Patients' Health Records Management in Ugandan Hospitals: A Case of Kabale Regional Referral Hospital

Nabimanya Daniel[1], Sembatya Richard[2], Atuhaire Ambrose[3], Businge Phelix Mbabazi[4]
[1, 4]*Kabale University, Ugandan*
[2, 3]*Mbarara University, Ugandan*

Abstract

Personal health record (PHR) is considered as an emerging patient-centric model of health information exchange, where people can share their health information to other people, however most health facilities in Uganda have not yet adopted it. The study investigated the patients' health record management at Kabale Regional Referral Hospital. The researcher interviewed fifty (50) Interviewees and data was analyzed using NVIVO version 11.The findings revealed that 88% of the total interviewees express the need for their information to be kept secret from untrusted parties while 12% of the total interviewees didn't express the need for their information secrecy from untrusted parties. When asked what they feel about what should be done to stop information disclosure to untrusted parties , 20% of the Interviewees expressed concern for keeping their information in closed rooms, 60% of the Interviewees expressed concern for information storage in the computer with passwords and 20% of the respondents expressed concern for hiring external authorities to store their information. The study concluded that privacy of patients' records was vital to the patients and recommended that security measures be implemented.

1. Introduction

Healthcare has changed over the years with the incorporation of information and communication technologies. This transformation also affected other aspects of healthcare, such as: the relationship between patients and doctors; the ways to deliver healthcare; and the capacity of data analysis for clinical and research purposes. Nowadays, EHRs are part of day-to-day activities [1] Day reality in most health facilities around the world. With the introduction of mobile computing and wireless communication technologies, applications are now designed to run in smart-phones and to use sensor networks to monitor patients in real-time. Healthcare professionals can access all the relevant or needed data through many computer interfaces (e.g. Desktops, smartphones, and Tablets). Likewise, the patients can have readily access to their medical journals by Internet. Essentially, information and communications technology help to improve quality of healthcare and patient's experience at reduced costs.

Notwithstanding, the security risks grew proportionally. Huge amounts of data have to be securely transmitted, processed, and stored. Systems can be potentially misused in patient's detriment. Privacy infringements can be caused by, e.g., purpose misuse, vague purpose specification, lack of patient's consent, and privacy policies. Security is one of the most imperative requirements for the success of systems that deal with highly sensitive data, such as medical information.

Legal Requirements: Legislation regarding confidentiality of health information is in place in countries around the world. In US, HIPAA (Health Insurance Portability and Accountability Act) regulates the privacy and confidentiality of health information, and there are sections regarding health research in HIPAA. PIPEDA (Personal Information Protection and Electronic Document Act) in Canada and Data Protection Act 1998 (effective since 2000) [2] in UK are some of the examples that are in place for privacy and confidentiality of health information. In Australia, New South Wales Health Records and Information Privacy Act 2002 which was effective since September 2004 also stated "The organization that holds health information must not use the information for a purpose other than the purpose for which it was collected unless the use of health information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics in the public interest". The legislation makes the situation more complicated.

A feasible solution is to encrypt the data prior to outsourcing to the cloud. Symmetric encryption does not work as it requires the encryptor and the decryptor to use the same key. It is likely both parties are not the same (e.g. The laboratory encrypts a medical record while a clinic decrypts it). In this case, key management remains the biggest issue. Asymmetric encryption can be used instead, compared to the traditional public key infrastructure (PKI), Identity-based encryption (IBE) shall be preferred as the encryption (e.g. laboratory) does not need to obtain the patient's digital certificate in advance which may be inconvenient or impractical. Instead, it may just use his name or national number

as the identity to encrypt the data. The patient can decrypt the data using his own secret key, which is given by a Private Key Generator (PKG). In practice, it may be a government authority.

It seems IBE can act as the security solution for PHR in the theoretical framework. However, when we look into the practical scenario, it seems to be difficult to facilitate, and hence impractical. IBE can only allow one specific person to decrypt. Other than this particular person, no one else (except the PKG) can decrypt. It is suitable if there is no sharing of PHR among different persons, but this will lead to an impractical situation.

