mobile device failure (hardware/software)

Network outrages Or server failure (hardware or software)

Wherever any of this happens, it leads to delays in access of the systems or failure by the users to perform the functions for which they are supposed to. Thus, system designers must do their best to develop contingency plans that will ensure continued access of these vital systems.

3.4.3 Pseudonymization

A pseudonym can help protect privacy. By using a method known as pseudonymization, sensitive data can be secured while still providing people access to less important components. To handle sensitive data, this method replaces crucial data elements with pseudonyms. This method prevents immediate access to the information.

3.4.4 Standards and Regulations

Any electronic health records system that ensures the privacy and security of patient data must adhere to standards. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the regulation that is most frequently used in the US. Health information is protected by federal law known as HIPAA, which also guarantees that patients can access their own medical records. The people in charge of safeguarding this information now have additional obligations. HIPAA sets security standards that are comprised of four areas as stated by Maiwald (2005). These four sections include technical security services, physical safeguards, technical security mechanisms and finally administrative procedures. The main objective of HIPAA is to keep customers' and employees' personal health information private, secure and confidential. The personal Health information must also be maintained in a manner that ensures high integrity and high availability in the event of an emergency. Another standard in use is the CEN/ISOEN3606-PartIV in Europe, which includes privacy and security directive. The CEN created this standard in 2008, which was then modified in 2010 with ISO approval. This standard's primary goal was to offer universal guidelines for creating interoperable electronic health systems. Efficiency, cost savings, and risk avoidance are the practical justifications for implementing standards.

3.4.5 Common Data Security Architecture

This is an open and extensible software framework and API specification that usually addresses communication and data security requirements. It was originally developed by Intel Architecture Lab (IAL).The main objectives of Common Data Security Architecture were:

Encourage interoperable ,horizontal standards

Offer essential components of security capability to the industry.

The Common Data security Architecture has three layers which include

System security services-this offers language interface adapter

Common security services manager-this is a cryptographic service provider, which performs bulk encrypting, digesting and digital signature in addition there is trust policy modules which implement policies defined by authorities and level of trust required to perform certain actions.

Security add-in modules- this layer provides modules that offer basic components in cryptographic algorithms and storage.

4. Methodology

4.1 Introduction

The section outlined the method to use in the study focusing on the significance of electronic health system integration framework for secure m-health services: a case of university of Nairobi hospital. The study adopted a cross section survey design. It outlined research design, the population of study, sample size, and data collection methods from the study participants and the tools that will be used for data analysis.

4.2 Study Design

According to (Wausi, etal, 2009), a research design is an account of the logical steps used to connect the research questions and procedure to data collection, analysis, and interpretation in a coherent manner. According to (Tarus, et al., 2015), the researcher points out that in a descriptive study, the researcher can use results obtained from the sample to make a generalization about the entire population. This study adopted a cross section survey design, the study collected both qualitative and quantitative data from various respondents by conducting interviews with participants or giving a questionnaire to the intended audience.

Study Population and sample size determination

A systematic random sampling technique was applied in this study. Equal opportunity was given to each person to participate in the study. The population for this study was staff using the University Health systems and the system developers at the University of Nairobi Hospital. The study's sample size was 44 system users and ICT personnel. The researcher was convinced that because they are more familiar with how the system works, the ICT staff members had the necessary knowledge of University Health systems. The two objectives of the study was used to come up with research questions. The study site for this research was chosen because they have had an E-Health system for the last five years which enabled collection of the required data successful.

Less than 100 of the employees listed on the University of Nairobi Health Services website meet the criteria for inclusion. The sample size of the staff who were willing to participate were determined by using Yamane Taro's

sample size calculation formula (Yamane, 1967).

n=N/(1+N(e)2)

Where:

n is the sample size of target population required for the study

N is the total population size of target population

e is the level of precision (error estimate) which is 0.05

n=N/(1+N(e)2)= n=100/(1+100(0.05)2)= 44 participants

44 people were therefore be contacted to participate in this study.

4.2.1 Pre-test

To guarantee that all study parameters are tested from the target group, the researcher did pre-test for the created questionnaire. Pre-testing was done by the researcher distributing questionnaires to a few random participants at the UoN Hospital. If queries arose, then the researcher was able to make necessary changes to the tool to ensure that the required information was captured during the study.

4.2.2 Data Collection

The primary method of data collection for this project was through questionnaires. The questionnaires were left and picked later at an arranged time by the respondents. To ensure a high response rate and to help when respondents sought clarifications, there was follow-ups via email, phone calls, and visits as needed. The questionnaire was administered to ICT staff and users who have roles in the University Health System (UHS). In addition to questionnaires the researcher used observation and structured interviews in order to gain more information on the Security of University Health System.

4.2.3 Data Management

Once data was collected, the questionnaires were checked by researcher to ensure that none was incomplete. Once this was done, the researcher stored these questionnaires in a lockable cabinet where they were safe. Data entry was then done followed by data analysis and finally the researcher once again stored the questionnaires in a lockable cabinet.

