

**PROTECTION OF PERSONAL DATA IN e-HEALTH: A COMPARATIVE
PERSPECTIVE BETWEEN TANZANIA AND GERMANY**

MBIKI MKUDE MSUMI

**A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY IN LAWS
DEPARTMENT OF PUBLIC LAW
THE OPEN UNIVERSITY OF TANZANIA**

2024

CERTIFICATION

The undersigned certify that they have read and hereby recommend for acceptance by the Open University of Tanzania a thesis entitled; **“Protection of Personal Data in e-Health: A Comparative Perspective Between Tanzania and Germany”**, in fulfilment of the requirements for the award of a Degree of Doctor of Philosophy (PhD) of the Open University of Tanzania.

.....

Prof. Alex Boniface Makulilo
(1st Supervisor)

.....

Date

.....

Dr. Hellen Kiunsi
(2nd Supervisor)

.....

Date

COPYRIGHT

No any part of this thesis shall by any means be reproduced, stored in any retrieval system or transmitted in any form being, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the author or the Open University of Tanzania on that behalf.

DECLARATION

I, **Mbiki Mkude Msumi**, declare that the work presented in this thesis is original. It has never been presented to any other University or institution. Where other people's works have been used, references have been provided. It is in this regard that I declare this work as originally mine. It is hereby presented in fulfilment of the requirement for the Degree of Doctor of Philosophy (PhD) Law of the Open University of Tanzania.

.....

Signature

.....

Date

DEDICATION

To my lovely daughter, Filsan Hussein.

ACKNOWLEDGEMENT

I glorify your name, Father Lord, for this journey.

I am most grateful to my supervisor, Professor. Dr. Alex B. Makulilo and Dr. Helen Kiunsi for their support, guidance, and encouragement. It was a huge honour and pleasure to learn from them. I wish to thank my family for their love and never-ending belief in me, sometimes against impossible chances.

In particular, I wish to thank my Mother, Zebina Msumi, for her solid confidence in me and for being my greatest inspiration.

My darling daughter, Filsan, thank you for your devotion and patience.

I wish to convey a special word of thanks to the entire staff at the Faculty of Law, particularly my departmental members at the Open University of Tanzania. God bless you abundantly.

ABSTRACT

This doctrinal and comparative legal research investigates the legal implications of processing personal data in Tanzania's electronic healthcare services (e-Health). The study provides insight into the privacy of health records in the legal and regulatory framework for protecting patients' health records in Tanzania's e-Health systems by using the German legal and regulatory framework as a model for legislative reforms. This study establishes that Tanzania does not have a harmonized and specific law governing electronically generated health data. The available Data Protection Regulation does not guarantee personal data protection under e-Health systems. The problem emanates from existing health policy, on the one hand, and the legislator's failure to address legal challenges caused by the application of technology in protecting patients' information in the e-Healthcare delivery system, on the other. Therefore, the study urges the Government of Tanzania to adopt harmonized laws to protect patients' privacy under the e-Health delivery system by using the German framework as a benchmark.

Keywords: *Privacy and confidentiality, patients' information, patients' personal data protection, electronically generated health data.*

TABLE OF CONTENTS

CERTIFICATION	ii
COPYRIGHT	iii
DECLARATION	iv
DEDICATION	v
ACKNOWLEDGEMENT	vi
ABSTRACT	vii
LIST OF DOMESTIC LEGAL INSTRUMENTS	xiii
INTERNATIONAL, REGIONAL AND SUB-REGIONAL LEGAL INSTRUMENTS	xiv
LIST OF CASES	xvi
CHAPTER ONE	1
GENERAL INTRODUCTION	1
1.1 Background to the Problem	1
1.2 Background to the Problem	1
1.3 Statement of the Problem	10
1.4 Research Objectives	12
1.4.1 General Objective	13
1.4.2 Specific Objective	13
1.5 Research Questions	13
1.6 Literature Review	14
1.7 Research	25
1.7.1 Doctrinal Legal Research	25
1.7.2 Comparative Legal Research	28

