GSAR Journal of Applied Medical Sciences ISSN: 2584-2323 (Online)

GSAR Journal of Applied Medical Sciences
ISSN: 2584-2323 (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/gsarjams-home/

e-HEALTH PRIVACY: QUEST FOR SAFEGUARDING PATIENT'S DATA IN TANZANIA

BY

Mbiki Mkude Msumi

Head of Department (Public Law) and Lecturer, Faculty of Law, The Open University of Tanzania. A highly accomplished Lawyer & Legal Scholar. 10 plus experience in case assessment & analysis, strategy, negotiations, and public speaking.

Article History

Received: 15/08/2024
Accepted: 21/08/2024
Published: 23/08/2024

Vol – 1 Issue – 8

PP: -01-11

Abstract

This paper sought to establish the awareness of the importance of patient privacy and safeguarding personal data in the realm of electronically generated health records. It aims at ensuring that health data is kept private and only accessible to authorized individuals who can view or modify sensitive health information and to explore the legislative framework that governs the management and safeguarding of patient information. The paper established that even though some legislative frameworks and policies regulate the relationship between patients and medical practitioners. No policy or Legislation in place that regulates electronically generated healthy data. It is revealed that there exist problems of inadequate storage of patient records, which leads to the possibility of access to patient records, which may lead to the violation of patient privacy and confidentiality. It presents strategies for mitigating risks from e-health technologies and reviews accountability mechanisms in Tanzania.

KEYWORDS: e-Health, Patient's data, Privacy, Electronic Health Records (HER), Data protection

1. Introduction

Data protection is crucial in safeguarding individuals' privacy, especially in today's digital age where vast amounts of personal information are collected, stored, and processed by various entities. This is especially important as the global economy is moving towards digital where various data are shared electronically including personal health-related data. In this context, it is important patient's data be protected under e health. Hence, the right to privacy lies directly at the centre of data protection and, therefore, a proper understanding and safeguarding of data protection in the digital age may be fulfilled only by properly understanding the right to privacy.

The e-Health can be best described as "the use of social software to promote collaboration between patients, their caregivers, medical professionals, and other stakeholders in health through the reliance and use of technology.[1] The e-Health innovations are critical for providing healthcare services across Tanzania, creating significant risks to users' online privacy. Information shared in e-health applications includes some of the most intimate and sensitive details about someone's life or health status.[2] Beyond mere embarrassment, privacy breaches can also inflict great harm, with direct consequences for employment, insurance coverage, and physical safety. However, e-health, based on information and communication technologies, raises legal concerns about privacy capacity for professionals, service providers, and patients.[3]

Initially, e-Health data were developed and used at several academic inpatient and outpatient medical facilities.[4] None contained all the information in the paper chart, and most e-health data today are still a cross-collection of computerized and paper data.[5] Some e-Health data developed between 1971 and 1992 were developed with hierarchical or relational databases around or added to hospital billing and scheduling systems, while others were developed as clinical systems to help improve medical care and for use in medical research.[6]

In the late 1980s and early 1990s, hardware became more affordable, powerful, and compact. Using personal computers, local area networks, and the Internet provided faster and easier access to medical information and initiated web-based

[1] Ibid
[2] Ibid

[3] *Sittig DF, Ash J editors. Clinical information systems: Overcoming adverse consequences. Sudbury, Mass.: Jones and Bartlett; 2011.*
[4] *Weed L.L., "The Problem Oriented Record as A Basic Tool in Medical Education, Patient Care and Clinical Research". Ann Clin Res 1971. June;3(3): pp. 131-4.*
[5] *Institute of Medicine. The Computer-based Patient Record: An Essential Technology for Health Care. Revised Edition. Dick RS, Steen EB, Detmer DE, editors. Washington, DC: National Academy Press; 1997*
[6] *Pryor T.A., (et al) "The HELP system". J Med Syst 1983. April;7(2): pp 87-102.*

*Corresponding Author: **Mbiki Mkude Msumi.**

e-health data.[7] Early use of e-Health also included data interchange for claims processing and image scanning as a method for document capture.[8] These efforts saved time by eliminating filing and retrieving charts, photocopying, and chart location control.[9] More clinical use began when the physician workstation became the term for personal computers integrated with e-Health data that allowed access to physician notes, orders, consults, laboratory results, radiological studies, direct patient measurements, nursing assessments and notes, and patient care procedures. Workstations interfaced with tools such as drug references, clinical manuals, textbooks of medicine, literature search engines, and electronic communication.[10]

While some e-Health data were developed on minicomputers, most were initially developed on large mainframe computers and, in either case, had limited storage, which required the use of removable disk packs or tape for extra data storage, nightly downtimes for database back-up and dedicated/wired terminals. Only a few early e-health data allowed physicians to enter orders, prescriptions, and notes, and data entry was done through keyboards focused primarily on laboratory and medication review.[11] While usually hospital-based, many of the early e-health data had features and functionalities that are still used and important today.

Any information pertaining to a person's health, medical background, and care received is referred to as patient data. This information is essential for medical research, therapy planning, and ailment diagnosis. Patient information may contain contact information, age, gender, and ethnicity. Past medical history, allergies, surgeries, and family medical history.Details regarding past and present medical ailments, ailments treated, drugs taken, and invoices. protocols.Billing details, insurance information, and appointment history. The purpose of safeguarding patient data is to protect the confidentiality, integrity, and availability of patients' personal and medical information. This involves implementing measures to ensure that patient data is not accessed, disclosed, altered, or destroyed by unauthorized individuals or entities. Safeguarding patient data is crucial for maintaining patient trust, complying with legal and regulatory requirements (such as Tanzania Personal Data Protection Act), and ensuring the quality and continuity of care.