Sharing of Records: In some cases, doctors may want to discuss the patient's medical situation with other doctors or researchers. It is especially important if the case is very special or has never been discovered before. It can not only help the patient who may receive assistant from other specialists, but also help future patients with the same symptom. Thus, it would be good if the medical system allows the sharing of PHR among specialists or researchers in the same area. IBE cannot facilitate this kind of sharing as it only allows the patient himself/herself to decrypt but not anyone else.

Several socioeconomic factors have contributed to increase the interest in the PHR area. Examples include the wider availability of mobile devices with high computing capabilities, the growth in coverage of mobile cellular networks and the necessity to need to actively adequate healthcare and support for people wherever they may be [4]. Ultimately, the world has reached a point, in which more people have access to mobile phones than to proper sanitation (toilets or latrines) and clean water [5].

The attention around the PHR area is spread all around the globe, which has recently led the world health organization (WHO) to develop surveys and reports focused specifically on such solutions [3]. Applications surveyed include mobile telemedicine, decision support systems, solutions for raising treatment compliance and awareness, Electronic patient records (EPR). Among the conclusions drawn from such studies is the fact that in the future and after an adequate evaluation, PHR solutions are expected to be integrated into and improve existing country-wide health strategies [4].

The deployment of PHR solutions is particularly promising in emerging countries in which health authorities can take advantage of the flourishing mobile market to bring adequate healthcare to un-served or underserved communities. Indeed, specialized applications for health surveys and surveillance play a crucial role in such regions, providing a rich repository for decision making systems in the field of public health [4]. application in this category typically involve remote data collection of primary healthcare(PHC) indicators, referred to family-related data, sanitary conditions, identification of common diseases in a given region, or from people tracking with chronic conditions/diseases. The data can be collected for example at health units located within the target communities or during visits to the patients` homes. This process is usually carried out by health teams that include medical personals (physicians and nurses) or health agents responsible for specific regions. The data collected is then used by health authorities. Allowing them to take place effective actions based on more accurate information about the health conditions in the area surveyed.

The DPAPB (Data Protection and Privacy Bill) of Uganda requires that patients` Data must be protected; however, a preliminary study conducted at Kabale Regional Referral Hospital revealed that, patients` health records must be protected. Data kept on paper forms which are easy to lose or even leak to untrusted channels. This has even brought doubts among patients wondering if their records are safe wherever they are kept. The most important concern refers to security even though medical data is usually subject to a very strict legislation aiming to prevent unauthorized use or disclosure, [5]. The available literature demonstrates that majority of the health systems in Uganda do not employ robust security solutions.

The study assessed the patients' health records management in Kabale Regional Hospital and the study sought to develop a framework for secure sharing of patients` health records at the Hospital level. Specifically looking at the status of medical records storage and disclosure to other parties, measures to stop information disclosure to untrusted parties.

2. Literature Review

In Uganda, there is no specific data protection or privacy law that directly applies to mHealth. In addition, Uganda has not implemented specific laws that govern the use and disclosure of health and medical data in general (i.e., an omnibus health data law similar to HIPAA) [6]. Ugandan Law however does recognize the right to privacy as a human right. Ethical and legal policies for the protection of health are generally not well developed. The ministry of health has promulgated a National Health Services Laboratory Policy that requires laboratory staff to safeguard privacy and confidentiality. Dr. Catherine Omaswa in Uganda National eHealth Strategic Plan document of 2013 to 2016 states that findings from literature show that Uganda is making great progress in embracing the use of ICTs and the accompanying potential to make major contributions to improving access and quality of health services.

According to the World Health Organization (who.int), Health services include dealing with the

diagnosis and treatment of disease, or the promotion, maintenance and restoration of health. They include personal and non-personal health services. Health services are the most visible functions of any health system, both to users and the general public. Service provision refers to the way inputs such as money, staff, equipment and drugs are combined to allow the delivery of health interventions. The online business dictionary (businessdictionary.com) defines health services as the acts of taking preventative or necessary procedures to improve a person's well-being. This may be done with surgery, the administering of medicine or other alterations in a person's lifestyle.