1.8	Ethical Consideration	29
1.9	Significance of Study	29
1.10	1.9 Scope of Study	31
1.11	Limitation of Study	32
CHAPTER TWO		33
CONCEPTS AND THEORIES OF PERSONAL DATA PROTECTION		
IN e-HEALTH		33
2.1	Introduction	33
2.1.1	Personal Data.....	33
2.1.2	Privacy.....	40
2.1.3	e-Health Data Privacy	51
2.2	Theories Underlying Personal Data Protection in e-Health	55
2.2.1	Non-intrusion Theory	56
2.2.2	Seclusion Theory of Privacy	60
2.2.3	Control and Limitation Theories of Privacy	63
2.2.4	The Restricted Access/Limited Control Theory (RALC)	67
2.3	Conclusion.....	76
CHAPTER THREE		78
LEGAL AND POLICY FRAMEWORK ON e-HEALTH PERSONAL DATA		
PROTECTION.....		78
3.1	Introduction	78
3.2	International Legal and Policy Framework	80
3.2.1	The Universal Declaration of Human Rights, 1948 (Hard Law)	81

3.2.2	The International Covenant on Civil and Political Rights (ICCPR), 1966. (Hard Law)	82
3.2.3	The UN Convention for the Protection of Individuals with Regards to Automatic Proccesing of Personal Data of 2018 (Hard Law).....	84
3.2.4	WHO Declaration on the Promotion of Patient Rights in Europe of 1994. (Hard Law)	86
3.2.5	Right to Privacy in the Digital Age (GA Res. 71/199) (Soft Law).....	86
3.2.6	General Assembly Resolution 45/95 and Guidelines for the Regulation of Computerized Personal Data Files of 1990 (Soft Law)	87
3.2.7	OECD Guidelines on the Protection of the Privacy and Transboundary Flaws of Personal Data RE 2013. (Soft Law)	89
3.2.8	UN System of Privacy and Data Protection in the e-Health Subsector.....	90
3.3	e-Health Personal Data Protection under Regional Instruments.	92
3.3.1	The Convention 108+ of the Council of Europe, 2018	92
3.3.2	EU Data Protection Directive 95/46/EC	96
3.3.3	EU's Medical Device Directive (93/42/EEC).....	99
3.3.4	The European Convention on Human Rights (ECHR), 1953	101
3.3.5	The European Union Data Protection Regulation (EU) 2016/679 (GDPR).....	106
3.3.6	European Data Protection Commission, 2018	109
3.3.7	The Council of Europe in Development of Right to Privacy and Personal Data Protection.....	111
3.3.8	The African Charter on Human and Peoples' Rights, 1981.....	112

3.3.9	African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)	114
3.3.10	African Declaration on Internet Rights and Freedoms, 2014.....	119
3.4	e-Health Personal Data Protection under Subregional Instruments.	122
3.4.1	e-Health Personal Data Protection under East African Community (EAC)	122
3.4.2	e-Health Personal Data Protection under SADC.....	124
3.4.3	e-Health Personal Data Protection under ECOWAS	127
3.5	Foreign Practice from other Jurisdictions	131
3.6	Conclusion.....	132
CHAPTER FOUR.....		134
PROTECTION OF PERSONAL DATA IN e-HEALTH IN GERMANY		134
4.1	Introduction	134
4.2	The Context of Germany in the e-Health System	134
4.3	e-Health Card System.....	141
4.4	Legal and Regulatory Framework in Germany	143
4.4.1	Europe	143
4.4.2	General Law	147
4.4.3	Specific Legislation.....	158
4.5	Personal Data Protection Institutions in Germany	168
4.6	Conclusion.....	172
CHAPTER FIVE.....		175
PROTECTION OF PERSONAL DATA IN e-HEALTH IN TANZANIA.....		175
5.1	Introduction	175