4.2.3.1 Data Analysis and Presentation

The information from the respondents' completed questionnaires was coded and entered into a computer statistics tool. Data analysis and the presentation of the findings were done using SPSS version 23.0, a statistical package for the social sciences. Correlation and Regression data analysis techniques were used.

4.2.3.2 Correlation Analysis Technique

In statistics, correlation means that there is a relationship between various events. In statistics, the term "correlation" refers to the relationship between various occurrences.

For the purpose of conducting a reliable correlation study, detailed observations of two variables are required, which gives us a benefit in terms of acquiring results. 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 was 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.

Simple metrics: Findings from research can be categorized easily. The results can be between -1.00 and 1.00. There can only be three possible overall conclusions from the analysis.

4.2.3.3 Regression Analysis technique

A multiple regression analysis was undertaken to further gauge the association among the independent variables on secure service delivery at the University of Nairobi Hospital. To aid this SPSS V 21.0 was used to facilitate the outcomes of the multiple regressions for the study. Predict a research in the near and long term, Understand service security levels. Review and comprehend how various factors affect each of these things. The extent to which changes in the dependent variable (secure service) was influenced by all the four independent variables (Information integrity, Pseudonymization, information confidentiality and information availability) was explained by the coefficient of determination.

Yi=f(xi,β)+ei

Where Y is the dependent variable which was secure M-health system

Xi was the independent variable of Confidentiality.

Xii was the independent variable of pseudonymization.

Xiii independent variable integrity

Xiv independent variable availability

Thus

Y=(Xi+Xii+Xiii+Xiv,β)+ei

In both techniques, results were presented using tables, frequency charts and graphs, and the findings will be presented using tables, graphs, bar charts , pie charts, mean and also standard deviation.

4.2.4 Ethical Considerations

Approval to conduct research was sought from the Mount Kenya University ethical review committee as well as National Commission for Science, Technology and Innovation (NACOSTI) clearance certificate before the commencement of the study.

5. Research Analysis, Findings

5.1 Results

The main objective of this study sought to design a model for electronic health system Integration framework for secure M-Health information systems.

This objective was achieved and managed to evaluate and investigate the existing frameworks for electronic health Integration. The review of the current form of framework revealed that mobile based Health Information systems are unreliable and do not enable professional health workers access to patients' data at any given time.

The results from this project revealed that over 70% believed introduction of Confidentiality, Integrity and availability on the security of M-health systems would make University Health systems processes convenient.

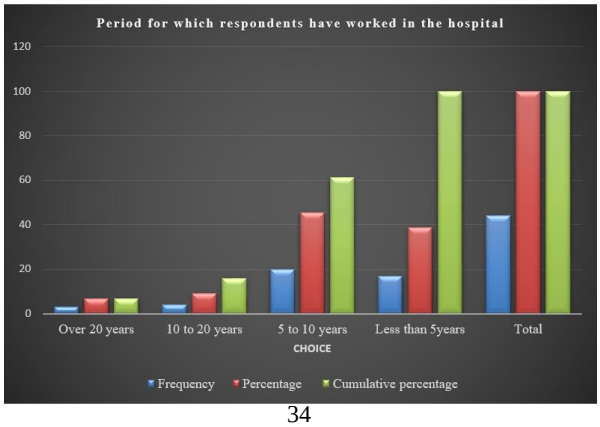
The second objective was to develop a framework for secure integration of M-health systems.

The framework was developed, built and tested. University Health System framework was found to be working well, consisting of entities for security measures. The developed framework was validated. Evaluation of its applicability and usability revealed that it can reduce the vulnerability and improve security level of university health Systems, thus making seamless intervention where M-Health security concern is raised.

The first question is to find out period for which the respondents have worked in the hospital.

Table 1. Period which respondents have worked in the Hospital

Choice	Frequency	Percentage	Cumulative percentage
Over 20 years	3	6.82	6.82
10 to 20 years	4	9.10	15.92
5 to 10 years	20	45.46	61.38
Less than 5years	17	38.62	100.00
Total	44	100.00	



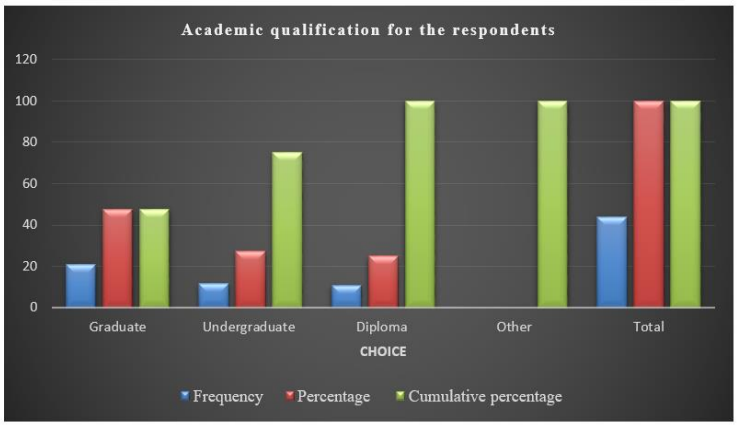
Based on 44 respondents, 6.82% of them indicated to have worked in hospital for over 20years. 9.10 % had worked for between 10 to 20 years. Another 45.45% had worked in hospital between 5 to 10 years and the last 38.62% had worked in hospital a period less than 5 years.