3. Challenges in Securing Electronic Health Records

Securing electronic health records in a scenario where many people or multiple actors potentially access information is a complex and costly activity. The definition of a secure model for data exchange would require the application of the following principles. Availability of information which refers to the level of accessibility of information upon request from the user. According to [7], in healthcare, the availability of information is essential in the provision of integral health services. Garson and Adams's study as cited in [7] states that the availability of information should be provided under a secure scheme in which confidentiality is also guaranteed. To protect the confidentiality of information, access to patient's data should be carried out under the principles of relevance and need to know. The principle of relevance prevents information overload and protects the patients privacy by restricting the release of information to the relevant data required to support the health process [8]. The principle of need-to-know guarantees that only personnel who required the information and have access privileges will be allowed to extract the data. Integrity of information is not a matter of incorporating additional security mechanisms within the system or securing the communication channel but also by ensuring that only authorized users can access, add or alter stored data [8].

User's willingness to adopt eHealth Systems - There is a significant potential for e-health to deliver cost-effective, quality healthcare, and spending on e-health systems by governments and healthcare systems is increasing worldwide. However, there remains a tension between the use of e-health in this way and implementation. Furthermore, the large bodies of reviews in the e-health implementation field, often based on one particular technology, setting or health condition make it difficult to access a comprehensive and comprehensible summary of available evidence to help plan and undertake implementation. This review provides an update and re-analysis of a systematic review of the e-health implementation literature culminating in a set of accessible and usable recommendations for anyone involved or interested in the implementation of e-health. [1]

Electronic health records generates complete data about patients. According to [1], EHR is the collection of electronic patient records about patients' health, past medical history, progress reports, diseases, medication and laboratory test results. These data have the ability to generate a complete record/information [1]

Electronic health record is vital to manage health related problems through complete and accurate information about the patients. EHR is crucial for better healthcare management as it provides integrity and accuracy of data in healthcare organizations, which is pivotal to both medical and legal areas [9].

3.1. Health Informatics

Health Informatics (HI) is "the interdisciplinary study of the design, development, adoption and application of IT-based innovations in healthcare services delivery, management and planning" [10]. In this research, we mainly deal with HI applied to public health (i.e., Public Health Informatics) and clinical medicine (i.e., Medical Informatics. Nonetheless, HI solutions can spread through a broad range of other fields, e.g., nursing, dentistry, pharmacy, biomedical research.

Lately, the term eHealth (electronic process in health) has been increasingly used to refer to health informatics using the Internet and related technologies [11]. In this research, we are particularly interested in the following eHealth sub-categories: Electronic Health Records (EHR), Personal Health Records (PHR), and mobile health (mHealth). Each of them is defined and briefly discussed below.

International Health System Standards - In this section, the researcher reviews literature on the US Health Insurance Portability and Accountability Act of 1996, Health Level 7 and the European Directive 95/46/EC on protection of personal data.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was released in the US in 1996 with a compliance date of April 14, 2003 to help improve healthcare delivery by streamlining health insurance coverage. Health Insurance Portability and Accountability Act sets standards for privacy of individually identifiable health records [12]. It regulates health providers such as hospitals on the permissible use and disclosure of identifiable health records [12]. It specifies that without written patient authorization of a highly prescriptive and purpose specific form, the health

providers may only make certain use of identifiable health records and may only disclose it to third parties for sanctioned purposes that are minimum necessary to accomplish treatment [12]. This act regulates both electronic and paper records.

Health Insurance Portability and Accountability Act (HIPAA) requires that patients be provided a privacy notice to educate them about their rights. This should indicate who will be able to see and use their medical records, what use will require the patient's specific authorization and their right to inspect, copy and change their medical records [13]. The providers are required to provide an accounting of all disclosures. The authorization to release patient's information must contain at least the description of the information to be released, the name of the person or entity authorized to release this information, a description of each of the purpose of the requested use or disclosure, an expiration date and the signature of the individual and date [13].

HIPAA states that providers should not use consent as a condition for treatment and that the health system should have an emergency access procedure.

3.2. Electronic Health Record (EHR)

EHR is probably the most widespread eHealth technology. According to the Healthcare Information and Management Systems Society:

"The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates and streamlines the clinician's workflow. The EHR has the ability to generate a complete record of a clinical patient encounter as well as supporting other care-related activities directly or indirectly via interface including evidence-based decision support, quality management, and outcomes reporting." [14].

EHRs are made for primary use, i.e., meaningful use for patient's treatment, with an implied trusted domain and confidentiality among medical staff. EHR are also increasingly being used for secondary purposes, such as release of data for governmental health programs and research [15].