Electronic Health Records (EHRs) provide a comprehensive view of a patient's medical history, medications, test results, and other relevant data, enhancing coordination among healthcare providers and reducing the risk of errors. The development of technology, in which communication is improved, has increased the links between patients and doctors in delivering health services worldwide.[12] Accordingly, as technology evolves, the healthcare industry will likely see further integration of digital solutions to improve patient outcomes and streamline healthcare delivery.[13]

The result is an increase in e-Health services where personal data are shared between patients, doctors, and service providers. While these advancements offer numerous benefits, addressing data privacy, security, and regulatory compliance challenges is crucial to ensure the ethical and responsible use of technology in healthcare.

Unlike the traditional approach, the e-Health service provides patients with direct support for disease self-management.[14] The e-Health technologies can save a lot of time and give patients and the public more information about their health. For example, Telemedicine allows patients to consult with healthcare professionals remotely through video calls, phone calls, or secure messaging platforms. This is because the online arena provides rapid and instant data sharing, which involves applications such as Twitter, Facebook, and YouTube, including online websites developed for information sharing and interconnectivity.[15] In addition, ICT integration in healthcare can enhance patient outcomes, increase accessibility to healthcare services, and improve overall healthcare delivery.[16] The e-Health technologies have been indicated as a critical solution to challenges and gaps in delivering quality health care.[17] However, it's essential to consider and address challenges related to data security, privacy, and the digital divide to ensure equitable access to these technologies. Yet, the application of ICT in health delivery systems presents threats to privacy and confidentiality legal rights likely to discriminate and violet protection of patient personal data[18]

Data could also be represented in various graphical formats, which mainly facilitates the management of critically ill patients. While not widespread, new applications and functionalities were being developed and used. For example, physicians began to use electronic documentation, but many

[7] *Salenius SA, (et al. l) "An Electronic Medical Record System With Direct Data-Entry and Research Capabilities." Int J Radiat Oncol, Biol, Phys 1992;24(2):369-76.*
[8] *Ibid.*
[9] *Beeler P.E. (et al. l). "Decision Support Systems." Swiss Med Wkly 2014;144: w14073.*
[10] *Madison L.G., (et al) "Case Study of User Assessment of a Corrections Electronic Health Record. "Perspect Health Info Manage 2011; 8:1b.*
[11] *McDonald C.J., (et al) "The Medical Gopher a Microcomputer System to Help Find, Organize and Decide about Patient Data." Western J Med 1986. December;145(6):823-9.*
[12] *Sittig DF, Ash J editors. Clinical information systems: Overcoming adverse consequences. Sudbury, Mass.: Jones and Bartlett; 2011.*
[13] *Ibid*
[14] *See, for example, Megbowon E, T, "Information and Communication Technology Development and Health Gap Nexus in Africa", Front Public Health. 2023, pg 23*
[15] *Ibid*
[16] *Sittig DF, Ash J editors. Clinical information systems: Overcoming adverse consequences. Sudbury, Mass.: Jones and Bartlett; 2011.*
[17] *Ibid*
[18] *Weed L.L., "The Problem Oriented Record as A Basic Tool in Medical Education, Patient Care and Clinical*

*Corresponding Author: **Mbiki Mkude Msumi.**

did not believe that computerization saved time, although they appreciated its value for administrative functions and for producing printouts.[19]

Networks of microcomputer workstations were used to write all inpatient orders linked to an Electronic Health Record. While this significantly lowered patient charges and hospital costs, the systems required more physician time than the paper charts.[20] Likewise, initial attempts at nurse charting failed because they required time-consuming manual data entry. Automated management of patient records became available by developing patient data management systems, which could be connected to bedside monitoring devices to record and interpret patient data in e-Health.[21]

Some specific areas, including admission, pharmacy, laboratory, surgery, radiology, respiratory therapy, and infectious diseases, were interfaced with or completely developed within e-Health.[22] However, laws still required hospitals and practitioners to be accountable for the accuracy and completeness of medical records, and thus, all documents had to be reviewed and signed.[23] While regulatory and accrediting agencies restricted the auto-authentication of medical records, electronic signatures could and were being used within e-Health.[24]

Numerous privacy and security concerns accompany the increased use of e-health data. A data breach refers to any breach of security that leads to the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.[25] A violation of electronically generated health data could result in several consequences, such as identity theft, fraud, or the public damage of an individual's health information, as well as the release of sensitive information about the health status of the data subject.[26]

Data breaches violate an individual's right to privacy and erode trust in the health care system. As technology evolves and health systems become more complex, the likelihood of data breaches increases. Health systems must invest in information security and data protection to combat this risk. The fast-growing issues facing healthcare delivery services and coverage, privacy, and security of electronically generated health data to the extent that for patients, remain crucial obstacles to the acceptance of the system. Patients, providers, and healthcare facilities continue demanding that these records be securely protected.[27]

Muhimbili National Hospital (MNH), one of the biggest government Hospitals in Tanzania, implemented a computer system in 2004.[28] Implementing a computer system in a hospital in 2004 was a forward-thinking move, especially considering the potential improvements in patient care, record-keeping, and overall efficiency that technology can bring. Various modules of the computer system were designed to suit all departmental operations. The parts successfully implemented during this early stage were the registration and billing modules. The Government introduced the National Health Strategy in 2012[29] and updated it in 2019 to improve ICT. The strategy guides the implementation of digital health initiatives.