From the study the researcher noted a good number of staff had relative experience at the hospital over 5years.

The second question was to find out the academic qualification for the respondents.

Table 2. Academic qualification for the respondents

Choice	Frequency	Percentage	Cumulative percentage
Graduate	21	47.73	47.73
Undergraduate	12	27.27	75.00
Diploma	11	25.00	100.00
Other			
Total	**44**	**100**	



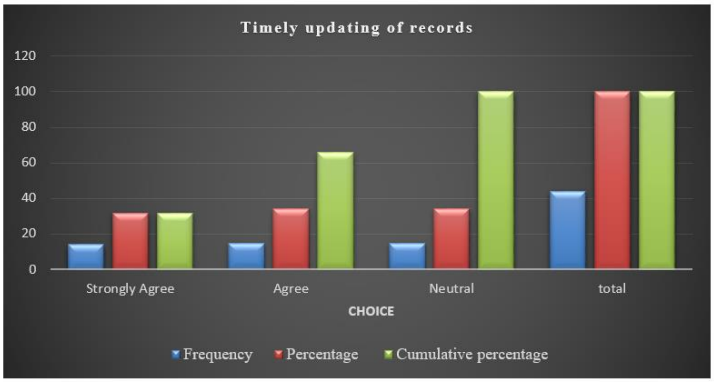
Out of 44 respondents, 47.73% of respondents hold Graduate. 27.27% holds Undergraduate and lastly 25.00% diploma holders.

From the table above, evidently, the vast majority of respondents' i.e., 75.00%, have undertaken education with research component in it and understand the research activities well.

The questions intend was to know the level of Hospital ensuring that all actors add the medical records as soon they are through with the patient to ensure completeness and reliability.

Table 3. Timely addition of medical records in ensuring completeness

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	14	31.80	31.80
Agree	15	34.10	65.90
Neutral	15	34.10	100.00
total	**44**	**100.00**	**100.00**



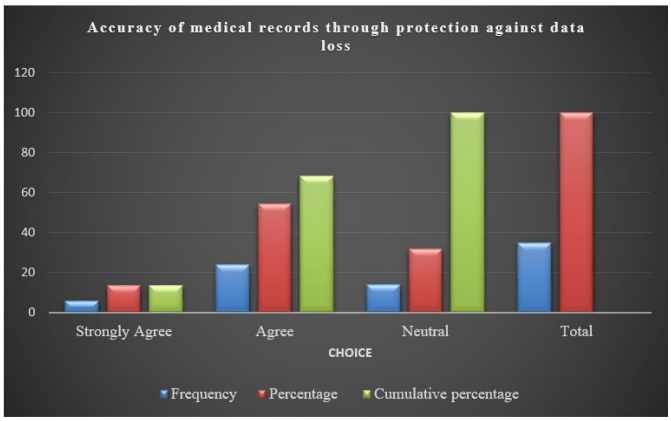
From a total of 44 responses, 31.80% of the respondents strongly agreed that timely addition of medical records in ensuring completeness is observed, 34.10% agreed. A similar 34.10% were neutral.

This indicates that if Electronic Health System Integration Framework for Secure M-Health Service, 65.90% of staff would find it helpful.

Researcher asked respondents if the hospital has ensured accuracy of medical records though protection of information against loss.

Table 4. Response on accuracy of medical records through protection of information against loss

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	6	13.64	13.64
Agree	24	54.54	68.18
Neutral	14	31.82	100.00
Total	35	100.00	

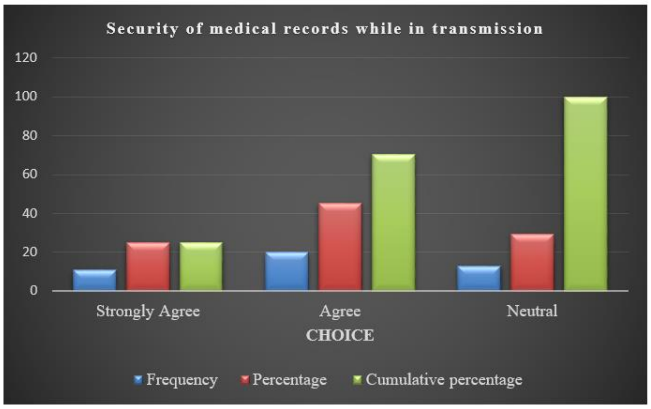


Out of 44 responses, 13.64% of the respondents strongly agreed on accuracy of medical records through protection of information against loss. Another 54.54% agreed on the same. 31.82% of the respondents were not sure. So, we can conclude that protection of information against loss of medical records was key.