Personal Health Records (PHR) is not as widespread as EHRs. A PHR is a user-centered application that allows individuals to manage their own health information and to share it with other people and/or healthcare providers [16]. PHR can be helpful for maintaining health (fitness and wellness reasons) as well as a tool to help with illness (treatment of patients). Examples of commercial PHR are HealthVault and Patients like Me. Such systems can be also integrated to other eHealth systems but specially mHealth applications. For instance, heart/glucose monitoring devices and mobile applications (e.g., run/walk trackers, calorie counters).

4. Security and Privacy for Healthcare

The respect of privacy is sine quinoa to healthcare. Its importance, as mentioned by [17], has been already manifested ages ago in one of the most widely known of Greek medical texts, the Hippocratic Oath.

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about." Excerpt from Hippocratic Oath [18].

High quality healthcare requires individuals to share their personal health information with healthcare professionals [16]. Furthermore, information should be complete and accurate. If patients cannot trust that their information will be kept secure, they will be reluctant to share it (or even to use the service). If health professionals cannot trust the organization to keep records secure, they will not put complete information. In both cases this leads to inferior healthcare. It is therefore paramount that privacy and security concerns are addressed during the design and development of any health information system. This section introduces the security and privacy technologies related to the research. For the sake of clarity, this part of the background is organized in four macro topics:

- General concerns on security and privacy
- Security mechanisms
- Privacy Impact Assessment (PIA)
- Data obfuscation and anonymization

That is, moving from the general to the specific concepts.

5. mHealth Security and Privacy

Essentially, mHealth inherits problems from mobile computing and wireless networks. The communication channels are more vulnerable due to their wireless characteristics (e.g., network eavesdropping and spoofing) and mobile devices

have more constrained amount of processing power and memory (i.e., need for lightweight cryptography). Devices can be shared among users, and they are more vulnerable to theft, loss and damage, which may result in data breaches, data loss, and privacy infringements.

Regarding the general issues linked to mHealth security and privacy, some interesting publications can be discussed. From a more technical perspective, stated by [20], the authors proposed a number of security and privacy recommendations for mHealth developers. These recommendations were made based on a preliminary survey of 169 papers, resulting in the nine general recommendations listed below:

- Access control – Use of patient-centered access control mechanisms (e.g., role-based access control), in which users should be able to allow or deny access to their information at any moment.

- Authentication – Users should be able to authenticate with a unique ID and password (or multi-factor authentication). Passwords should be kept in secrecy and should reach appropriate levels of security.

- Security and confidentiality – Use of encryption mechanisms (e.g., AES) with proper parameter configurations (i.e., key size).

- Integrity – Use of message authentication codes and digital signatures.

- Inform patients – Present privacy policy to users before collection of data that informs about the user rights and specifies the purposes of data collection and processing.

- Data transfer – Use secure communication channels (e.g., TLS, VPNs) while transferring data among entities. Notify user about data transfers.

- Data retention – Inform users about retention policy. The data should be kept only for the necessary time to accomplish the initial purpose. User should be able to check when data is deleted.

- Body Area Network communication –Use security mechanisms for authentication and key distribution among sensors and smart-phones; establish secure communication channels among devices.

- Breach notification – In case of data breaches, the competent authorities and users should be notified. Entities should help users in order to relieve the consequences and restore possible damages.

Overall, the recommendations help developers to have a glimpse about privacy and security issues in mHealth. However, they are incomplete if compared to existing legislations on privacy and data protection, and thus, have limited practical use. In the case of European Union (EU), the General Data Protection Regulation (GDPR) is the upcoming regulation for personal data privacy and protection, replacing the EU Data Protection (Directive 95/46/EC, 1995).

Many countries (i.e., separate legal jurisdictions) however do not have specific legislation for data privacy. This does not imply a legal void in the area, but privacy rights might stem from the constitution or consumer rights; and in the case of healthcare, from medical codes of conduct, and so on. Thus, from the legal perspective, some publications help to bridge this gap between privacy and mHealth technologies. For example, [19] presents a list of five guiding principles for mobile privacy in the context of developing countries (that map to principles of the GDPR):

Principle 1. Address Surveillance Risks – Projects should take steps to ensure that user data is secure from third party surveillance, e.g., user discriminatory profiling can be made by mobile operators and government.

