East African Journal of Education and Social Sciences
EAJESS November –December 2023, Vol. 4, No. 6, pp. 17-28
ISSN: 2714-2132 (Online), 2714-2183 (Print). Published by G-Card
DOI: https://doi.org/10.46606/eajess2023v04i06.0330.

Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulations

Neema Eugene Shiyo
ORCiD: https://orcid.org/0009-0003-3158-7115
Department of History, Political Science and Development Studies, Dar es Salaam University College of Education, University of Dar es Salaam, Tanzania

Email: nemyangel@yahoo.com

Abstract: This paper sought to establish the awareness of the importance of patient privacy as well as the awareness of available policies guiding the handling of patients' personal and health records. Using the case study design, the study collected data from doctors, nurses, ICT officers as well as patients from four hospitals selected purposively in Dar es Salaam and Dodoma regions of Tanzania. A total of 43 respondents participated in this study. Data was subjected to thematic analysis using the NVIVO 12 plus computer package. Results show that both providers and users of e – health services in Tanzania consider patient privacy to be an important issue and they relate it to morality, personal respect and dignity. Level of awareness of existing government institutions guiding the work of health service providers was found to be low. It is concluded that, the presence of regulatory institutions is not enough if these institutions are not known, valued, considered and used by members of organizations. There is a need for the e – health service providers and patients to familiarize themselves with available policies and regulations for the health providers and for the government to promote these regulatory institutions.

Keywords: awareness; e-health; institutions; patient privacy.

How to Cite: Shiyo, N. E. (2023). Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulation. East African Journal of Education and Social Sciences 4(6), 17-28.
Doi: https://doi.org/10.46606/eajess2023v04i6.0330.

Introduction

In routine situations the use and importance of rules and standard operating procedures is well documented (March & Simon 1958). One example of these routine situations is the work of health service providers. In the provision of health services, one of the most recent and accepted and promoted development is the use of ICT in keeping patients' records. Currently, the development of electronic health records management is being emphasized across the world. Globally, ICTs play an increasingly integrated role in the provision and management of healthcare services, known as e-health. In this regard, in 2005 the World Health Organisation recognized e-health as the way to achieve cost-effective and secure use of ICTs for healthcare and related fields, and urged its member states to consider drawing up long-term strategic plans for developing and implementing e-health services and infrastructure in their respective health sectors (Healy, 2008).

Tanzania is among the developing countries that have embraced this new way of recording patients' information. According to the URT (2013), e-health is the cost-effective and secure use of information and communication technology in support of health and health-related fields, including healthcare services, health surveillance, health literature, health education, knowledge and research. E-health introduces ranges of services, among others, electronic health records, mobile health services (m-Health) or telehealth (provision of health services at a distance) and e-learning by health workers which

has improved the quality, efficiency and access of health services (Msumi, 2018).

According to URT (2019), electronic health is an umbrella term to encompass all concepts and activities at the intersection of health and information and communication technologies, including mobile health, health information technology, electronic health records and telehealth. URT (ibid.) presents three main functions of e-health. These include the delivery of health information to health professionals and health clients through the internet and telecommunications media, the use of ICTs to improve public health services (e.g. through the education and training of health workers) and finally, the use of health information systems to capture, store, manage, or transmit information on patient health or health facility activities.

The paper is divided into six sections. The first section after the introduction engages, in short, some of the available related literature to set the background for the intended argument. The next section presents the theoretical framework that informs the study. Section four handles the methodology part while section five presents the findings and discussion. Conclusion on the findings is given in section six, followed by a list of references used in this study.

Background to ICT usage in Health Services

Digital ICT has been used to facilitate healthcare services by various organizations (public and private) in a wide variety of contexts. Service providers around the world are trying to develop electronic healthcare systems that can simplify patients' record management because the traditional paper-based records are inadequate in meeting the requirement of modern healthcare service delivery (Rezaeibagha, 2013). Electronic health information systems involve sharing data from many sources within or among organizations. All relevant information about a patient is stored in the computer system of the service provider known as electronic health records for storage and reference purposes (Msumi, 2018). Electronic health record is the application of internet and other related technologies in the healthcare industry to improve the access, efficiency, effectiveness and quality of clinical and business processes utilized by healthcare organizations, practitioners, patients and customers in an effort to improve the health status of patients (Obuaku-Igwe, 2021; Rezaeibagha, 2013). In other words, electronic health record is an electronic record of medical information of patients that can be created, gathered, managed and consulted by authorised people within and outside healthcare organisations (URT, 2019).

Digital technology has the ability to transform healthcare service delivery to a more proactive and consumer-oriented model of care and improve the cost, quality, confidentiality and accessibility of healthcare service. Using e-health records management, particularly e-patient records, gives better access to patient data compared to paper-based records systems. E-health record systems help health service providers to safely share and exchange patients' data and have easier control over patients' information (Rezaeibagha, 2013).