The researcher asked the respondents whether the hospital ensured that medical records were protected against distortion while in transmission through electronic media.

Table 5: Security on medical records while in transmission

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	11	25.00	25.00
Agree	20	45.45	70.45
Not Sure	13	29.55	100.00

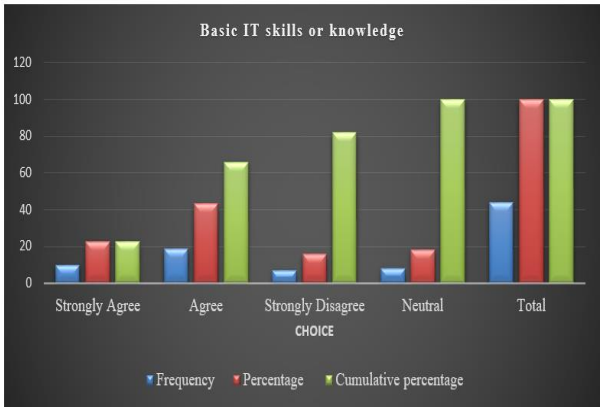


From the above question, 44 responded. Out of which 25.00% strongly agreed presence of security on medical records while on transmission. 45.45% agreed too. 25.81%, while 29.55% are not sure. This means that 70.45% respondents believed in the availability of secure environment in medical records transmission.

The researcher asked respondents for thought about the Hospital in ensuring that employees have basic IT knowledge to key in accurate data.

Table 6. Responses on whether the Hospital ensured its employees have basic IT knowledge to key in accurate data

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	10	22.72	22.72
Agree	19	43.20	65.92
Strongly Disagree	7	15.90	81.82
Not Sure	8	18.18	100.00
Total	44	100.00	

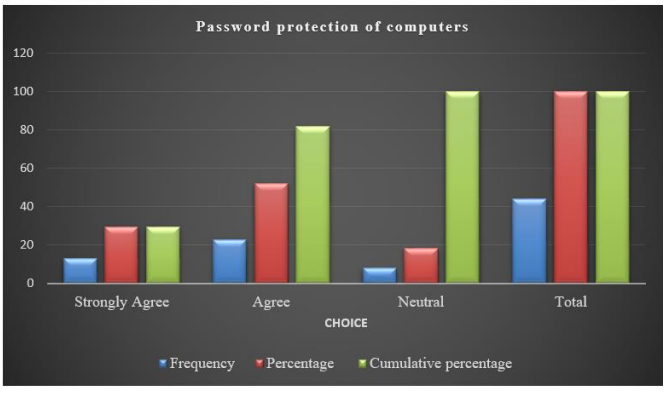


There were 44 responses, 22.372 strongly agreed. 43.20% Agreed, 15.90% Strongly Disagreed, while 18.18% were not sure. Guided by the responses, the researcher came to the conclusion that most of respondents were satisfied that the hospital ensured employees have basic IT knowledge thus using the proposed system was viable.

The researcher asked respondents whether Passwords have been put in computers for protection of data.

Table 7. Protection of data through computer passwords

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	13	29.55	29.55
Agree	23	52.27	81.82
Not sure	8	18.18	100.00
Total	44	100.00	

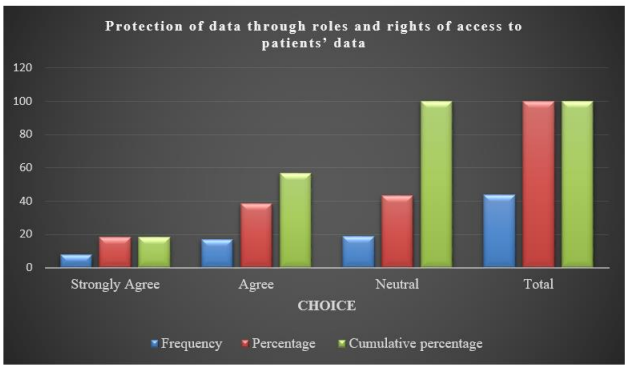


Most respondents agreed with the computer protection that has been put in place.

The researcher asked respondents whether The Hospital has ensured that the system has various users with different roles to avoid unauthorized access of patients' data.