Principle 2. Limit Data Collection and Use – Projects should limit data collection to what is absolutely necessary for the project's goal, e.g., by employing access control, data retention policy, and not collect unnecessary data.

Principle 3. Promote and Facilitate Transparency – Projects should be transparent about what data is collected, how it is shared, and how it might be used in the future, e.g., user notifications, data transfer policies, audit trails of others that also have access to the data.

Principle 4. Incorporate User Feedback – Projects should give users the ability to access, amend, and/or delete their data, e.g., create user interfaces, create communication channels to receive feedback from users.

Principle 5. Assume Responsibility – Projects should assume accountability for potential risks and harms incurred via their projects and plat- forms, e.g., perform risk assessment, plan incident response, and notify data breaches.

The content of the recommendations and the guiding principles offer a good starting point for developers and project leaders. However, in practice, security and privacy analysis should be done case-by-case, given the complexity, multiplicity of actors, jurisdictions, and highly culture-specific dimensions of privacy.

6. Methodology

The researcher collected data from patients and medical practitioners within Kabale Regional Referral Hospital using an interview method. Kabale Regional Referral Hospital was selected because it comprises of several semi-autonomous sections offering a variety of healthcare services to a wide range of patients. More so, choice of case study was based on proximity and availability of all research participants in the same location which favored this research given limited resources in a developing country set up. The researcher collected data from different departments and sections within KRRH because health records pertaining to patients attending these departments is very sensitive to privacy and yet important for healthcare.

The objective of these interviews was to determine requirements by patients and medical personnel on medical data sharing. The interview guide was categorized based on the study specific objectives. The collected data was grouped and analyzed descriptively. The selection of 50 patients was done using the confidence interval method. (Eduard and Johannes 1999) This method uses the formula:

Sample size $n=z2(pq)\ e2$
Where:
n= the sample size (50)
z= standard error associated with the chosen level of confidence (1.96)
p= estimated percent in the population
q= 100 – p
e= acceptable sample error

The collected data was analyzed using NVIVO version 11 and is presented in the next chapter.

7. Findings

The Summary of the data analyzed as per requirement is presented in the Table below.

7.1 Existing health System

Kabale Regional Referral Hospital (KRRH) is owned and operated by the government of Uganda. It constitutes several units, departments and directorates that manage their own facilities and offer specialized quality medical care to patients. KRRH is a referral hospital in Western Uganda and provides training facilities for Kabale University Faculty of Medicine courses and other various medical schools around Kigezi Region. Data collection to determine patient data sharing and security needs was done within KRRH premises in different departments.

Table 1: Existing Health System

S/N	Requirement	Sub Category	Brief Statistic
A	Existing Situation	The Hospital systems	Generally, data flow among the different entities of KRRH is fairly structured and has high prospective to integrate eHealth systems
Aa		Frequency of Visits	Majority of patients do not make frequent visits to a health service provider for at least in a year
Ab		Patient Information shared	A big percentage of patients often give out information on every visit and they are not sure where is kept and how it's preserved.
Ac		Data security Privacy Concerns	A greater number of patients mind about privacy and confidentiality of their health records while a small percentage do not mind or have no idea about what it is used for.
Ad		Knowledge on Privacy enforcement on digital devices	A big number of patients have Insignificant proficiency on use of security measures on electronic devices. A visible number do not have an idea on such measures.
Ae		Knowledge about HER	A bigger number of patients do not know about EHR while a small percentage have heard or learnt about HER

B	Required Situation		Generally, many patients expressed a need for better means of achieving required services in terms of data sharing and security.
Ba		Data to Share Privately with health practitioner	A big number of patients feel Comfortable sharing any information with a health practitioner while some limit it to only sexual health information.
Bb		Need for personal Data securing	Almost All patients want to be in charge of their personal health information and determine who accesses it
Bc		Data Sharing Across medical experts	A good percentage of patients are positive about health practitioners sharing their personal health information but only for treatment purposes.
Bd		Fear of EH Systems?	Many patients fear unauthorized access with the use of EH systems. Some fear technology change and device theft while some exhibited no fear at all.
Be		Preference of particular Device	A big percentage of the respondents preferred to use personal mobile phones for their mobility, availability and perceived ease of use.

Data to analyse the existing needs and requirements for patient data sharing and security to their personal e-health data was collected using an interview guide. This data was analysed and is presented below in Table 1 based on the interview guide and research objectives.