5.2	The Context of Tanzania in e-Health System	176
5.3	Analysis of the Country's Policy Framework on the Health Sector	180
5.3.1	Tanzania National Health Policy, 2003.....	180
5.3.2	The Tanzania Information Communication Technology Policy (ICT) 2016.....	184
5.4	Legal and Regulatory Framework for Personal Data Protection in e-Health	188
5.4.1	General Domestic Law on Privacy and Personal Data Protection on e-Health	188
5.5	Conclusion.....	210
CHAPTER SIX		212
SUMMARY OF RESEARCH FINDINGS, RECOMMENDATIONS AND CONCLUSION		212
6.1	Summary of Research Finding	212
6.2	Conclusion.....	217
6.3	Recommendations	219
6.3.1	Recommendations on the Law Reforms	219
6.3.2	Recommendations on Institutional Reforms	222
6.3.3	Recommendations on Policy Reforms	223
6.3.4	Recommendations to Future Legal Researchers.....	224
6.3.5	Other Recommendations	224
BIBLIOGRAPHY		228
APPENDICES		235

LIST OF DOMESTIC LEGAL INSTRUMENTS

The Constitution of the United Republic of Tanzania, 1977 (RE 2008)

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

The HIV and AIDS (Prevention and Control) Act, 2008

The Human DNA Regulation Act, 2009

The Medical Laboratory and Technicians Act, 2019

The Medical, Dental and Allied Health Professionals Act, 2017

The National Strategy on e-Health in Tanzania, 2019-2024

The Pharmacy Act, 2011

The Tanzania Communications Regulatory Authority Act, Cap.172 RE 2002

The Tanzania Information Communication Technology Policy (ICT), 2016

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

The Tanzania National Health Policy, 2003

The Tanzania Personal Data Protection Act, 2022

INTERNATIONAL, REGIONAL AND SUB-REGIONAL LEGAL INSTRUMENTS

International Instruments.

The General Assembly Resolution 45/95 and Guidelines for the Regulation of Computerized Personal Data Files, 1990

The International Covenant on Civil and Political Rights, 1966

The OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980 (RE 2013)

The UN Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981

The UN Right to Privacy in the Digital Age (GA Res. 71/199)

The UNAIDS, Considerations and Guidance for Countries Adopting National Health Identifiers, June 2014

The United Nations Guiding Principles on Business and Human Rights, 2011

The Universal Declaration of Human Rights, 1948

The World Health Organization Declaration on the Promotion of Patients' Rights in Europe, 1994

Regional Instruments

The African Charter on Human and Peoples' Rights, 1981

The African Union Convention on Cyber Security and Personal Data Protection, 2014

The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Directive 97/66/EC of 15 December 1997 concerning the processing of personal

data and the protection of privacy in the telecommunications sector

The EU Convention of the Council of Europe, 2018

The EU General Data Protection Regulation, 2018

The Medical Device Directive (Council Directive 93/42/EEC of 14 June 1993)

Sub Regional Instruments

The East Africa Legal Framework for Cyber laws, 2011

The SADC Model Law on Computer Crime and Cybercrime 2012.

The SADC Model Law on Data Protection 2012.

The SADC Model Law on Electronic Transactions and Electronic Commerce 2012.

The Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS
2010.

The Treaty for Establishment of the East African Community, 1999

LIST OF CASES

Data Protection Commissioner v. Facebook Ireland and Maximillian Schemes (Schemes II), ECLI:EU: C:2020:559, 16 July 2020

Eisenstadt v. Baird.: 405 U.S. 438 (1972)

Federal Constitution Court of German (FCC) –BverfG, 1 BvR 16/13 (2018)

Jamii Media Company Ltd v. The Attorney General (2017) TLS LR 447.