Table 8. Protection of data through roles and rights of access to patients' data

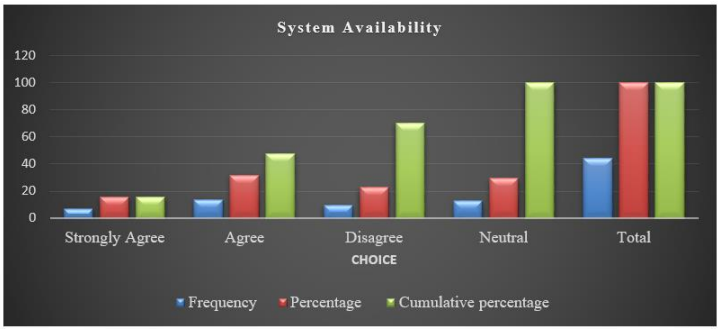
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	8	18.18	18.18
Agree	17	38.64	56.82
Not sure	19	43.18	100.00
Total	44	100.00	



The researcher asked respondents if The University Health system is always up and running

Table 9. Availability of system

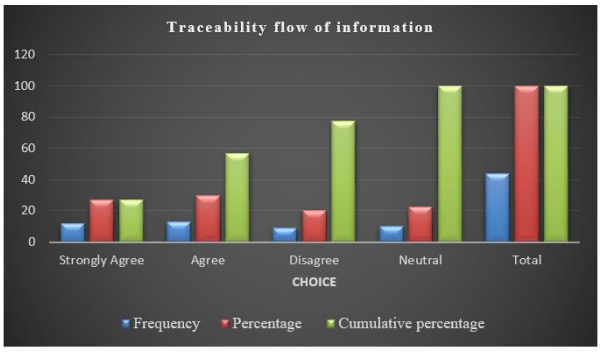
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	7	15.91	15.91
Agree	14	31.82	47.73
Disagree	10	22.72	70.45
Not sure	13	29.55	100.00
Total	44	100.00	



The researcher asked respondents whether the flow of information in the University Health system is traceable through logging and documentation

Table 10. Traceability flow of information

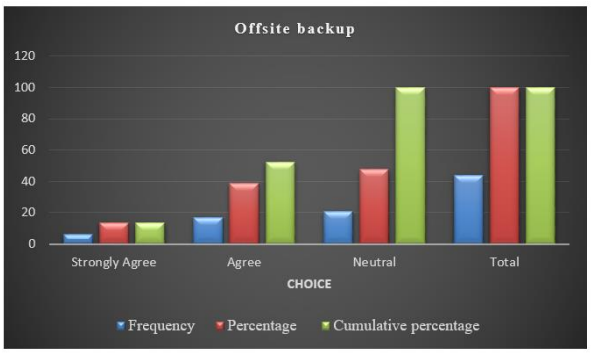
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	12	27.27	27.27
Agree	13	29.55	56.82
Disagree	9	20.45	77.27
Not sure	10	22.73	100.00
Total	44	100.00	



The researcher asked respondents if there is an offsite backup of the patient data.

Table 11. Offsite backup availability

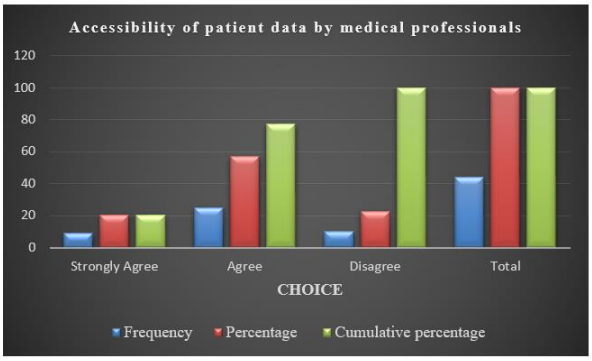
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	6	13.64	13.64
Agree	17	38.64	52.28
Not sure	21	47.72	100.00
Total	44	100.00	



The researcher asked respondents if Healthcare professionals have access to patients' information when needed.

Table 12. Accessibility of information by medical professionals

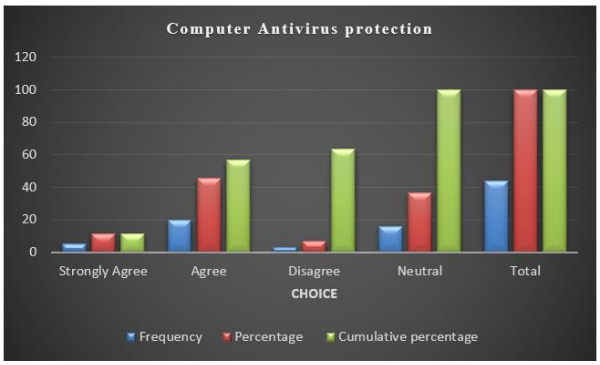
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	9	20.45	20.45
Agree	25	56.82	77.27
Disagree	10	22.73	100.00
Total	44	100.00	



The researcher asked respondents if the computer being used has an updated Antivirus

Table 13. Use of Anti-Virus

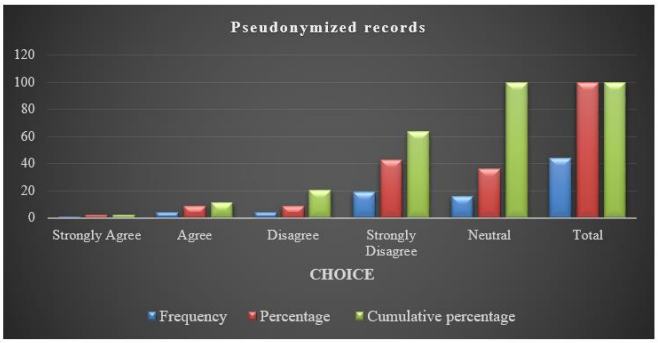
Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	9	20.45	20.45
Agree	25	56.82	77.27
Disagree	10	22.73	100.00
Total	44	100.00	



The researcher asked respondents if Patient records are always Pseudonymized.