It is arguable that the potential benefits of electronic health records can be enjoyed if there is trust, privacy, confidentiality and protection of health data and related patients' information in specific terms (Peter, 2010). Privacy of health information is the right and desire of a person to control the disclosure of personal health information. In privacy, there must be a way for a service provider to prevent information about the patient that was obtained for one purpose from being used or made available for other purposes without the patient's consent (Rezaeibagha, 2013). One important step is to establish proper legislations to define patients' rights to privacy. Patients need to know how their information will be kept and who can access their health records and for what purpose (Peter, 2010). Institutional, technological and legal measures have to be implemented by data collectors and controllers to protect patients' data against unlawful use, unauthorized access and against all other unlawful sharing and usage. Electronic health records management systems may improve the quality of data collection, information sharing, accessibility and usage. On the other hand, data security, privacy and trust remain the major concerns as e-healthcare platforms become universally accessible to users across various platforms (Obuaku-Igwe, 2021).

According to the National Committee for Vital and Health Statistics (NCVHS) (2005-2006), healthcare patients' data protection includes information security, confidentiality and privacy in healthcare systems. In this regard, health information privacy is an individual's right to control the acquisition, uses and disclosures of identifiable health data. Security

refers to physical, technological or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure. On the other hand, privacy deals with policy but security deals with tools to implement the policy (Rezaeibagha, 2013). There are concerns that electronic health records sharing may lead to loss of control of data by healthcare providers and may result in inappropriate use of sensitive patient records (Bowman, 2011). It has also been reported that healthcare industry has the highest per capita data breach cost. Additionally, in 2016, over 27 million patient records were affected in daily health data breach in the United States (Obuaku-Igwe, 2021).

Protection of patients' electronic records might mean investing in privacy policy and security technology tools and human resource capacity specializing in privacy policy and security issues (Adjerid et al., 2011). According to Pritts (2008), American Society places a high value on individual rights, personal choice and a private sphere protected from intrusion. Medical privacy is a major concern for many Americans as the medical records include intimate details like social behavior, personal relationships, mental health, physical health and financial status. Proper consideration like privacy policy and security concerns to protect electronic health records is important in order to avoid inappropriate disclosure of patients' health data and even loss of control. In Switzerland, according to Ama-Amadasun (2016), protection of patients' privacy has been successful due to the fact that the healthcare system is regulated by several effective legal frameworks responsible for setting the health laws and ensuring effective compliance.

Although e-health records management promise a number of considerable gains, they have also elicited concerns from legislators, privacy advocates and patient rights groups (Adjerid et al., 2011). The concerns are about the ability of ICT to ensure trustable levels of patient privacy. Also, there are concerns that e-health records will be a major source of future health privacy risk. People are citing failures to keep up with best practices and advancing technology, resulting in unanticipated data insecurity. This brings in the importance of governance and privacy policy (Bowman, 2011).

Research by Rezaeibagha (2013) investigated existing challenges confronting protection of electronic patient records security and privacy in Iran and Sweden. The author argued that coordination of different security and privacy laws among different electronic patient records is the priority issue in e-health record sharing security and privacy. In their part, Adjerid et al. (2011) explored the landscape of health privacy legislation at the state level and examined the impact of variations in such privacy and confidentiality laws across the United States on the progress of Health Information Exchanges. These authors found that of all the states with laws intended to promote health information exchange growth, only those that include requirements for patient consent see positive health information exchange outcomes.

Several studies have been conducted to establish methods of curbing the challenge of patients' electronic data security. Kruse et al. (2017) analyzed and discussed prominent security techniques for healthcare organizations seeking to adopt a secure electronic health record system for the healthcare industry. The authors concluded that, it is difficult to say with confidence what techniques should and should not be used, depending on the size and scope of a healthcare organization. In their part, Martinez et al. (2013), propose a general framework to enable the accurate application of statistical disclosure control methods to non-numerical clinical data. Keshta and Odeh (2020) observed that issues of privacy and security that relate to patient information can cause there to be relatively low electronic medical records adoption by a number of health institutions.

Notwithstanding the many challenges facing the issues of health information security and patient privacy, health management information systems are implemented in various countries with the expectation that they will contribute to improving primary health care delivery (Anifalaje, 2012). Using Northern Nigeria as the empirical context of the study, this author shows weak accountability and inadequate legislative frameworks to control the behavior and interest mediation of local health agents working in donor funded programs. In South Africa, the causes of data breaches have been attributed to factors such as criminal attacks, human error and system glitches (Obuaku-Igwe, 2021).

The Tanzania National e-Health Strategy 2013-2018 provides as one of its strategic principles that provision of e-health should guarantee patient information rights, integrity and confidentiality (URT, 2013). While the e-health strategy is not clear

in the form of privacy and data protection framework, one would have assumed that this is an industrial code of standards, rules and protocols for information exchange and protection in the e-health context. In addition, National Information and Communications Technology Policy of 2016 holds as one of its policy strategies that the government shall ensure the presence of relevant laws and regulations for the acquisition, development, adoption, use and disposal of ICT products, services, and protection of infrastructure, as well as to develop frameworks for coordination and promotion of ICT security (URT, 2016).