Katz v. United States, 389 US 347 (1967)

Olmstead v. US 1928. 277 US 438ff

The German Patient Data Protection Act, 2020

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Problem

This chapter acts as the foundational ground for the whole research study. This chapter provided the basic elements that acted as the guiding maps on how the study was to be conducted. Therefore, the chapter *inter alia* shall provide: the Background of the problem of the research study; the statement of the problem of the research study; the objectives of the research study; the literature review and the methodology.

1.2 Background to the Problem

Generally, the evolution of policies, laws, and institutions governing personal data in the health sector in Tanzania reflects a dynamic process shaped by historical legacies, socio-economic conditions, and ongoing efforts to promote health and development. During the colonial period, Tanzania was under German and then British rule. The primary focus of health policies and regulations was often on maintaining the health of colonial administrators, settlers, and military personnel rather than on the general population. Limited attention was given to the protection of personal data in healthcare, and the collection and use of health information were likely under the control of colonial authorities with little consideration for individual privacy rights.

Tanzania gained independence from Britain in 1961 under the leadership of Mwalimu Julius Kambarage Nyerere. During this period, there was a gradual shift towards self-governance and the establishment of indigenous institutions. The newly independent

government began to prioritize national development, including improvements in healthcare infrastructure and services. However, the focus on personal data protection may have been limited during this initial phase of nation-building. Following the formation of the United Republic of Tanzania in 1964 through the union of Tanganyika and Zanzibar, there were efforts to consolidate governance structures and develop national policies across various sectors, including healthcare. For instance, Tanzania Health Policy of 1990 that aimed to provide comprehensive healthcare services to all citizens and emphasized the importance of health information systems.

In 1967, there was a dramatic change in political and economic changes, whereby Tanzania adopted the socialist ideology, in which all major means of production were state-controlled.¹ Consequently, health service delivery was also under the control of the public sector. This situation persisted for three decades. The social economy changed following the global liberalization policy in which Tanzania embarked on the economic recovery program and liberalised its economy in 1986.²³ As a result of the adoption of the Zanzibar resolution , new policies and laws were formulated to facilitate the private health sector and health insurance policies.⁴ The introduction of private health services indeed broadens the landscape of health care delivery by expanding beyond public sectors to include private sectors, mission hospitals/health centres which have co-existed with state facilities for ages.

The increased competition has driven providers to enhance their services and quality

¹ This was the implementation of Arusha Declaration of 1967.

²Kiunsi, H., "Transfer Pricing in East Africa: Tanzania and Kenya in Comparative Perspective", ["eprint_fieldopt_thesis_type_phd" not defined] thesis, The Open University of Tanzania, 2017, Pg 228.

³ United republic of Tanzania Investment Promotion Policy, Dar Es- Salaam, Government Printers, 1990.

⁴ United republic of Tanzania Investment Promotion Policy, Dar Es- Salaam, Government Printers, 1990.

of care to attract patients on one side. Conversely, by diverting some patients to the private sector, public healthcare systems experience reduced strain, potentially leading to better efficiency and improved services for those who rely on the public sector. In this context, Tanzania introduced a National Health Policy⁵ to take on board changes in health delivery services. However, the policy is silent on electronically generated health-related data. Despite broadening healthcare delivery services, public and private healthcare delivery sectors still use the traditional physical approach of medical practitioners and patients.

It is important to note that the liberalization of the economy led to the introduction of ICT, which enhances communication. The development of ICT has had a significant impact on traditional healthcare delivery services, particularly in terms of the physical approach and barriers to service delivery. Unlike the traditional approach, the e-Health service provides patients with direct support for disease self-management.⁶ The e-Health technologies can save time and give patients and the public more information about their health. This is because the online arena provides quick and instant data sharing, which involves applications like Twitter, Facebook, YouTube, and online websites developed for information sharing and interconnectivity.⁷ 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.

Like many other countries, Tanzania has applied ICT in e-Health in healthcare

⁵ 2003.

⁶ Megbowon E, T, "Information and communication technology development and health gap nexus in Africa", Front Public Health. 2023.