Table 14. Patient records Pseudonymized

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	1	2.27	2.27
Agree	4	9.10	11.37
Disagree	4	9.10	20.47
Strongly Disagree	19	43.18	63.65
Neutral	16	36.35	100.00
Total	44	100.00	



5.2 Relationship between Information Security on Secure Service Delivery

5.2.1 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 15. Correlation Analysis

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

The results show that information integrity and service delivery have a strong beneficial association (r = .679, P-value < 0.009). This implies that Information integrity influences service delivery in University of Nairobi Hospital. The results also revealed a strong favorable association between information confidentiality and service delivery (r =.612, P-value < 0.013). Hence, suggesting that information confidentiality influences service delivery in University of Nairobi Hospital.

The results showed a strong correlation between information accessibility and service delivery (r = .574, P-value < 0.0426) thus, depicting that information availability influences service delivery in University of Nairobi Hospital.

5.2.2 Regression Analysis

A multiple regression analysis was undertaken to further gauge the association among the

independent variables on service delivery in University of Nairobi Hospital. To aid this, 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 (Secure 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 16. Model Summary

Model	R	R Square	Adjusted Square	R 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: Secure Service Delivery

Table 16 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

University of Nairobi 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 secure service delivery.

Table 17. 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 shows that the regression model significantly and accurately predicts the dependent variable. The F test shows the statistical significance of the employed regression model. The regression model generally statistically and significantly predicts the outcome variable that is a good fit for the data, as shown by the P=0.001, which is less than 0.05.

Table 18. 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	2.2	0.0274

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

Ybt = 7.232 + 0.802X1+ 0.769X2+ 0.473X3

According to the model, the service delivery will always be 7.232 if all of the predictor values are zero. The model predicts that service delivery will rise by 0.802 units whenever the value processed through information integrity changes by one unit. In addition, if information confidentiality changes by one unit the service delivery increases by 0.769.

The study's results also showed that service delivery will rise by 0.473 when information availability changes by one unit.

The t-test was used to determine the significance of each variable, which had a 0.05 base value. 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 demonstrates how there is a connection 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).

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 customer is involved throughout the entire service delivery process. Information security breaches can result in clinical diagnoses that are incorrect, which can have serious consequences for patients.

5.4 Developed Model

Table 15 in the example below displays the real data, but after the pseudonymization process, the sensitive material is concealed, and the de-identified data is still significant and useful for research.

Table 19. Basic Pseudonymization technique

Healthcare ID	Date	Name	Medication	Condition
2001567898761234	12/12/2022	Babu Loliondo	Insulin	CD(Conduct Disorder)
2008123456785000	10/05/2022	John Pombe	Dapotum	MH(Malignant hyperthermia)
2001567898761234	10/10/2022	Babu Loliondo	Thalitone	CKD

Table 20. Pseudonymized data (Health care ID & Name)

HealthCare ID	Date	Name	Medication	Condition
0102	12/12/2022	A12	Insulin	CD(Conduct Disorder)
452	10/05/2022	B02	Dapotum	MH(Malignant hyperthermia)
2712	10/10/2022	N17	Thalitone	CKD

The data for the concealed connective index is kept on another computer or in a secure location that is inaccessible to regular users.

Table 21. Health ID, healthcare identifier Pseudonym

Healthcare ID	Healthcare Identifier Pseudonym
2001567898761234	0102
2008123456785000	452
2001567898761234	2712

Table 22. Name and name Pseudonym

Name	Name Pseudonym
Babu Loliondo	A12
John Pombe	B02
Babu Loliondo	N17

The distinction between encryption and pseudonymization is that sensitive information and relationships are exposed when encryption or password authorization is used. Pseudonymization, on the other hand, exposes relationships while concealing critical information. Data patterns must be preserved for linking or analysis, and personal data that will be shared—internally or with a partner—must be concealed while being used—are the two key conditions for Pseudonymization.

As a result, risk exposure will be lower, and any possible effects of internal and external security breaches will be lessened. Pseudonymization successfully makes stolen data unusable for identity theft and other types of fraud. By employing de-identified data to identify accounts, process account papers, and record accounts, this makes secure outsourcing and offshore possible. The hospital can save money while greatly decreasing the security concerns associated with hiring third parties.