In Tanzania, Msumi (2018) offers a descriptive analysis of e-health regulations. The author found that in the absence of robust data protection legislation for processing personal health data in the context of e-health, the current constitutional right to privacy remains inadequate to offer a regulatory framework for the protection of patients' data. Another publication by Kajirunga and Kalegele (2015) investigated e-health solutions focusing on interoperability and collaboration in Tanzania. The study established that lack of standard procedures to guide the lifecycle of e-health systems across the health sector and poor willingness to collaborate among health stakeholders are key issues which hinder the manifestation of the benefit of digital ICT use in the health sector in Tanzania.

The work by Hamad (2019) reviewed the status of adoption and use of the e-health and challenges of the e-health system in Tanzania and offered an overview of an e-health system from international journals, conference reports, organizations' websites and other reports. It is observed that there are countless initiatives that consider the adoption and use of e-health system as the way to improve the health sector across the country such as health information system, teleconferencing, teleconsultations, m-health, e-health record and telehealth systems. Still, the author found that there are a number of challenges facing the health sector including ICT knowledge and skills, compliance with e-health standards and system interoperability. Mashoka et al. (2019) investigated the importance of using electronic medical records at the Muhimbili National Hospital, and the challenges and lessons learnt before and after implementation. The authors observed that the implementation of electronic medical records system should ensure that a comprehensive plan is in place that involves staff training, improving and installation of new information technology systems and funds for unforeseen issues and ongoing maintenance.

One trend that is demonstrated in the available literature about patients' privacy in the context of e-health record management is that the existing publications in developing countries have not explicitly investigated the issue of e-health record and patient privacy in relation to levels of awareness among health service providers and users. In countries like New Zealand, United Kingdom and Scotland, there is a framework of data governance with best practices and mechanisms to protect health data privacy at all stages of data development and use to ensure that the benefits of safe data are realised (OECD, 2015). The best practices pose a learning tool for health service providers and users. It is one thing to have institutions in place but quite another for the targeted behaviour exhibitors to be aware of the requirements, attach value to them and actually implement them. It is therefore important to explore whether the target group of e-health data handlers are actually aware of the importance of e-health patient privacy and whether the available regulatory institutions are known and are effectively valued and used to regulate behaviour.

Theoretical Framework

This study is informed by New Institutionalism which focuses on the role of institutions in shaping the actions of individuals and organizations. Institutions are defined as collections of interrelated rules and routines that define appropriate actions in terms of relations between roles and situations (March & Olsen, 1989). In the same vein, March and Olsen (1994) argued that institutions tend to provide a logic of appropriateness. This means that they establish expected appropriate behaviors for individuals and organizations. Individuals and organizations are expected to conform to established policies, laws, rules, regulations and norms. This premise is useful for understanding how the awareness and use of the available institutional framework for protection of personal data and patients' privacy in Tanzania helps in shaping the behavior of e-health service providers in selected hospitals involved in the collection, storage, use and dissemination of patients' information. This theoretical approach can be useful for assessing how current practices of patients' data handling by health professionals reflect awareness of and adherence to existing regulatory institutions in Tanzania.

New Institutionalism has three major variants namely Sociological Institutionalism, Historical Institutionalism and Rational Choice Institutionalism. This study was guided by the Rational Choice Institutionalism. This theoretical approach focuses on assessing the way behaviors of organizational members are a function of rules and incentives (Weingast, 1996). They view institutions as systems of rules and incentives or inducements to behavior in which individuals attempt to maximize their own utilities. This view is useful for understanding how the current institutional framework creates inducements for e-health professionals and how the professionals choose which institutions to adhere to.

Methodology

Design and Sampling

This study is qualitative and explorative in nature. Its qualitative nature offered the opportunity to uncover patients' privacy experiences and perspectives. Multiple case design was deployed to explore e-health records management mechanisms for safeguarding the privacy of patients in selected two public and two private hospitals in Dar es Salaam. Yin (2018) argues that a multiple-case study is preferred in many scenarios since the analytic conclusions from more than one case study will be more powerful than from a single case study. This design also allowed the use of multiple cases design in which the data collected facilitated establishment of the similarities and differences existing among the cases. This research work was carried out in Dar es Salaam and Dodoma regions of Tanzania.

Population and Sampling

This study employed the criterion sampling technique which is a type of purposive sampling where the researcher searches for cases or individuals who meet a certain criterion. Purposive sampling technique was employed for semi-structured interviews in the selected hospitals and the Ministry responsible for health. Public hospitals were Muhimbili and Mwananyamala while private hospitals were Aga Khan and Rabininsia hospitals. These hospitals were purposively selected because of their prominence in healthcare provision in Dar es Salaam and they used digital technologies in e – records management aspects like in collection, use, storage and dissemination of data.