7.2 Patients Requirements

The researcher interviewed fifty patients at Kabale Regional Referral Hospital using an interview guide. The interviews were to guide the researcher to determine the existing data sharing and security infrastructure at Kabale Regional Referral Hospital and determine requirements for patient centered data sharing and access with secure means.

7.2.1. Patients- Visit per Gender. The existing situation shows that the frequency for gender of patient visits to the hospital is moderate as for the males are slightly lower than the females. As shown in the 4.2, 46% of the male respondents visit the health facility, 54% of the female respondents visit the health facility.

Table 2: Patients- Visit per Gender

Patients- Visit per Gender	Frequency	Percent
Male	23	46
Female	27	54
Total	50	100

7.2.2. Patient's age group. The researcher wanted to know patients visit a health facility, they are respectively categorized principally by age group as part of the information required from them. Interviews show that 100% of the respondents as shown in the Table 3, 46% of the respondents were in the age bracket of 31 to 40, followed by the age bracket of 30 and below with 26%, then 20% of the respondents between the ages of 41 to 50, followed by 6% of the age bracket of 61 and above and 2% of the respondents were of the ages between 51 and 60 years.

Table 3: Patients age group

Age Bracket	Frequency	Percent
30 and below	13	26
31 – 40	23	46
41 – 50	10	20
51 – 60	1	2
61 and above	3	6
Total	**50**	**100**

7.2.3. Visitation period. The researcher wanted to know about how long they have known this health facility and paying a visit, the frequency of patient visits to the hospital are not high. As shown in the Table 4, 32% of the respondents have known the health facility and visited it in less than a year, 32% of the respondents have also known the health facility and visited it for 1 year, 26% of the respondents have well-known the health facility and visited it in 2 years, 10% of the respondents have also identified the health facility and visited it in 3 years and above. For the patients visits to the hospital has been either on doctor's appointment or those who are going for their first time.

Table 4: Visitation period

Visitation period	Frequency	Percent
Less than a year	16	32
1 Year	16	32
2 Years	13	26
3 Years	5	10
Total	**50**	**100**

7.2.4. Patients visit to the health facility. The researcher also wanted to know the percentage of respondents that had been admitted at the hospital and those paying a visit as well. Results in Table 5 show that 74% of the total respondents were admitted at the hospital by that time and 26% of the respondents were not admitted at the hospital by that time which indicates maybe they were paying a visit to the health facility**.**

Table 5: Patients visit to the health facility

Patients visit to the health facility	Frequency	Percent
Am admitted here	37	74
Attending to those who are admitted	13	26
Total	50	100

7.2.5. Respondent's Hospital Affiliation. The researcher further wanted to establish the percentage of respondents attached to different hospital departments. The hospital departments include pediatrics, obstetrics, general/medical, maternity, surgical and others. As shown in the Table 6, 58% of the respondents were attached to medical department, 34% of the respondents were found to be attached to obstetrics and 8% of the responds were also found to be attached to the pediatrics whereas other departments were not well attached to by any of the respondents who were selected for interviewing.

Table 6: Affiliation

Affiliation	Frequency	Percent
Pediatric	4	8
Obstetrics and Gynecology	17	34
Medical	29	58
Total	50	100

7.2.6. Need for information provided by hospital. The researcher also was interested in the perception of patients towards the security and awareness of how private their data may be secured when given to the health workers. As shown in Table 7, interview results show that 40% of the respondents were aware that the information collected from them at the hospital is for record purposes, 20% of the respondents were aware that the information collected from them at the hospital is for accountability purposes, 32% were aware that the information collected from them at the hospital is for creation of awareness about certain diseases and 8% of the respondents were aware that the information collected from them at the hospital is for decision-making purposes.

Table 7: Need for information

Need for information	Frequency	Percent
Record purposes	20	40
Accountability purposes on drugs	10	20
Creating awareness about certain diseases	16	32
Making Decisions	4	8
Total	50	100

7.2.7. Patients' health information storage status. The researcher wanted to find out if the information about them together with medical records they give at the time of health unit visit, is preserved.