Further, the Ministry of Health developed the Tanzanian Health Enterprise Architecture (THEA) to guide the national integrated Health Information System (HIS) development.[30] The THEA is used to design a hospital system called the Electronic Facility Management System (eFMS), which connects all government hospitals in Tanzania, including referral hospitals and government health centres.[31] The eFMS centralizes information from all government hospitals to the Ministry. This means that where the government data of a particular patient is required, it can easily be accessed via the application FMS. The eFMS has improved patient care by enhancing communication between providers and patients. In addition, the health information systems in Tanzania hospitals generally use Information and Communication Technology, the system known as The Government of Tanzania Hospital Management Information System (GoT-HoMIS), which is an electronic information system intended to Collect and report facility-level clinical information (basic patient-level clinical

[19] *Buckley A., "Know Me - A Journey in Creating a Personal Electronic Health Record." Stud Health Technol Inform 2015; 208:93-7.*

[20] *Chen E.S., (et al) "Characterizing the use and contents of free-text family history comments in the Electronic Health Record". AMIA Annu Symp Proc 2012; 2012:85-92.*

[21] *Pathak J, (et al) "Applying semantic web technologies for phenome-wide scan using an electronic health record linked Biobank." J Biomed Semantics 2012;3(1):10.*

[22] *Evans RS, (et al) "Enhanced notification of infusion pump programming errors." Stud Healh Technol Inform 2010;160 (Pt 1):734-8.*

[24] *J, (et al) "A European inventory of common electronic health record data elements for clinical trial feasibility." Trials 2014; 15:18.*

[25] *Nwauche, E.S "The right to Privacy in Nigeria:" Centre for African Legal Studies Publishers, 2007 P. 65*

[26] *Ibid*

[27] *March CA, (et al) "Use of Simulation to Assess Electronic Health Record Safety in the Intensive Care Unit." a pilot study. BMJ Open 2013;3(4).*

[28] *Ramadhan, J. M., (et al), "Implementation of Electronic Medical Records at an Emergency Medicine Department in Tanzania: the Information Technology Perspective", African Journal of Emergency Medicine, Vol 9, 2019*

[29] *Ibid*

[30] *The Ministry of Health and Social Welfare. Tanzania National eHealth Strategy June, 2013– July, 2018. http://www.tzdpg.or.tz/fileadmin/documents/dpg_internal/dpg_working_groups_clusters/cluster_2/health/Ke Sector Documents/Tanzania Key_ Health Documents/Tz_eHealth_Strategy_Final.pdf. (20.05.2024)*

[31] *Ibid*

*Corresponding Author: **Mbiki Mkude Msumi.**

dataset), and Support Health Facilities in service delivery management.[32]

Health information systems are crucial in collecting, managing, and analyzing health data to improve patient care, enhance public health outcomes, and support healthcare management. These systems control information technology to streamline processes, enhance communication, and provide valuable insights. These systems help monitor disease trends, track healthcare service utilization, and support evidence-based decision-making among healthcare practitioners.[33] Generally, the Tanzania Ministry of Health recognizes the importance of ICT in transforming healthcare delivery by enabling information access, data collection, and support of healthcare operations, management, and decision-making.

In addition, ICT provides more information about personal health status, quick and instant data sharing, quick access to medicine, medical consultation, laboratory services, and results. The relationship between doctor and patient is fiduciary. This trust enables patients to disclose personal and sensitive information to doctors or service delivery personnel of the hospital on one hand. On the other hand, doctors are obliged not to disclose all information received during the patient's treatment.

This is because, during treatment, patients share their secrets with hospital personnel, who are very sensitive. If patients' sensitive information is divulged, there is a possibility of not sharing such information in detail on one side. On the other hand, it may attract legal action against service delivery officers. Confidentiality under health services entails that patients' personal and medical information should remain between the patient and specific health service delivery personnel dealing with the cause of treatment. In this context, it is essential for the right to confidentiality should be protected.

2. An overview of Policies related to Protection of Patient Personal Data

Tanzania National Health Policy 2003

The Health policy was introduced in 2003 and serves as a directorial document for the health sector in Tanzania. It includes provisions or guidelines for adopting fast-growing technology and using e-health technologies to improve healthcare delivery services and their consequences. The policy emphasizes delivering equitable and quality healthcare services from the district to the regional level.[34] The policy sets a vision for developing the health sector in Tanzania. The objectives of the health policy are as follows. First, to improve the health and well-being of all Tanzanians and reduce the burden of disease while raising the life expectancy of the people of Tanzania.[35] Second, a comprehensive and integrated approach should improve the health status of all Tanzanians, particularly the vulnerable groups. It emphasizes promoting community-based health care, improving health infrastructure, strengthening the health workforce, and increasing access to essential health services.

The development of national health policies is crucial for poverty eradication and economic growth. It's an investment in the well-being and productivity of the population, which has far-reaching positive effects on a country's overall prosperity. A healthy population is more productive. When people have access to good healthcare, they are less likely to be sick or disabled, which means they can participate more fully in the workforce. This increased productivity contributes to economic growth.[36] The policy is in line with the Government Development Vision of 2025 goals, which strive to raise and improve the health status of all people by ensuring the delivery of effective, efficient, and quality healthcare services.[37]

The policy focused on implementing various health sector reforms to improve the efficiency and effectiveness of service delivery, health financing, and management. The policy made it clear that the Ministry of Health, as a technical Ministry, is responsible for all matters concerning the country's health.[38] Emphasis is placed on strengthening primary health care services as the foundation of the health system. The policy sought to explore and establish sustainable health financing mechanisms to reduce the financial barriers to accessing health services, such as the introduction of the National Health Insurance Fund. The policy focused on strengthening health information systems for better planning, monitoring, and evaluating health programs and outcomes. The policy encouraged collaboration between the public and private sectors to improve the quality and accessibility of health services.