Sources of Data

The first set of data was drawn from secondary sources where the researcher analyzed health policy documents, privacy and security documents, published evaluation reports, digital health strategic plans, journal articles, book chapters, conference reports, published research reports and websites. The second set of data was collected through the Key Informant Interviews conducted with knowledgeable respondents about e-health records and privacy issues. Furthermore, semi-structured interviews were conducted with the service users.

Statistical Treatment of Data

Thematic analysis was used with the Nvivo 12 Plus program to analyze the data. The software aided in data management, coding, analysis and interpretation of the transcribed files and policy documents. This study used general themes linked to the study objectives. The themes were created deductively from related literature. Word frequency, text search queries and auto-coding were all used in the software to create additional initial codes. The entire dataset or a single transcript was later searched using a text search query, and the results generated automatic coding of the data.

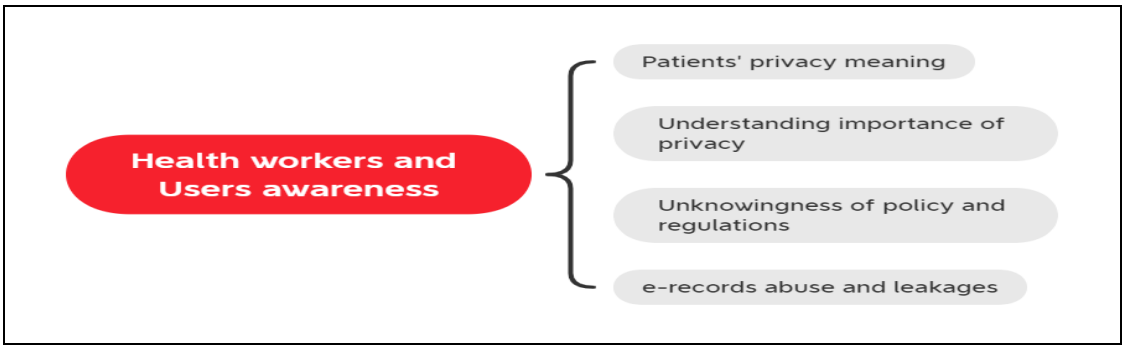

Figure 1: A Mind Map Showing Health Workers' and Users' Awareness Theme

As seen in Figure 1, the awareness of health providers and users about e-health patients' privacy issues yielded the following themes: patient's privacy meaning, understanding importance of

privacy, unknowingness of policy and regulations and information abuse and leakages.

Validity and Reliability

Validity and reliability in this study were assured through two ways. First, the instruments of data collection were pre tested with a group of eight university students on filed attachment to one of the hospitals. After the test, the instruments were improved before being applied in the field. Secondly, the field data from patients and health service providers was triangulated with data from government sources which are highly reliable. The aim was to check the extent to which results from the field confirmed or contradicted what the government was reporting. The process of data analysis was also rigorous and transparent using a modern computer software.

Ethical Considerations

All the respondents were treated with respect and their responses were handled with confidentiality. Names of respondents were never mentioned. Names of participating health service entities like hospitals were also concealed. Each hospital was labelled using alphabetical letters. Ethical guidelines for the University of Dar es Salaam were applied and all necessary permits sought and use as required.

Findings and Discussion

This section presents the results and discussions. It is guided by research questions of the study.

Research Question 1: Are Hospital Workers and Patients Aware of the Importance of Patient's Privacy?

Table: 1 is a presentation of results of the matrix codding query against hospitals, workers and patients on awareness of e-health patients' privacy.

Table 1: Awareness of e-health Patients' Privacy

Health providers and users' Awareness	Hospital A	Hospital B	Hospital C	Hospital D
Patient's privacy meaning	0	4	5	0
Understanding importance of privacy	9	12	14	2
Unknowingness of policy and regulations	14	21	33	5
E-records abuse and leakages	8	9	11	2

Interviewer: What does patient's privacy mean to you?

R25: Confidentiality of patient information with doctor (Hospital B, Status: Patient)
Interviewer: What does patient's privacy mean to you?

R26: Confidentiality of patient information (R26, Hospital B, Status: Patient)
Interviewer: What does patient's privacy mean to you?

R27: Confidentiality of patient and healthcare provider (R27, Hospital B, Status: Patient)
Interviewer: What does patient's privacy mean to you?

R28: Confidentiality of patient information (R28, Hospital B, Status: Patient).

Figure 2: Meaning of Patient's Privacy

Table 1 shows health providers' and users' awareness sub-themes and their coding references versus the studied hospitals. The table indicates that there were more coding references in unknowingness of policy and regulations across the three Hospitals A, B and C compared to hospitals D.

However, this does not mean that hospital D participants are more aware of policies and regulations protecting patient privacy. The table shows the implication of frequency of the response. The stronger the blue color, the higher the frequency and vice versa.