⁷ Ibid.

delivery, management, and decision-making processes. The purpose is to connect health services to improve healthcare quality and efficiency. For example, Muhimbili National Hospital (MNH) introduced the implementation of a computer system in 2004.⁸ 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.

To impress ICT, the National Health Strategy of 2019.⁹ The strategy is meant to guide the implementation of digital health initiatives. In this context, the Emergency Medicine Department at Muhimbili National Hospital (MNH) installed and implemented the first Electronic Medical Records (EMR) in 2015.¹⁰ The EMR focused on patient registration and billing for emergency centres used only. In implementing ICT facilities, the MNH management invested in training several staff members on using the new information technology system introduced at the hospital. The trained staff took charge while training new staff, who were taught basic computer skills and emergency department-specific tasks.¹¹

The EMR system aims to improve patient safety and healthcare quality and transform the healthcare industry. Health information technology leads to more efficient, safer, and higher-quality care.¹² This is because the EMR systems store and process various

⁸ Ramadhan, J. M., (et all), "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective", *African Journal of Emergency Medicine*, Vol 9, 2019.

⁹ Ibid.

¹⁰ Ibid.

¹¹ Kiunsi, H., "Transfer Pricing in East Africa: Tanzania and Kenya in Comparative Perspective", ["eprint_fieldopt_thesis_type_phd" not defined] thesis, The Open University of Tanzania, 2017.

¹² Joel S. M., (et all), "Assessing Electronic Medical Record System Implementation at Kilimanjaro Christian Medical Center, Tanzania", *Journal of Health Informatics in Developing Countries*, Vol 12, 2018.

types of clinical, administrative, and financial data about patients.¹³ In addition, the EMR enables healthcare providers to store, manage, and retrieve patient information electronically. Furthermore, it coordinates the retrieval of patient records from multiple health facilities, thus providing vital historical medical information for medical decision-making.

Consequently, several healthcare facilities in Tanzania, including hospitals and clinics, have adopted EMR systems from paper-based records to digital formats.¹⁴ This means that electronic health information management system positively affects healthcare. In this context, digitizing medical records improves efficiency, accessibility, and patient care. This is because adopting and using the EMR leads to major healthcare savings, reduces medical errors, and improves the quality of healthcare delivery. Apart from EMR via computers, Mobile phone usage has become widespread, even in remote areas. The availability of mobile phones created opportunities for mobile health (mHealth) interventions, such as SMS and mobile apps, to deliver healthcare information, appointment reminders, and disease management support.¹⁵

The development of health information technology, in general, and electronic health records, in particular, has brought enormous changes in health delivery worldwide.¹⁶

¹³ Ben-, Z., "Critical Success Factors for Adoption of Electronic Health Record Systems: Literature Review and Prescriptive Analysis". Information System Management. 2014.

¹⁴ Ben-, M., "The impact of EHR and HIE on reducing avoidable admissions: Controlling main differential diagnoses", BMC Med Inform Decision Making, 2013.

¹⁵ Gonçalves-Bradley DC, J., et al., "Mobile technologies to support healthcare provider to healthcare provider communication and management of care". Cochrane Database System Rev. 2020: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7437392> accessed 29/09/2023.

¹⁶ Verhenneman, G and Dumortier, J., 'Legal Regulation of Health Records: A Comparative Analysis of Europe and the US' in George, C et al., eHealth: Legal, Ethical and Governance Challenges, Springer, Heidelberg/New York/Dordrecht/London, 2013, pp.25-56, at p.25.

Globally, information and communication technologies are increasingly integrated with providing and managing healthcare and medical services, known as e-Health.¹⁷ According to the World Health Organization (WHO), an e-Health system securely uses information and communications technologies to support health and health-related fields, including healthcare services, health surveillance, health literature, health education, knowledge, and research.¹⁸ The e-Health may take various forms, such as mHealth, which entails health delivered through mobile technology), or telehealth, which entails providing health services at a distance, to mention a few. These forms of e-Health have improved the quality, efficiency, and access to health services globally, albeit their different level of development.