Surprisingly, the existing health policy does not cover e-Health mode of health service delivery. Instead, Tanzania has developed specific e-health strategies to outline the country's approach to accommodating Information Communication Technologies in the health sector.[39] These strategies focus on

[32] *March CA, (et al) "Use of Simulation to Assess Electronic Health Record Safety in the Intensive Care Unit." a pilot study. BMJ Open 2013;3(4).*

[33] *Mashoka R, J., (et al), "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective. Afr J Emerg Med. 2019*

[34] *Section 3.1 National Health Policy, 2003*

[35] *Ibid, Section 2.1*

[36] *Section 1 National Health Policy, 2003*

[37] *Ibid, Section 2*

[38] *Ibid, Section 1.2*

[39] *In 2012, the Ministry, through technical and financial support from RTI International and Centres for Disease Control and Prevention (CDC) under the Monitoring and Evaluation Strengthening Initiative (MESI), reviewed the draft National eHealth Strategy, seeking areas for improvement. The review process also followed a participatory approach driven by HSSP III strategic objectives. The National eHealth Strategy provides an appropriate basis to guide the development of eHealth in Tanzania. It adopts enterprise architecture (EA) - driven development approach to developing eHealth capabilities:*

*Corresponding Author: **Mbiki Mkude Msumi.**

health information exchange, electronic medical records, telemedicine, and health data security. The first is the National Digital Health Strategy 2019–2024. This strategy is in line with the Tanzania Development Vision 2025 goals. The second is the Health Sector Strategic Plan 2015–2020. There are several common gaps and challenges in many existing national health policies and strategies related to electronic health system, one is the inadequate or insufficient application of the policies. The generality of these recommendations might occasionally lead to difficulties or misunderstandings, necessitating the application of medical professionals' judgment and experience in order to handle challenging circumstances.

The Tanzania Information Communication Technology Policy (ICT) 2016

The National ICT Policy of Tanzania is a strategic document that aims to harmonize the potential of information and communications technology to drive socio-economic development, improve service delivery, and enhance the overall well-being of the citizens. The policy outlines various objectives, strategies, and action plans to promote the growth and sustainable development of the ICT sector. The policy focuses on extending the reach of ICT services to all regions, including remote and underserved areas, to bridge the digital divide and ensure that every citizen can benefit from the digital age.[40]

The policy promotes adopting e-government initiatives to improve public service delivery, such as e-health, online platforms for government services, and digital communication between citizens and government agencies.[41] The policy recognizes the importance of skilled human resources and seeks to enhance ICT education and training programs to produce a knowledgeable workforce capable of driving the digital economy.[42] It is in this context that the policy reflects on the use of electronic services to facilitate the provision of social and economic services such as tourism, governance, education, health, finance, and justice, which has significantly increased in recent years, and the industry has witnessed advancement in the area of Information Technology.

Most public institutions have progressively established electronic systems to enhance efficiency and productivity, and advanced technology is taking a good and promising future. Generally, the policy indicates a positive shift towards embracing digital solutions to cater to the needs of citizens and businesses in various sectors. This transition can lead to numerous benefits, such as increased convenience, cost-effectiveness, and improved access to services for a wider population. However, it's also crucial for such developments to be carried out carefully for data protection and privacy to ensure that all individuals can benefit equally from these technological advancements.

The absence of specific legislation directly addressing electronic health data privacy often leads to a reliance on broader constitutional and statutory provisions, along with international agreements, to safeguard privacy. The Constitution of the United Republic of Tanzania, established in 1977, serves as a foundational legal document ensuring various rights, including privacy protection. Additionally, statutory provisions within different laws, though not explicitly targeting electronic health data, contain clauses relevant to privacy, providing some protection for health information.

These frameworks ensure that personal data and privacy in e-Health, among other issues, are well protected. Recognizing the value of personal data in e-health, termed sensitive data, is the cornerstone of the e-health delivery system. This is because the harm that could be caused if, by any chance, such data falls into the hands of the wrong person is likely to cause serious damage to patients and the e-health delivery system.

3. e-Health Legal framework

In Tanzania, health laws regulate privace and confidentiality often predate the advent of e-health services. While these laws might not explicitly mention e-health services, they typically encompass provisions safeguarding patient privacy and confidentiality in various healthcare settings. However, as technology advances and new forms of healthcare delivery, like e-health services, emerge, there is often a need to update and adapt these laws to address the nuances and challenges of digital health platforms.

These laws include the Medical, Dental and Allied Health Professionals Act, 2017; the Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005; Human DNA Regulation Act, 2009; and the HIV and AIDS (Prevention and Control) Act 2008, which contain provisions that regulate medical confidentiality. These regulations set the standards for healthcare professionals in Tanzania to maintain patient confidentiality and privacy. Maintaining patient confidentiality and privacy is paramount for healthcare professionals to uphold ethical standards and comply with legal regulations. Healthcare professionals should only access patient information when it is necessary to provide care or fulfill their job responsibilities. Access to patient records should be limited to those who need the information to perform their duties. Healthcare professionals and staff should receive regular patient confidentiality and privacy policy training. This helps ensure they understand the importance of safeguarding patient information and know the correct procedures. Patient consent should be obtained before sharing information with other healthcare providers or third parties, except when required by law for treatment, payment, or healthcare operations.

Leverage what currently exists in the Tanzanian eHealth landscape. Understand what the new components are and where they fit in existing structures. Define information structures to fit current needs and to support anticipated ones. Demonstrate how technology and resource constraints dictate both what is feasible and the path forward.

[40] *National Information and Communication Policy 2016, p.14.*

[41] *National Information and Communication Policy 2016, p.10.*

[42] *National Information and Communication Policy 2016 p 19.*

*Corresponding Author: **Mbiki Mkude Msumi.**

The Constitution of the United Republic of Tanzania 1977

The Constitution of Tanzania, adopted in 1977, does not have a specific Article that explicitly recognizes the right to personal data privacy. Nevertheless, it contains provisions that could be interpreted as offering some degree of privacy protection. Article 16(1) in particular sets principle that every person has the right to enjoy the protection of the law to enforce their rights and obligations. This provision can be interpreted to include a right to privacy. However, this right is not absolute as it is observed. It requires state authority to lay its legal procedures, circumstances, manner, and extent to which the right of privacy may be infringed upon without prejudice. The Constitution further requires the protection of reputation rights and freedom from non-interference, and it prohibits the disclosure of confidential information, among other things.[43] The court of law has the same opinion on respecting people's privacy as *Jackson Ole Nemeteni and 19 Others v the Attorney General*.[44] The High Court of Tanzania held that in the absence of a procedure prescribed by law, the administration of a provision of any law that seeks to limit an individual's fundamental rights is susceptible to abuse and cannot, therefore, be saved under Article 30(2) of the Constitution.[45]