Patient's Privacy Meaning

The initial question that was asked to the interviewees aimed at establishing their level of understanding of the meaning of patient's privacy in the provision of health services. Nine of eleven interviewed patients expressed what patient privacy meant to them. Six of the nine patients discussed confidentiality when referring to patient privacy. In other words, the study found that respecting someone's privacy and not disclosing personal or potentially sensitive information about them is what

it means to be confidential, especially if that information has been shared in confidence.

Furthermore, three others defined patients' privacy in sharing information with health workers alone. Thus, data must not be availed to unauthorized individuals not involved with the patient's direct well-being, as exhibited in the following excerpt.

In these results, the respondents associated privacy with self-worth and secrecy. They expect that their medical records and data would be handled in a way that preserves their dignity. These results reflect those of Princeton Survey Research Associates for the California Healthcare Foundation (1999) who also found that more Americans trust commercial health insurance plans than they do government-run health programs for medical care since private hospitals maintained more private and confidential patient record systems than public healthcare facilities. The study also discovered that people developed behaviors to safeguard their medical privacy, such as providing only a partial medical history and requesting that a doctor does not record all the information in order to maintain their privacy. In general, the findings indicate that patients and health workers are aware of the meaning of patient's privacy.

Interviewer: What does patient's privacy mean to you?

R10. Patient information to be shared with health specialist only (R10, Hospital C, Status: Patient).

Interviewer: What does patient's privacy mean to you?

R11. Patient information shared with doctor or nurse only (R11, Hospital C, Status: Patients)
Interviewer: What does patient's privacy mean to you?

R12. Privacy of the patient information (R12, Hospital C, Status: Patients)

Figure 3: Meaning of Patient's Privacy

Understanding the Importance of Patient Privacy

Out of 43 interviewees, 31 expressed understanding of the importance of e-health patient privacy issues. However, the understanding of health workers and patients varied. Health workers' understanding involved everyday service provision. First, health workers reported caring for patients during consultation provision. The consultation is offered on a one-to-one basis, meaning that only a doctor and a patient are involved. The one-to-one arrangement, the study found, is designed to protect patients' privacy and health workers perceived the situation as understanding the importance of privacy. In reply to the question, 'to what extent does patients' privacy matter in your daily job activities?' A health worker from Hospital D replied, "To a large extent because the service provided is one to one." This view was echoed by another informant who said, "To a large extent because consultation is done based on one-to-one."

This finding is consistent with the new institutionalism theory by March and Olsen (1989) that institutions such as the studied hospitals tend to have a logic of appropriateness. The logic of appropriateness is seen in that, hospitals establish expected appropriate behavior of individuals and organizations for dealing with patients' privacy. Health workers and their hospitals are expected to conform to established policies, laws, rules, regulations and norms. In this case, appropriateness means conforming to the one-to-one arrangement during consultation with patients. The one-to-one arrangement during consultation with patients is about abiding with the institutional guidelines and practices for safeguarding privacy. This accords with the earlier observations by Adjerid et al. (2011) which showed that in telemedicine, the challenge was maintaining patients' privacy.

In addition, the one-to-one consultation signals institutions' understanding of patient's privacy which ensures that patients' privacy is protected. Privacy encourages patients to express themselves more freely and relaxed in the consultation room. If the doctor seeks to understand the client's privacy, it will motivate the patients to talk in the hope that whatever they say will remain confidential between the two parties. In responding to the question, 'to what extent is patient privacy important'? a study participant from Hospital A responded by saying: "It

is important because believing the health worker will make the patients express freely." Another interviewee from Hospital B stated, "to a large extent, because it is the key of work." These responses confirm what Pritts (2008), found about how the American society placed high value in individual privacy. Therefore, observing privacy during the consultation becomes a norm that health workers must comply with.

Vu et.al (2021) found that in Vietnam individuals or organizations processing personal data are not allowed to share to a third party the data they have collected unless with the consent of the data subject or with special request from competent state agencies. Health workers, this study found, understand that privacy is the right of the patients. Privacy must be protected during the provision of the services. When asked 'what are the advantages of patient privacy'? A typical response from a health worker from Hospital A was, "it is the right of the patient." A similar response from Hospital C was, "it is the responsibility of the doctor to protect the patient's privacy." In this sense, service providers are actually expected to behave in certain standards and acceptable ways. This is established in the minds of both providers and patients.

Other responses indicated understanding the significance of protecting privacy, particularly in the digital era where information can be quickly shared. For instance, a respondent from Hospital C said, "It is important because, in this digital era, information spreads quickly." Princeton Survey Research Associates for the California Healthcare Foundation (1999) showed that major threats to privacy are electronic piracy, medical personnel who disclose personal information or authorized users. Additionally, they discovered that the transition from paper to electronic recordkeeping makes it harder to protect the privacy of personal information and medical records. This differs from the findings presented here where it was found that health workers understand the importance of privacy in the same digital era. It is worth to note that results indicate that health workers are aware of the importance of patient privacy and recognize that it is the patient's right and the workers' primary duty to make sure that they protect it.