In general, e-Health is beneficial and effective in disease management as it provides direct support.¹⁹ This is because online platforms such as Twitter, Facebook, YouTube and many other websites offer quick and instant data sharing effective information, and interconnectivity.²⁰ As a result, e-Health provides more information about their health quickly. Scholars pose that the e-Health integrated e-healthcare system is cross-institutional, cooperative with the stakeholders in healthcare, and interlinks patients with physicians, dentists, hospitals, pharmacies, and health insurance funds.²¹ Even though e-Health is evolving in developing countries, empirical evidence shows that

¹⁷ George, C *et al.*, *eHealth: Legal, Ethical and Governance Challenges*, Springer, Heidelberg/New York/Dordrecht/London, 2013, vii.

¹⁸ Verhenneman, G and Dumortier, J., 'Legal Regulation of Health Records: A Comparative Analysis of Europe and the US' in George, C *et al.*, *eHealth: Legal, Ethical and Governance Challenges*, Springer, Heidelberg/New York/Dordrecht/London, 2013 <https://www.google.com/search?client=firefox-b-d&q=eHealth+meaning> (accessed 8 April 2023)

¹⁹ Hyppönen, H., "Towards a Joint View of the European eHealth Priorities," *SWOT Analysis of Patient Empowerment and Patient Summary activities in Europe. Reports*, vol. 15, 2008, p. 2008.

²⁰ Available at <http://www.merriam-webster.com/> accessed on 16 October 2020 at 17:09.

²¹ *Ibid.*

few e-Health projects in African countries offer an opportunity for people living in underserved and rural areas to obtain improved healthcare services.²² The low level of e-Health adoption in African countries is due to several factors, including limited technology penetration. Nonetheless, mobile technology has profoundly affected the delivery of e-Health in Africa.²³

In Tanzania, e-Health has been very beneficial as public and private hospitals and health centres use e-Health delivery systems. During the COVID-19 pandemic, for example, Telemedicine was widely adopted to enable virtual consultations between patients and healthcare providers, reducing the need for physical visits to clinics and hospitals. Studies have shown that Telemedicine can be as effective as in-person consultations for many conditions and improve access to care for patients who may face barriers to in-person visits.²⁴ Again health apps were used to provide patients with information and support for managing chronic conditions such as diabetes and hypertension. This was achieved by using some apps to provide personalized diet and exercise plans, track medication schedules, and remind patients to take their medications.²⁵ As a result, using health apps improved patient engagement and self-management, leading to better health outcomes.

With the increased efficiency and acceleration of information transfer between

²² Khalifehsoltani, S.N and Gerami, M.R., 'E-Health challenges, opportunities and experiences of developing countries', International Conference on e-Education, e-Business, e-Management and e-Learning, 2010.

²³ Kaplan, W.A., 'Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?' Globalization and Health, 2006, Vol.2, No.9 2006, pp.1-14.

²⁴ Chilunjika, S.R.T. and Chilunjika., "A Embracing e-health systems in managing the COVID 19 pandemic in Sub-Saharan Africa." Social Sciences and Humanities Open, 2023, Vol. 8(1).

²⁵ Ibid.

information technology networks, the barriers to prompt and reliable information exchanges, including health information and medical imagery, have been greatly eased. People can access information faster and more easily than was previously possible. The value of e-Health lies not in the communication technology but in the ability to share medical information and expertise with others.²⁶ In the process, all relevant information about a patient is stored in the computer system of the medical practitioner and other related parties, known as electronic health records (EHRs), for record and reference purposes.