The Cybercrimes Act 2005

The Cybercrimes Act of 2015 addresses various cyber-related offences, including unauthorized access to computer systems, data interference, computer-related fraud, and cyberbullying. It plays a significant role in deterring privacy breaches and protecting data by establishing legal frameworks and consequences for those who engage in cybercrimes. It aims at creating a safer digital environment and ensure accountability for individuals or entities involved in such offences.[46] There have been not many cases of privacy in the country lately. However, in the case of *Jamii Media Ltd v. Attorney General,*[47] The Court ordered that the Government put in place procedures to be used by the Police when requesting information under the Cybercrimes Act, 2015 instead of relying on the general provisions which may be used to infringe the right to privacy. The court ruled that under section 32 (4) of the Cyber Crime Act, Police are not allowed to take items but to take the evidence needed through a printed form. The court emphasized the importance of the Police seeking the court's intervention in circumstances where the Police failed to secure data or information under the provision.

In this case, the petitioner operated a website that anonymously provided users a platform to post and engage in discussions of social, economic, or political significance. Under the Cybercrimes Act, the Police issued orders demanding the disclosure of information regarding the platform's users, threatening to prosecute the petitioner if they did not comply. The petitioner filed a petition to challenge Sections 32 and 38 of the Cybercrimes Act as unconstitutional for offending Articles 13(6)(a), 16, and 18(1) and (2) of the Constitution. The petitioner contended that Section 32 of the Cybercrimes Act takes away the right to privacy, and Section 38 of the Cybercrimes Act offends the right to be heard. The High Court of Tanzania ('the High Court') held that Section 32 of the Cybercrimes Act was within permissible national and international proportional limits and that it was not unreasonable for people possessing relevant data to disclose to investigators. *Deogras John Marando v Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd,*[48] The respondent used the image of the appellant in company advertisements and for commercial purposes without the appellant's consent.

Although there was no comprehensive law in Tanzania to protect personal image and privacy, the High Court relied upon Article 16 of the Constitution. It drew from common law principles to award general damages in favour of the Appellant. The High Court adopted the following principles in its judgment in this case: there must be an intrusion of personal privacy of the claimant on their identity/image by the respondent, there must be appropriation of the claimant's image or celebrity or likeness for the respondent's advantage in any form but in particular commercial purposes; there must be lack of consent from the claimant; and there must be proof that the respondent earned profit out of the illegal use of the claimant's image.

In the case of *Raymond Paul Kanegene and Bob Chacha Wangwe v The Attorney General,*[49] the petitioner was challenging the constitutionality of sections 16 and 39(2)(a) and (b) of the Cybercrimes Act, which were alleged to violate the right to privacy and the right to freedom of expression under Articles 16 and 18 of the Constitution. Section 16 of the Cybercrimes Act provides that any person who publishes information or data presented in a picture, text, symbol, or any other form in a computer system knowing that such information or data is false, deceptive, misleading, or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or concealing Commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than TZS 5 million (approx. €2,010) or to imprisonment for a term of not less than three years or to both. Concerning Section 39 (2)(a) and (b) of the PDPA, the submissions were based on the argument that the Minister's power to prescribe the procedures requiring service providers to divulge specified information and identify

[43]Ibid, Article 16(3).
[44] Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam(Unreported)
[45]See the case of *Jackson Ole Nemeteni and 19 Others v the Attorney* General Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam(Unreported).
[46] Sections 31, 32, 33, 34, 35 and 37 of The Cyber Crimes Act, 2015.
[47] Miscellaneous Application No.9 of 2016, High Court of Tanzania at Dar es Salaam.
[48] High Court of Tanzania, Civil Appeal No 110 of 2018 (unreported).
[49] High Court of Tanzania, Consolidated Misc. Civil Cause No. 15 OF 2019 & No. 5 OF 2020.

*Corresponding Author: **Mbiki Mkude Msumi.**

service recipients interferes with the right to privacy and private communication under Article 16(1) of the Constitution, and the right to freedom of opinion and expression, the right to seek, receive and disseminate information and ideas without restrictions as provided under Article 18 of the Constitution. It was argued that service providers should not be compelled to give information without the consent of the person who issued such information.

The High Court held that a statutory provision's constitutionality is not determined by what could happen in its operation but by what it provides for and that the mere possibility of a statutory provision being abused in actual operation will not make it invalid as a matter of general rule. On that ground, the petition was dismissed, and it was held that the impugned provisions do not violate the constitutional provisions.

In *Kisonga Ahmed Issa & Another v Republic, Court of Appeal of Tanzania, Consolidated*,[50] In Francis Nyandindi v Republic, High Court of Tanzania (at Dar es Salaam), Article 16 of the Constitution was used to refuse admissibility of evidence of a questioned statement during a criminal investigation on the ground that the statement recorded the statement of the accused. At the same time, their privacy rights were being violated.

The Act plays a critical role in enhancing the protection of patient data by establishing a legal framework to combat cybercrimes, including those that target sensitive health information. This legislation typically includes provisions to prevent unauthorized access, data breaches, and misuse of personal health data, thereby ensuring that healthcare providers implement robust security measures. The Act also often stipulates severe penalties for violations, serving as a deterrent against potential cyber threats. Ultimately, the Cybercrimes Act strengthens the overall integrity and confidentiality of patient data, promoting trust in digital healthcare systems and safeguarding patient privacy.