This study further found that health workers consider patient privacy to be very important as it reduces societal stigma and humiliation. As such, breaching a patient's privacy can affect the person and the institution. The patient can be humiliated because of the illness. People can stigmatize the patient after knowing about their sickness. To illustrate, a study participant from Hospital C said, "It reduces stereotype." The question was: 'Is patients' privacy important'? A doctor from Hospital C replied, "Yes, because you never know the impact of leakage of patient information." Another similar response from a doctor in Hospital C was, "Sickness is stressing, so it depends on patients' perceptions." This finding is in line with the theory of March and Olsen in 1989 that institutions, such as the hospitals shape the actions of individuals. In this finding, therefore, health workers feelings and behaviors are shaped by the institutional norms, values and regulations. The shaping has influenced them to see how violating and breaching patients' privacy can affect their wellbeing in the society.

Findings from this study show that health institutions contribute in making their members feel responsible in observing the appropriate actions that safeguard patients' privacy. The findings similarly support earlier studies which found that the use of regulations, laws and ethics helped in shaping how heath workers felt when dealing with e-records. For example, George and Bhila (2019) reported that breaching patient's privacy resulted into big problems. They came to the conclusion that integrity ought to be the main strategy for achieving positive outcomes in the privacy protection of patients. This is confirmed, for example, in the response that says it is the responsibility of the doctor to ensure patient's privacy. Likewise, Vu et.al (2021) found that heath workers who failed to protect privacy encountered administrative fines. It can therefore be concluded from these findings that health workers and patients are aware of the importance of protecting patients' privacy and realize that breaching privacy can have ill effect on the person

In addition, six out of eleven interviewed patients reported that privacy was important to them and they connected privacy with confidentiality. The study found that privacy referred to keeping patients' information secret. In the digital era, the study found that patients worried that information could be shared easily with unauthorized persons without protecting privacy. In responding to a question, 'Is privacy important?' Patients' replies are exhibited in figure 5.

Research Question 2: Are the Respondents Familiar with Existing Policies and Regulations?

Out of 43 interviewed participants, 32 expressed unknowingness of policies and regulations regarding protecting the patient's privacy. Out of the 32 participants, 24 were health workers and others were patients. Typical responses from the health workers were as in figure 4.

However, not everybody agreed with the responses. Four health workers reported being aware of the policies and regulations regarding the issue of patients' privacy. For example, in responding to the question, 'Are you familiar with any policy or guideline for guiding the protection of patients' privacy?' An Assistant Nursing Officer from Hospital B replied, "Yes, Hospital B policy provides quality patient services." A similar response from a health worker (doctor) from Hospital A was, "Yes, civil law: to disclose patients' information without the patient's consent is not allowed." The responses indicate discrepancy among the health workers about their awareness of the policies and regulations protecting patients' privacy. However, it is explicitly clear that the awareness of the policies is poor. Some health workers confuse policies with the professional ethics of conduct studied in colleges which is more emphasized by the learning institutions. A similar response from a patient from Hospital C was, "I believe because they have professional ethics and responsibility to protect patients' privacy."

Interviewer: Are you familiar with any policy or guideline for guiding protection of patients' privacy?

R22: NO

Interviewer: Why are the policies or guidelines for guiding protection of patients' privacy not familiar?

Interviewer: Are you familiar with any policy or guideline for guiding protection of patients' privacy?

R17: No, we use the ethics learnt at school (R17, Hospital A, Status: Worker, Department: Unit in charge, Education: Diploma, Position: Unit in charge).

Figure 4: Unknowingness of Policies and Regulation

It was noted that policies and regulations' awareness is taken for granted by the hospital management and the ministry responsible for health services in Tanzania. Hospital management was found to be not making efforts to ensure that the available policies and regulations are known to the health workers. Therefore, policies are available but frontline employees are unaware of such policies. In responding to a question about why policies or guidelines for guiding the protection of patients' privacy are not known, a doctor from Hospital C responded, "It is not a priority of the ministry of health." Yet, not all respondents agreed on the responses. Other participants thought that it was the laziness of the health workers. Health workers are not trying to read and be familiar with the available policies. For example, an Assistant Nursing Officer from Hospital B said, "Laziness of workers because policies are available but they are not reading."

Patients also showed a high level of unknowingness of existing policies or regulations safeguarding patient privacy. A patient from Hospital B said, "I don't know if there are any policies." A similar response was from a hospital A patient who said, "No, but I think there are regulations or policies like security and confidentiality of patient's information."

Some additional general questions were asked to check how quickly health workers would refer to policies and regulations as the framework guiding their handling of patients' data. Health workers (doctors, nurses and lab specialists) were found to be more aware of and quicker to refer to their professional, ethical codes of conduct than policies and regulations laid down by the government. Thematic analysis found that doctors insisted on observing ethics in protecting confidentiality than on understanding the policies and regulations.