De-identified data can be used by system integrators, developers, and system administrators for the health software industry to estimate E-Health projects that deal with sensitive health data, design and test new systems that draw on existing operations for sensitive health data, and maintain E-Health systems that manipulate sensitive data.

6. Conclusion and recommendation

6.1 Introduction

This section summarizes the recommendations and conclusions which were arrived at after analysis of the data. It also gives suggestions for further research reference to the general objectives of the study.

6.2 Summary of Findings

The results from this project revealed that over 70% believed introduction of Confidentiality, Integrity and availability on the security of M-health systems would make University Health systems processes fairly convenient.

It was established that a good number, over 60% of staff had relative experience at the hospital over 5years, and at least 75% of these have acquired relevant academic qualification diploma and above in the field of specialty.

On the issue of timely update of medical records, I was noted that if Electronic Health System Integration Framework for Secure M-Health Service, 65.90% of staff would find it helpful.

On the issue of protection of medical records data, the researcher noted that a number of security measures have been put in place for this, including rights and roles in level of access, offsite backup availability, anti-virus installation and IT support team in place with at least 65% basic IT knowledge provisioned.

Patient records have not been Pseudonymized, thus making information gathered to easily allow the individual to be directly identified.

6.3 Conclusion

The study findings indicated the framework applied at University of Nairobi hospital has a gap to address pseudonymized records.

The study also revealed that the introduction of the proposed M-health framework based on service architecture model would improve security levels of the system.

The Electronic health system integration framework for secure m-health services demonstrated significance medical health records secure environment, enabling use of data and or information without infringement to patients.

6.4 Future Research Recommendations

The introduction of The Electronic health system integration framework for secure m-health services in University of Nairobi Hospital is an enhanced solution that would improve in healthcare and associated policies frameworks to be revised and improved for better health services not only in the Hospital but in the country at large.

A more focus should also address on expanding and integrating of similar systems and solutions deployed in other similar and blended environments and thus expand its usage in other hospitals in the country.

Explore and innovate possibilities to increase related services on the framework including simulations on some of the hospital activities that require similar facility in improving secure M-health.

Acknowledgments

We greatly appreciate the valuable contributions of our Mount Kenya University fraternity more so the school of computing and Informatics for offering us learning materials and a conducive environment to do the study. We also thank the University of Nairobi Hospital employees for their immense contribution of participating in this study. We extend our thanks to Lucy Namaswa for her immense contribution in logistics for the whole study.

Authors contributions

Samuel Nandasaba drafted the manuscript while Prof. Gregory Wanyembi and Dr. Geoffrey Mariga revised it. Prof. Gregoy Wanyembi was responsible for coming up with the topic of study as Dr. Geoffrey Mariga assisted in coming up with the objectives of the study. Samuel Nandasaba was responsible for Literature review as Dr. Geoffrey Mariga and Prof. Gregory Wanyembi revised the literature review. Dr. Geoffrey Mariga was responsible with designing of data collection Instruments and in analysis of data collected. Samuel Nandasaba was responsible for data collection. All authors read and approved the final manuscript.

Funding

Not Applicable

Competing interests

The authors of this paper declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

References

Ahmed, I., & Mousa, A. (2016). Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. *International Journal of Advanced Computer Science and Applications, 7*(9), 229-236. https://doi.org/10.14569/IJACSA.2016.070933

Beebe, N. L. V. S. R. (2005). Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security. Proceedings of the 2005 SoftWars Conference, Las Vegas, 1-18. Las Vegas.

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century.Informatik 2015. Bonn:Gesellschaft fur Informatik e.V..(S.553-770).

Bendiek, A., & Metzger, T. (2015). *Deterrence theory in the cyber-century.* Working Paper, Research Division EU/Europe Stiftung Wissenschaft und Politic, German Institute for International and Security Affairs.

Bowman S. (2013). Impact of electronic health record systems on information integrity: quality and safety implications. Perspect. Health Inf. Manag. 10, 1c

Brands, S. (2003). Privacy and Security in Electronic Health. *Security*, 1-12.

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

Charitoudi, K., & Blyth, A. (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. *Journal of Information Security, 4*(January), 33-41. https://doi.org/10.4236/jis.2013.41005

David, F. (2006). *Mobile application security system: Bell labs technical journal, 11*(3). https://doi.org/10.1002/bltj.20188

Elkhodr M., Shahrestani S., & Kourouche, K. (2012). A proposal to improve the security of mobile banking applications. InProc. of ICT and Knowledge Engineering, pages 260–265. IEEE. https://doi.org/10.1109/ICTKE.2012.6408565

Gejibo S., Mancini F., & Mughal, K. (2015). Mobile data collection: A security perspective. In: Sasan A, editor. Mobile Health: A Technology Road Map. Switzerland: Springer, Cham; 2015:1015-1042. https://doi.org/10.1007/978-3-319-12817-7_42

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness : towards an information security awareness process. 104(August 2012), 69-79. https://doi.org/10.23919/SAIEE.2013.8531867