Tanzania Personal Data Protection Act 2022 (TPDPA)

The Tanzania Personal Data Protection Act (TPDPA), which came into force in 2022, marks a significant step in safeguarding individuals' data across all sectors of the country. The primary objective of this Act is to establish a comprehensive framework that outlines the principles and minimum standards for collecting and processing personal data.[51] This means that in any non-union matter, this law shall not apply. By setting minimum requirements for collecting and processing personal data, the TPDPA aims to ensure that public and private entities handling such data adhere to specific standards. This helps prevent misuse, unauthorized access, or unauthorized sharing of personal information.

The Act outlines key principles for protecting personal data, such as data minimization (collecting only necessary data), purpose limitation (using data only for intended purposes), accuracy, storage limitations, integrity, and confidentiality.[52] Under these principles, fair, lawful, and transparent data is understood in the rational collection and processing of personal information. Data processing should be conducted in a manner that is fair and transparent to the individual whose data is being collected and processed. This means that individuals should be informed about the purposes for which their data will be used and clearly understand how it will be handled. Transparency is key to building trust with data subjects and ensures that they have control over their personal information. In data processing, stakeholders can be broadly categorized into two main roles: controllers and processors. In general, these principles ensure that personal data is handled responsibly and ethically.

The data controller is the entity that determines the purposes and means of processing personal data, while the data processor processes the data on behalf of the data controller. This is well articulated under Part IV of the Act. This entails the provision of the identity of the controller or processor, laying down the purpose of the collection, ascertaining persons to whom data will be disclosed, and specifying whether the supply of information is intentional or mandatory.[53] This means that data processing must be carried out in compliance with applicable laws and regulations. In this context, the organizations collecting and processing personal data must have a legitimate basis for doing so. Hence, it must adhere to the legal requirements, such as obtaining explicit consent from the data subject when necessary or having another lawful basis for processing, like fulfilling a contract, complying with a legal obligation, protecting vital interests, performing a task in the public interest, or pursuing legitimate interests where those interests do not override the individual's rights and freedoms.

In collecting personal data, the law requires the controller to give certain information to the subject at the time of data collection, identifying him or her and stating the purpose of such data collection, of which the collection shall not be unlawful.[54] In addition, personal data collected shall only be used for the intended purpose and not otherwise unless the data subject agrees to the use of data collected for the purpose not intended.[55]Data should be collected for a specific, clear, and legitimate purpose. This purpose should be communicated to the individuals from the data collected.

In many jurisdictions, Tanzania being one, data protection laws allow exemptions or exclusions for data processing for personal or household activities. These exemptions are often designed to prevent overly burdensome regulations on individuals using data for everyday, non-commercial

[50] *Criminal Appeal No. 17 of 2016 and 362 of 2017.*
[51] Long title of Personal Data Protection Act 2022
[52]
[53] Ibid, section 22
[54] Ibid, Section 23 (2)
[55] Ibid, Section 25(1)

*Corresponding Author: **Mbiki Mkude Msumi.**

purposes.[56]The law further requires the data controller or data processor to collect data directly from the data subject.[57] However, without consent, personal data cannot be processed.[58] Personal data can be processed without consent if they are publicly available in situations where noncompliance is necessary as a requirement of other written laws or in cases where the data controller has legal obligations and is subject to protecting the vital interest of the data subject, for the administration of justice, or in the public interest.[59]It's generally considered good data management practice for a data controller to only retain data for as long as it is necessary and relevant for the purpose for which it was collected. The Act require organizations only to collect and retain data that is strictly necessary for the purpose for which it was collected and for a specific period unless agreed otherwise with the data subject.[60]The longer data is held, the greater the risk of a data breach or unauthorized access. Storing unnecessary data increases the surface area for potential security incidents. It's also essential to have mechanisms to periodically review and delete data that is no longer needed. This can be done through regular audits and assessments of the organization's data.

Unlike other data, the law requires that in processing sensitive data, there must be written consent from the data subject.[61] The provision clearly states that no sensitive personal data shall be processed unless the data subject has given written consent to processing such data. Even where the data subject has given consent to process personal data, the law gives the subject the right to withdraw their consent at any time during the processing without explaining why they are withdrawing their consent.[62] In the context of PDPA, sensitive data include data concerning health.[63] There are exceptions to this rule that sensitive data shall not apply, where the Minister responsible may determine the situations where they cannot be removed even with the data subject's request to remove certain data. This can be in circumstances where the processing of such data requires fulfillment in certain written laws or before the court of law for certain trials.[64] Again, in the situation where processing is necessary for purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with his employment, to protect the vital interests of the data subject or another person where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; to protect the vital interests of another person, in case where consent by or on behalf of the data subject has been unreasonably withheld, under all these situations the Minister responsible may intervene if need to do so.

Further circumstances apply where processing is carried out by any entity or association that exists for political, ethical, religious, or employment union purposes during its appropriate activities. The processing is carried out for scientific research per the specific guidelines. It relates only to individuals who are placed under the supervision of health professionals; such data may be collected for medical reasons in the interest of the data subject without jeopardizing his interests.[65]

The Act states that personal data should be collected for specified, explicit, and legitimate purposes, and the data should not be further processed in a manner incompatible with those original purposes.[66] In simpler terms, it means that when an organization collects personal data from individuals, it should be clear and transparent about the reasons for collecting it. The data should only be used for those specific purposes, and any subsequent use or processing of the data should be consistent with the original intent and within the bounds of the law. This principle prohibits the consistent and arbitrary collection of information about people without having a thorough, clear, and genuine purpose. Data controllers can only process personal information against the purpose for which they registered.[67] This is whether you use and disclose the data in a way that those who supplied the information would expect it to be used and disclosed. For example, personal information can be transmitted to the controller's agents who carry out data operations on behalf of such controllers and do not recall it for their purposes. Suppose an organization wishes to use the data for a new or different purpose that was not originally communicated to the data subjects. In that case, they will need to seek additional consent from the individuals or find another lawful basis for the new processing.