A Health Records Officer from Hospital A, when asked 'how do you maintain patient's privacy in using files?' replied: "The required staff only can access files and they have professional ethics." Thus, workers insist on ethics when dealing with patient records in manual systems and e-records. For

example, ethics significantly influenced the behavior of officers in sharing patients' records with health insurance companies. In response to a question on whether sharing information with insurance could affect patients' privacy, one doctor from hospital A replied, "Not at all because those working at insurance are doctors guided by ethics." In responding to a question about challenges faced in protecting patient's privacy, a doctor from Hospital C replied, "some doctors ignore their ethics," The responses indicate that doctors use their professional ethics to guide their medical practices in handling patients' privacy. The results also show that a code of ethics is more familiar to them than talking about issues relating to laws, policies and regulations.

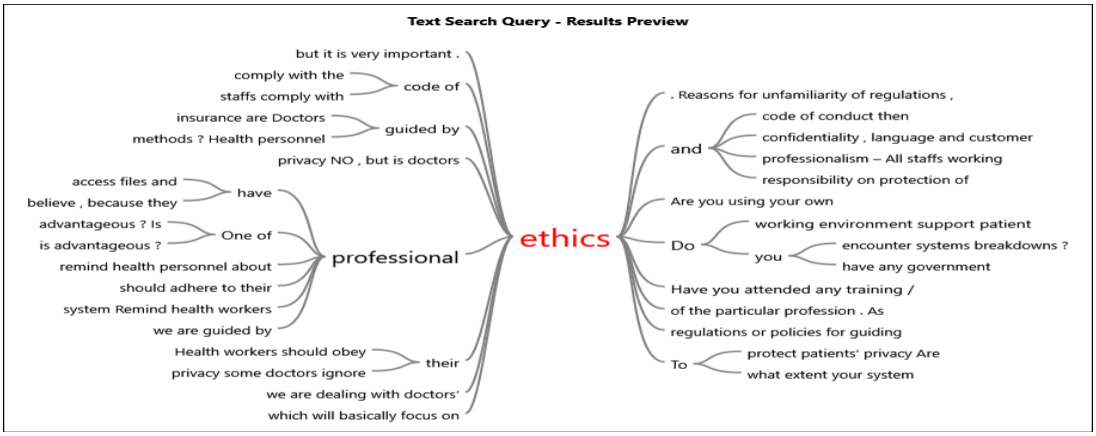

Figure 5: Text search Query-Word tree for ethics

Figure 5 shows a result of a text search quality for ethics. The diagram indicates how the word ethics was used in the context of safeguarding patients' privacy. The word tree shows how respondents kept making reference to the health services code of ethics for the providers of the service. Each time the question demanded on the use of regulations and policies, these respondents thought of code of ethics. These results show that the code of ethics occupies a more significant portion of these respondents' knowledge base. The most conspicuous institution for these respondents is the code of ethics. They refer less to other institutions like regulations and policies.

Conclusions and Recommendations

This study set out to explore the extent to which hospital workers and patients are aware of the importance of patients' privacy especially in the age of digital data. It also set out to assess the extent to which they are aware of existing institutions meant to guide and regulate the daily work of e – health service providers in Tanzania. Whereas most of the respondents were found to be well aware of the importance of patients' privacy, the existing laws, policies and regulations guiding the handling of patients' data to ensure privacy, are not well known to both health workers and patients. Because of high level of unknowingness among both health providers and patients, health service providers and patients refer to medical ethical codes of conduct as the source of their confidence in the work of health providers. So, existing institutions meant to guide the work of health service providers in Tanzania are not being used effectively due to lack of awareness of their existence.

It is therefore recommended that health workers have the duty to inform themselves of the existing government institutions meant to guide and regulate their work. It is crucial for health providers to know and use these existing regulatory institutions because of two reasons. One is that the institutions are laid down to guide their work and it is therefore their duty to know and use them. The intention of the government is to protect individual rights to privacy. This objective cannot be realized if the intended users of the institutions are not aware of their existence. Second, it is the right of the patient to have their privacy properly protected under an institutional framework backed by government authority. Accompanying this right, however, is the duty of every patient to make effort to familiarize themselves with the existing regulations meant to protect their privacy.

References

Adjerid, I., Acquisti, A., Padman., R., Telang., R. & Adler-Milstei, J. (2011). Impact of Health Disclosure Laws on Health Information Exchanges. Draft paper for WEIS.

Ama-Amadasun, M. (2016). Patients' Privacy Rights Protection: A survey of healthcare centres from a Swiss perspective. Faculty of Business and Management, UGSM- Monarch Business School, Switzerland.

Anifalaje, A. A. (2012). Exploring the Role of Health Management Information Systems in Improving Accountability Arrangements for Primary Health Care Delivery in Less Developed Countries: A Case of Northern Nigeria (PhD Thesis). London School of Economics.