Table 8: Record Status

Record Status	Frequency	Percent
Keep in their record rooms	47	94
Throw them away	3	6
Total	50	100

Results show as indicated in Table 8 that a total of 94% of the respondents were sure that the information, they give is kept in record rooms and a total of 6% of the respondents were not sure if it's stored or not. This indicates that a bigger percentage of the patients are well sure that information is kept in the health facility record rooms.

7.2.8. Need for Security. If asked if their information should be kept secret/private from unauthorized persons, in the Table 9, 88% of the total responds express the need for their information to be kept secret from untrusted parties, 12% of the total responds did not express the need for their information secrecy from untrusted parties.

Table 9: Need for Security

Need for Security	Frequency	Percent
Yes	44	88
No	6	12
Total	50	100

All the results show that large number of respondents were not confident that their information secrecy and storage not guaranteed security.

7.2.9 The patients' fear for their information disclosure. Patients if asked whether their medical records will be disclosed to other parties across the health facility systems, as shown in Table 10. A total of 64% respondents said its true it is being disclosed and 36% of the total respondents it's not disclosed to other parties. This implies that a bigger number of patients expressed concerns and fear for their information disclosure to other untrusted parties which poses a threat to most not willing to give out the right information.

Table 10: Patients' information disclosur*e*

Patients' fear	Frequency	Percent
Yes	32	64
No	18	36
Total	50	100

7.2.10. Safeguarding measures of patient's information. The researcher wanted to find out how they feel about what should be done to stop information disclosure to untrusted parties, as shown in Table 11, 20% of the respondents expressed concern for keeping their information in closed rooms, 60% of the respondents expressed concern for information storage in the computer with passwords and 20% of the respondents expressed concern for hiring external authorities to store their information. This implies that most of the respondents expressed concerns for security about sharing information their give out for treatment at the hospital.

Table 11: safeguard patient's information

Safeguard Patient's Information	Frequency	Percent
Should keep the information in closed rooms	10	20
Should keep the information in computers with passwords	30	60
Should keep the information in computers with passwords	10	20
Total	50	100

7.2.11. Patients' acceptability of eHealth services. The researcher wanted to establish if electronic health services are a better way than traditional way of storing patient's medical records. 46% of the respondents strongly agree with the eHealth service, 25% of the respondents also prefer the eHealth service, 26% of the respondents were neutral to any means of storage and only 2% of the respondents disagree with the eHealth services. As indicated in the Table 12, a bigger number of the responds prefer to have their medical records be kept in computerized system which is a good indication for electronic security.

Table 12: Acceptability of eHealth services

Acceptability of eHealth services	Frequency	Percent
Strongly agree	23	46
Agree	13	26
Neutral	13	26
Disagree	1	2
Total	50	100

7.2.12. Patients' acceptability of secure systems. Of the 50 respondents that were interviewed 100% had a positive attitude towards introduction of computerized security systems to track who should and who shouldn't access patient's medical records once its collected from patients at the time of hospital visit and this implies that almost all the respondents were in agreement with implementation of the secure systems for data sharing across the hospital general data system.

7.2.13. Patients' acceptability of secure sharing. Finally, the researcher wanted to establish which data sharing method will be preferred to the respondents for this framework. 100% of the respond's respondents prefer a secure and more private ways of sharing their medical records with authentication from the owner of the data before it is shared, a small percentage did not have any idea about it and this indicated that almost all preferred secure sharing.

8. Recommendation(s)

This research produced a framework for secure sharing to personal medical health records across the health systems in developing countries. Future work will involve building an actual system to implement the requirements gathered in this research and implementing it in the real world. Other information security domains such as telecommunication and network security, business continuity and disaster recovery, application and system development security and physical security are outside the scope of this research, but future research can look into integrating them into this framework.

This research acknowledges that some patients may not be able to use electronic devices such mobile phones or computers. This does not negate their rights to privacy. There is need for future research on how to enable such patients to be able to manage sharing of their electronic health records.

9. Conclusion

From the data analysis illustrated in the Tables, there is a significant positive perception towards the need for health data sharing and access. The analysis

however shows that absolute data Security in terms of Confidentiality, Integrity and Availability need to be a central consideration. A big number of respondents are very cautious about their privacy because they say that health data is very sensitive and they would not have it accessed by people they do not know or trust. There are a big number of people who want their medical records to be kept private and secure. Most of the patients would like to have ubiquitous control their medical records.