The Act further requires that personal data be adequate, relevant, and not excessive concerning the purpose for which they are processed.[68] The focus is ensuring organizations collect and process only the minimum personal data required to achieve their legitimate objectives. By adhering to this provision, organizations can limit privacy risks and ensure that individuals' data is handled responsibly and with respect for their privacy rights.

There are, however, some unclear provisionswith regard to protection of dpatient data. For example, the Act prohibits the processing of personal data for direct commercial advertising purposes.[69] Despite the prohibition, it remains unclear whether the section data handlers can trade the personal data of their data subjects. The Act also falls short regarding the security breach notification front. Procedures for handling data breaches ought to be outlined in the Data Protection Regulation to compel data handlers to give data subjects

[56] Section 25(2) of the PDPA
[57] Ibid, Section 23(1)
[58] Ibid, Section 23(3)
[59] Ibid, Section 29(1)
[60] Ibid, Section 28 (1) and (2)
[61] Ibid, Section 30(1)
[62]Ibid, Section 30(2)
[63]Ibid, Section 3
[64]Ibid, Section 30(3)
[65] Section 30(5) of Tanzania Personal Data Protection Act, 2022
[66]
[67] Ibid Section 14 (1), (2)
[68] Ibid Section 5(c)
[69] Ibid Section 35

*Corresponding Author: **Mbiki Mkude Msumi.**

advance notice of any security breaches involving their personal information, its effects, and the remedial action taken. The obligation for data breach notification would be significantly strengthened by a directive for data processors and collectors to notify affected subjects within a stipulated time of becoming aware of data breaches.

In addition, provisions regulating data transfer is opaque regarding data subjects' consent to bodies that collect, process, store, or use personal data outside Tanzania's borders. As data subjects have not been accorded the "power of consent," their data may be prone to misuse. For example, the Act gives full legal rights to an heir apparent, meaning they could consent to process private information on behalf of any other party incapable of such consent.[70] It, however, lacks a legal interpretation rationale, as it does not spell out which "party" is alive, incapacitated, or deceased. This section may be prone to abuse, as an heir may not meet the legal threshold to consent on behalf of someone else due to reasons such as being underage, coercion, or other technicalities.

Generally, the TPDPA appears to be a comprehensive legal framework designed to modernize data protection practices in Tanzania, aligning with international standards such as the GDPR. The protection of patient data within the e-Health domain is of paramount importance, given the sensitive nature of medical information and the increasing reliance on digital platforms for healthcare delivery. Ensuring strong data protection measures is not just a regulatory requirement but also a fundamental ethical obligation to maintain patient trust and ensure the integrity of the healthcare system.

4. The shortcomings.

The shortcomings of the laws governing e-Health patient data are a critical concern for the healthcare industry, policymakers, and patients. Many laws governing e-health data were created before the advent of modern digital health technologies and do not adequately address contemporary issues such as artificial intelligence (AI) and machine learning in healthcare. The pace of legislative updates is slow compared to the rapid evolution of technology, resulting in outdated regulations that do not address current risks and opportunities.

Different regions and countries have distinct regulations, leading to inconsistencies in how patient data is handled. This fragmentation complicates cross-border healthcare and data sharing. Existing laws often fail to provide adequate protection against data breaches and cyber-attacks, leaving patient data vulnerable. Patients may not have a clear understanding or control over how their data is used, as consent processes are often complex and not user-friendly. The study further reveal the issue of data ownership ambiguities, there is often confusion and ambiguity regarding who owns patient data, patients, healthcare providers, or third-party service providers. For example, among the laws discussed in this article, there is no express provision on e-Health data ownership and whether individuals whose information has been released have any power over it once it is under the control of third parties or at the risk of any danger. There is also no provision for the situation when such data has been transferred to a certain destination outside Tanzania. For research purposes, what will the fate of a data subject be? Neither is it clear when an individual has the right to demand their personal e-health information be deleted from the records of the parties who collected it, even if this is for legitimate reasons. It's important to note that while ICT development can bring about positive changes, challenges such as infrastructure gaps, affordability, digital literacy, and cybersecurity must be addressed to ensure that the benefits are accessible to most citizens, including those in underserved and marginalized communities.

Implementing electronic healthcare service delivery requires significant changes in workflows and processes, and some healthcare professionals may resist adopting new technologies. Overcoming resistance to change and ensuring proper training are essential for successful integration. Another challenge is the lack of ICT skills for many healthcare professionals, training on the proper use of e-Health technologies, and data protection's importance. Such skills may lead to accidental data breaches or other compliance issues.

5. Conclusion and recommendation

The study noted that while e-Health technologies are applied differently in many nations, they all have the ability to support patients' privacy and health while also giving therapy and tracking advancement. The author's primary issue is how to better secure patient privacy and data, as well as how to make e-Health technology easier to use in Tanzania. The privacy implications of e-health technology advancements are contingent upon several contextual circumstances, including national health legislation, healthcare finance situations, and healthcare institutions.

Improving the laws governing e-Health patient data is indeed crucial for enhancing patient privacy, security, and trust in digital healthcare systems. There is a need to implement comprehensive data protection laws that specifically address e-Health data, ensuring all personal health information is protected. The need to ensure that patients have explicit control over their data, with clear, informed consent required for data collection, use, and sharing. The government to instruct healthcare providers and digital health companies to be transparent about how patient data is collected, used, stored, and shared. Development of strong data governance policies that define roles, responsibilities, and processes for managing patient data. The government need to have in place accountability mechanisms to ensure that organizations and individuals handling patient data are held responsible for any misuse or breaches. Provide regular training for healthcare professionals on data protection, privacy, and security best practices. Conduct awareness campaigns to educate patients about their rights regarding their health data and how to protect their privacy online. Educating patients and communities about the benefits and proper use of e-Health

[70] Ibid Section 34 (4).