Bowman, D. (2011). Panel: HIEs Will Be a Major Privacy Concern in 2011. Available Online at: https://www.fiercehealthcare.com/ehr/panel-hies-will-be-a-major-privacy-concern-2011.

Chinyemba, A. (2011). Fostering Transparency, Good Governance and Accountability in Institutions of Higher Learning Through Records Management. Paper read at the XXI Bi-Annual East and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) General Conference on "Access to Information: Archives and Records in Support of Public Sector Reform in Context", Maputo, Mozambique, 6-10 June 2011.

George, J., & Bhila, T. (2019). Security, Confidentiality and Privacy in Health of Healthcare Data. International Journal of Trend in Scientific Research and Development 3(4), 373-377.

Hamad, W.B. (2019). Current Position and Challenges of E-Health in Tanzania: A Review of Literature. Global Scientific Journal, 7(9), 364-376.

Healy, J. (2008). Implementing e-Health in Developing Countries: Guidance and Principles. International Telecommunication Union (ITU), Geneva.

Kajirunga, A., & Kalegele, K. (2015). Analysis of Activities and Operations in the Current E-Health Landscape in Tanzania: Focus on Interoperability and Collaboration. International Journal of Computer Science and Information Security,13 (6), 49 – 54.

Keshta, I & Odeh, A. (2020). Security and Privacy of Electronic Health Records: Concerns and Challenges. Egyptian Informatics Journal, Available online at: https://doi.org/10.1016/j.eij.2020.07.003.

Kruse, C.S., Smith, B., Vanderlinden, H &Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of Medical System, 41: 127.

March, J. G., & Olsen, J. P. (1989). Rediscovering Institutions. New York: Free Press.

March, J. G., & Olsen, J. P. (1994). The logic of appropriateness. ARENA Working Papers, WP 04/09. Centre for European Studies, University of Oslo.

March, J. G. and H. A. Simon 1958. Organizations. New York: Wiley. 2nd ed 1993. Oxford: Blackwell Publishers.

Martinez, S., Sanchez, D &Valls, A. (2013). A Semantic Framework to Protect the Privacy of Electronic Health Records with Non-Numerical Attributes. Journal of Biomedical Informatics, 46, 294-303**.**

Mashoka, R.J., Murray, B., George, U., Lobue, N., Mfinanga, J., Sawe, H. & White, L. (2019). Implementation of Electronic Medical Records at an Emergency Medicine Department in Tanzania: The Information Technology Perspective. African Journal of Emergency Medicine, 9, 165-171.

Msumi, M. M. (2018). An Overview of eHealth Regulations in Tanzania. Datenschutz Und Datensicherheit - DuD, 42(6), 373–375. https://doi.org/10.1007/s11623-018-0959-4.

Obuaku-Igwe, C. (2021). The Effectiveness of E-Health Services: Evidence from Mom-Connect in South Africa. Academia Letters, 577, 1-5.

OECD (2015) Health data governance: Privacy, monitoring and research. OECD Publishing, Paris.

Peter, H. (2010). Ensuring trust in e-Health through Strong health data protection. Journal of the American Medical Informatics, 303, 18-40.

Princeton Survey Research Associates. (1999). Attitudes and Opinions of Turkish People about Privacy and Confidentiality of Health Information in Electronic Environment. Princeton Survey Research Associates for California Healthcare Foundation. Retrieved on 01 May 2023, http://www.chcf.org/media/press-releases/1999/americans-worry-about-the-privacy-of-their-computerized-medical-records.

Pritts, J. (2008). The importance and value of health information: Roles of HIPAA Privacy Rule and the Common Rule in health research.

Rezaeibagha, F. (2013). Privacy and Data Security of Electronic Patient Records (EPR) Sharing: Case Studies: Iran and Sweden. Master of Science in Information Security. Luleå University of Technology, Sweden.

URT (2013). Tanzania National eHealth Strategy June, 2013 - July 2018. The United Republic of Tanzania (URT), Ministry of Health and Social Welfare.

URT (2016). National Information and Communications Technology Policy 2016. Implementation Strategy 2016/17-2020/21. The United Republic of Tanzania (URT), Ministry of Works, Transport and Communication.

URT (2019). Digital Health Strategy July 2019 – June 2024. The United Republic of Tanzania, Ministry of Health, Community Development, Gender, Elderly and Children.

Vu,Y. Han, E., Tran, T., & Nguyen, K. (2021). Navigating Data Privacy Issues (Part 2). Article in 'Mondaq: Connecting Knowledge and People'. Accessed at: https://www.mondaq.com/privacy-protection/1091628/navigating-data-privacy-issues-part-2, on 16th May 2023.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods. 6th Edition. Sage Publications, Inc. London, United Kingdom.

Weingast, B. (1996). Institutional Theory. In R. E. Goodin (Eds.), (1996), A New handbook of Political Science, Oxford: Oxford University Press.