EHRs are comprehensive digital patient records that carry or are linked with other health-related data. As a result, the collection, use, and storage of medical information in the computerized system facilitate easy access for further use and reference. Consequently, most health information management systems share data from many sources within or among organizations. Sharing health and medical information has brought challenges in protecting personal data and subjecting patients to risk their health if such information is used contrary to intended objectives. There have been numerous cases of data breaches and infringement of data in e-health globally. For example, Life Labs, Canada's largest medical laboratory, suffered a data breach in 2019 that exposed the personal information of 15 million customers. The stolen data included names, addresses, dates of birth, and lab test results.²⁷

²⁶ O'Donoghue, J., Herbert, J., "Data Management within mHealth Environments: Patient Sensors, Mobile Devices, and Databases." *Journal of Data and Information Quality*. 4: 5. October 2012. Available at <https://doi.org/10.1145/2378016.2378021>. Retrieved on 15 October 2020 at 13:53.

²⁷ Motti, V.G., Berkovsky, S. (2022). Healthcare Privacy. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds) *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham. https://doi.org/10.1007/978-3-030-82786-1_10.

In Tanzania, e-Health faces various challenges, hindering its widespread adoption and efficiency. Limited access to stable internet connections and electricity in remote areas impedes the implementation of e-Health services. Another challenge is the inadequate training among healthcare workers in utilizing e-Health tools and technologies, which significantly restrains their effective implementation and usage. There is also a problem of insufficient funding and budget allocated for e-Health initiatives, which in most cases hinders the development and maintenance of digital health infrastructure. Several concerns about data privacy and security recently posed significant challenges to its acceptance. Inadequate measures to safeguard patient data from cyber threats and breaches undermine trust in e-Health systems. There is also the absence or inadequacy of clear regulatory frameworks and policies regarding e-Health practices, which might lead to legal and ethical dilemmas, affecting the adoption and development of these technologies.

The phenomenon must be regulated to avoid any risks likely to arise from e-Health transactions and to take full advantage of e-Health. In this context, Data protection regulations are enshrined in international and domestic laws. Despite its many advantages, the e-Health industry in developing countries, particularly Africa, is much less established and regulated than in the developed world like Germany, where e-Health is well established and regulated. However, in relative terms, India and South Africa illustrate developing countries with better legal systems that regulate e-

Health.²⁸ Many developing countries do not have legislation that generally or specifically regulates e-Health, Tanzania being one of them.

The absence of specific legislation is counterproductive to adopting a robust e-Health system and makes individuals concerned about their personal information's privacy, integrity, and confidentiality. This is perhaps because health information is highly confidential and sensitive data. Moreover, unlike paper-based records, personal information held in digital format is highly vulnerable to loss and theft. Therefore, the study explores how best e-Health data can be protected in Tanzania in light of Germany's e-Health legal framework.

1.3 Statement of the Problem

Indeed, the development of information technology has brought significant and transformative changes to the traditional ways of health service delivery. These advancements have revolutionized how healthcare is accessed, delivered, and managed, improving patient care, greater efficiency, and enhanced collaboration among healthcare professionals. One of the most significant advancements is transitioning from paper-based medical records to electronic health records. EHRs enable healthcare providers to access patient information in real-time, facilitating better care coordination, reducing errors, and improving patient safety.

Information technology has facilitated telemedicine's rise, allowing patients to receive

²⁸ Implementing e-Health in Developing Countries: Guidance and Principles of 2008.

medical consultations, diagnosis, and treatment remotely through video conferencing and other digital communication tools. This has proven especially valuable in reaching patients in remote or underserved areas and during emergencies or pandemics. e-Health services, which involve using electronic technologies to deliver healthcare services and share personal data between patients, doctors, and service providers who become the third party to the information and not the party to the contract, bring several challenges related to data privacy, security, and ethical considerations. e-Health services often deal with sensitive personal health information.

Despite efforts to embrace ICT for health services, Tanzania faces challenges in implementing the e-Health delivery system. These challenges include low computer skills among personnel, insufficient ICT infrastructure, and the widespread use of paper-based systems across hospitals and mostly in rural areas.²⁹ Indeed, access to and privacy of health-related information related to healthcare service delivery is a critical issue in healthcare systems worldwide, particularly in Tanzania. Electronic healthcare service delivery, or e-Health or telehealth, holds great potential for improving healthcare accessibility, efficiency, and patient outcomes. However, e-Health delivery service has challenges. One of the most critical challenges is ensuring the confidentiality and security of patient data. Healthcare data is sensitive and subject to strict privacy regulations. A breach in security could lead to serious consequences, including identity theft and compromised patient care.