*Corresponding Author: **Mbiki Mkude Msumi.**

services can drive participation and engagement. A legal framework governing health data collection, storage, and use is essential for successfully implementing e-Health in Tanzania. The framework should ensure that the privacy and confidentiality of patient's health information are well protected. Developing and implementing e-Health solutions requires following national and international regulations, standards, and guidelines. Legal frameworks for data protection, telemedicine, and electronic health records should be established or updated to accommodate the digital healthcare landscape.

Access to high-speed and reliable internet is crucial for e-Health initiatives. It enables healthcare providers to access and share EHRs, telemedicine services, and other health-related information. In rural or remote areas, where internet infrastructure might be lacking, efforts should be made to expand coverage through various means like satellite connections, mobile networks, or community Wi-Fi initiatives. Developing or adopting suitable software solutions is essential. These software solutions must be user-friendly, secure, and compliant with global privacy regulations.

The success of e-Health in Tanzania depends on the readiness and willingness of healthcare providers and patients to use the technology. It is essential to provide training and education to healthcare providers and patients on the benefits and use of e-Health. Health professionals need intensive training in data processing so they will be in a good position to advise patients on protecting and using their medical records. Healthcare providers and stakeholders must implement proper security measures and adhere to established guidelines and standards for electronic health record management. It is also essential to provide adequate training and support to healthcare providers and users to ensure that they are proficient in using the technology and aware of potential risks and how to mitigate them.

Many e-Health technologies are involved in collecting and transmitting sensitive patient data. Policies must address privacy and security concerns to protect patient information. Balancing data access for healthcare providers while safeguarding patient privacy is a delicate task. There is a need for e-Health policy that is appreciated to enable and facilitate patient mobility, licensing agreements, and data sharing. Regulation of personal data privacy in public and private sectors must be strong and comprehensive to safeguard people’s right to privacy. Data privacy legislation must be visionary and not reactionary. Legislators must keep up with modern society by enacting legislation that anticipates future innovations, thus being useful for the long term. E-Health policy should be developed as tools and guidelines to allow developing countries to adopt reforms and create a database of e-Health national laws.

The digital age has highlighted the need for robust protection of e-Health patient data, highlighting the growing concern of vulnerabilities in electronic health records (EHRs), necessitating a comprehensive approach that includes technology, policy, and education.

In conclusion, protecting patient data stored in electronic health records is a continual process that calls for cooperation and constant work. Through the use of cutting-edge technology, strict adherence to regulations, and the promotion of awareness and education, the healthcare industry can greatly improve patient data privacy, which will eventually raise trust and improve healthcare outcomes.

REFERENCES

1. Ailey D, (et al.). "Systematic review of evidence for the benefits of telemedicine", J Telemed Telecare. 2002
2. Bowman S. Impact of electronic health record systems on information integrity: quality and safety implications. Perspective Health Information Management 2013
3. Buckley A, Fox S. Know me - a journey in creating a personal electronic health record. Stud Health Technol Inform 2015
4. Chen ES, Melton GB, Burdick TE, Rosenau PT, Sarkar IN. Characterizing the use and contents of free-text family history comments in the Electronic Health Record. AMIA Annu Symp Proc 2012
5. Elrod J, Androwich IM. Applying human factors analysis to the design of the electronic health record. Stud Health Technol Inform 2009
6. Evans RS, Carlson R, Johnson KV, Palmer BK, Lloyd JF. Enhanced notification of infusion pump programming errors. Student Health Technological Information 2010
7. HIV Legal Network. "Halt the Harm: Ending and Avoiding Criminalization of HIV, COVID-19, and Other Public Health Challenges in Canada." Policy Brief, 2022
8. https://www.osha.go.tz/about-us?language=eng accessed 30/9/2023
9. Institute of Medicine. The Computer-based Patient Record: An Essential Technology for Health Care. Revised Edition. Dick RS, Steen EB, Detmer DE, editors. Washington, DC: National Academy Press; 1997
10. Madison LG, Phillip WR. A case study of user assessment of a corrections electronic health record. Perspect Health Inf Manag 2011
11. March CA, Steiger D, Scholl G, Mohan V, Hersh WR, Gold JA. Use of simulation to assess electronic health record safety in the intensive care unit: a pilot study. BMJ Open 2013
12. Mashoka R, J, (et al), "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective. Afr J Emerg Med. 2019
13. Megbowon E, T, "Information and communication technology development and health gap nexus in Africa", Front Public Health. 2023
14. Ministry of Health and Social Welfare. Tanzania National eHealth Strategy June 2013– July 2018.http://www.tzdpg.or.tz/fileadmin/documents/d

*Corresponding Author: **Mbiki Mkude Msumi.**

pg_internal/dpg_working_groups_clusters/cluster_2/health/Ke Sector Documents/Tanzania Key_ Health Documents/Tz_eHealth_Strategy_Final.pdf.
15. Nwauche, E.S The right to Privacy in Nigeria: Centre for African Legal Studies Publishers, 2007
16. Pathak J, Kiefer RC, Bielinski SJ, Chute CG. Applying semantic web technologies for phenome-wide scan using an electronic health record linked Biobank. J Biomed Semantics 2012
17. Pryor TA, Gardner RM, Clayton PD, Warner HR. The HELP system. J Med Syst 1983. April
18. Ramadhan, J. M., (et al.), "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective", African Journal of Emergency Medicine, Vol 9, 2019
19. Salenius SA, Margolese-Malin L, Tepper JE, Rosenman J, Varia M, Hodge L. An electronic medical record system with direct data-entry and research capabilities. Int J Radiat Oncol, Biol, Phys 1992
20. Sinda, A., & Kamuzora, F., Privacy and Data Protection in Tanzania: found in https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania, 2018 (accessed on 19 October 20023 at 12:48)
21. Specthrie L, Berg W, Fishman S, Walker L, Gapay L. Power to the portables. Health Information 1992. August

*Corresponding Author: **Mbiki Mkude Msumi.**