10. References

[1] Qureshi, Q.A., (2012). Determining the users 'willingness to adopt electronic health records (ehr) in developing countries. Gomal University Journal of Research, 28(2), pp.140-148.

[2] Act, Data Protection. "Data protection act." London Station off (1998).

[3] Archibald, S., Coggshall, J.G., Croft, A. and Goe, L., (2011). High-Quality Professional Development for All Teachers: Effectively Allocating Resources. Research and Policy Brief. National Comprehensive Center for Teacher Quality.

[4] Protection, D., Bill, P. and Analysis, L. 'Uganda : Legal Analysis', 2015.

[5] Noor, T.H., Sheng, Q.Z., Ngu, A.H., Alfazi, A. and Law, J., (2013), October. Cloud armor: a platform for credibility-based trust management of cloud services. In Proceedings of the 22nd ACM International Conference on Information and Knowledge Management (pp. 2509-2512).

[6] Noor, T.H., Sheng, Q.Z., Ngu, A.H., Alfazi, A. and Law, J., (2013), October. Cloud armor: a platform for credibility-based trust management of cloud services. In Proceedings of the 22nd ACM International Conference on Information and Knowledge Management (pp. 2509-2512).

[7] Coker, T.R., Rodriguez, M.A. and Flores, G., (2010). Family-centered care for US children with special healthcare needs: who gets it and why? Pediatrics, 125(6), pp.1159-1167.

[8] Lannuzel, D., Tedesco, L., Van Leeuwe, M., Campbell, K., Flores, H., Delille, B., Miller, L., Stefels, J., Assmy, P., Bowman, J. and Brown, K., (2020). The future of Arctic sea-ice biogeochemistry and ice-associated ecosystems. Nature Climate Change, 10(11), pp.983-992.

[9] Anderson, P.D., Mehta, N.N., Wolfe, M.L., Hinkle, C.C., Pruscino, L., Comiskey, L.L., Tabita-Martinez, J., Sellers, K.F., Rickels, M.R., Ahima, R.S. and Reilly, M.P., (2007). Innate immunity modulates adipokines in humans. The Journal of Clinical Endocrinology and Metabolism, 92(6), pp.2272-2279.

[10] Doos, L., Ward, D., Stevens, A. and Packer, C., (2016). Accuracy of pharmaceutical company licensing predictions: projected versus actual licensing dates. Journal of Pharmaceutical Health Services Research, 7(2), pp.117-122.

[11] Mettler, T. and Raptis, D.A., (2012). What constitutes the field of health information systems? Fostering a systematic framework and research agenda. Health Informatics Journal, 18(2), pp.147-156.

[12] Kulynych, J. and Korn, D., (2003). The new HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: help or hindrance for clinical research? Circulation, 108(8), pp.912-914.

[13] Annas, G.J., 2003. HIPAA regulations-a new era of medical-record privacy? New England Journal of Medicine, 348(15), pp.1486-1490.

[14] Vreeland, A., Persons, K.R., Primo, H.R., Bishop, M., Garriott, K.M., Doyle, M.K., Silver, E., Brown, D.M. and Bashall, C., (2016). Considerations for exchanging and sharing medical images for improved collaboration and patient care: HIMSS-SIIM collaborative white paper. Journal of digital imaging, 29(5), pp.547-558.

[15] El Emam, K., Jonker, E., Arbuckle, L. and Malin, B., (2011). A systematic review of re-identification attacks on health data. PloS one, 6(12), p.e28071.

[16] Paul, C.R., (2006). Introduction to electromagnetic compatibility (Vol. 184). John Wiley and Sons.

[17] Cooper, J., (2007). Cognitive dissonance: 50 years of a classic theory. Sage.

[18] Edelstein, L., (1943). Andreas Vesalius, the humanist. Bulletin of the History of Medicine, 14(5), pp.547-561.

[19] Hussain, M., Chen, D., Cheng, A., Wei, H. and Stanley, D., (2013). Change detection from remotely sensed images: From pixel-based to object-based approaches. ISPRS Journal of photogrammetry and remote sensing, 80, pp.91-106.

[20] Catalina, MARTÍNEZ MEDIANO, and GALÁN GONZÁLEZ Arturo. Técnicas e instrumentos de recogida y análisis de datos. Editorial UNED, 2014.