Health, M. O. F. (2017). *Kenya Standards and Guidelines for mHealth Systems.*

Hong, K. S., Chi, Y. P., Chao, L. R., &Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. https://doi.org/10.1108/09685220310500153

Innab, N. (2018). Availability, Accessibility, Privacy and Safety Issues Facing Electronic Medical Records. *International Journal of Security, Privacy and Trust Management, 7*(1), 01-10. https://doi.org/10.5121/ijsptm.2018.7101

Iwaya, L. H., Ahmad, A., & Babar, M. A. (2020). Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study. *IEEE Access 2020, 8*, 150081-150112. https://doi.org/10.1109/ACCESS.2020.3015962

Kellerman, A. L., & Spencer, J. S. (2013). What it will take to Achieve The As Yet -unfulfilled promises of Health information technology, Pubmed/23297272.

Leon, N, Schneider, H., & Daviaud, E. (2012). Applying a framework for assessing the health system challenges

to scaling up mHealth in South Africa. BMC Med Inform Decis Mak. 2012, 12: 123-10.1186/1472-6947-12-123. https://doi.org/10.1186/1472-6947-12-123

Liddick, D. (2013). Techniques of Neutralization and Animal Rights Activists. *Deviant Behavior, 34*(8), 618-634. https://doi.org/10.1080/01639625.2012.759048

Lizasoain, A., Tort, L. F., Garcia, M., Gomez, M. M., Leite, J. P., Miagostovich, M. P., Cristina, J., Colina, R., & Victoria, M. (2015). Environmental assessment reveals the presence of MLB-1 human astrovirus in Uruguay. *J. Appl. Microbiol., 119*, 859-867. https://doi.org/10.1111/jam.12856

Lucas J. (2013). *Oracle,an Introduction to the basics of data integrity enforcement in a variety of environments.* Amis technology blog.

Maranda, A., & Majchrzycka, A. (2016). Secure development model for mobile applications. *Bulletin of the polish academy of sciences technical sciences 64*(3). https://doi.org/10.1515/bpasts-2016-0055

Ministry of health. (2016). Kenya national ehealth policy. 2016-2030.

Nganji, J. T., & Nggada, S. H. (2011). Disability-aware software engineering for improved system accessibility and usability. *International Journal of Software Engineering and Its Applications, 5*(3), 47-62.

Nkosi, M., & Mekuria, F. (2010). Cloud computing for Enhanced mobile health applications: IEEE. https://doi.org/10.1109/CloudCom.2010.31

Pernebekova, A. P., & Ahbergenovich, B. A. (2015). Information Security and the Theory of Unfaithful Information. *Journal of Information Security, 06*(04), 265-272. https://doi.org/10.4236/jis.2015.64026

Salim, H., & Salim, H. M. (2014). A Systems Thinking and Systems Theory Approach Cyber Safety : A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks By. (May).

Schein, R., Wilson, K., & Keelan, J. (2010). Literature review on effectivess of the use of social media: A report for Peel Public Health. *Challenges, 129*(1), 63. Retrieved from http://www.peelregion.ca/health/resources/pdf/socialmedia.pdf

Serhani, M. A., Benharref, A., & Nujum, A. R. (2014). Intelligent remote health monitoring using evident-based DSS for automated assistance, 2674-7. https://doi.org/10.1109/EMBC.2014.6944173

Shifali, A., Yttri, J., &Nilsen, W. (2014). *Privacy and security in mobile health(Mhealth) research.*

Simplicio, M. A., Iwaya, L. H., Barros B. M., Carvalho, T. C. M. B., & Naslund, M. (2015). Secourhealth: A delaytolerant security framework for mobile health data collection. *Biomedical and Health Informatics, IEEE Journal of, 19*(2), 761-772. https://doi.org/10.1109/JBHI.2014.2320444

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). Challenges of implementing e-learning in Kenya: A case of Kenyan Public universities. *The international review of research in open and distributed learning, 16*(1). https://doi.org/10.19173/irrodl.v16i1.1816

University of Nairobi. (2021,January 23). Fact file. https://uonbi.ac.ke/fact-file

Vimalachandran, P., Wang, H., Zhang, Y., & Whittaker, F. (2018). Ensuring Data integrity in electronic health records: A quality Health care implication.

W. Li, L. Cheng, (2013). *Effects of neutralization techniques and rational choice theory on Internet abuse in the workplace.* Pacific Asia Conference on Information Systems, Jeju Island, Korea.

Wallis, L., Blessing, P., Dalwai, M., & Shin, S. (2017). Integrating mHealth at point of care in low- and middle-income settings : the system perspective. *Global Health Action, 10*(00). https://doi.org/10.1080/16549716.2017.1327686

Wausi, A. N., & Waema, T. M. (2009). *Organizational implementation of Information systems innovations* (Unpublished doctoral thesis). University of Nairobi, Kenya.

WHO. (2018). *Use of appropriate digital technologies for public health* (Vol. 28).