A doubt arises when there is a lack of harmonized regulations related to e-Health

²⁹ Hamad, W., 'CURRENT Position and Challenges of e-Health in Tanzania: A review of literature Master of Science in Information System', 2019.

implementation. Various authorities have set these laws and guidelines on general healthcare delivery services but not on electronically generated health-related data. This lack of harmonization can confuse healthcare providers, patients, and other stakeholders, such as service providers who are data controllers. Existing laws may not adequately address the complexities of e-Health technologies and their specific challenges. Traditional healthcare regulations might not cover telemedicine, health apps, and remote patient monitoring issues. The absence of protection for patients' personal information may endanger e-Health delivery services and place patients' character at risk. Personal data protection regulations are vital for the implementation of e-Health delivery services.

Therefore, in addressing the problem of the absence of a comprehensive legislation and regulations regarding e-Health Data Protection in protecting patient privacy in Tanzania, the researcher undertook a comparative analysis on the law and practice in Tanzania to the foreign jurisdiction of Germany in regarding to the protection of e-Health Personal Data Protection. The researcher aimed at drawing lessons from Germany that may be instrumental in the framing of a comprehensive legal framework in the United Republic of Tanzania on matters regarding e-Health Personal Data Protection.

1.4 Research Objectives

The researcher was dully guided by two objectives, general objective and the specific objectives in the course of conducting this research study.

1.4.1 General Objective

The general objective of the study was establishing a comparative legal analysis on the e-Health Personal Data Protection within the jurisdictions of the United Republic of Tanzania and Germany so as to come up with a common ground to the development of the law on the above sector in Tanzania.

1.4.2 Specific Objective

The researcher was guided by the following specific objectives of the study;

- i) To analyse the German legal framework on e-Health Personal Data Protection.
- ii) To analyse the Tanzania legal framework on e-Health Personal Data Protection.
- iii) To make a comparative legal analysis on the legal framework from the jurisdictions of the United Republic of Tanzania and Germany.

1.5 Research Questions

The researcher was confined into answering the belowforth questions.

- i) How do Germany's laws governing e-Health and privacy strike a balance between facilitating advancements in healthcare technology and protecting individuals' privacy rights?
- ii) How do Tanzanian Laws governing e-Health and privacy strike a balance between facilitating advancements in healthcare technology and protecting individuals' privacy rights?
- iii) How do Tanzania's laws on eHealth and privacy compare and contrast with those of Germany, and what implications do these differences have for the protection of individuals' privacy in the context of electronic health data?

1.6 Literature Review

The topic of data protection in disclosing e-Health is written from the perspectives of scholars from developed and developing countries. The study reviews the following literature to provide insight and understanding of e-Health personal data protection with a view of a demonstration of the research gap.

Makulilo provides a comprehensive state of the literature on data protection in Africa for a decade from 2001 to 2012.³⁰ The author discusses data protection in general from an African perspective. However, a clear focus on e-Health is missing in this literature.³¹ The author reviews the state of research and literature on privacy and data protection across Africa for over two decades since 2000, immediately before the first data privacy law policy was adopted in Cape Verde. In this article, Makulilo covers studies in data privacy law in general.

Ndabambi, *et al.*,³² examine the challenges faced by healthcare professionals in Botswana in managing patient records in a way that ensures privacy and confidentiality. The scholars further investigate the extent to which the legislative framework that governs the management of patients' information can protect the privacy and confidentiality of patients' records. Even though some laws and policies regulate the patient and medical practitioner relationship (such as the Botswana Health

³⁰ Makulilo, A.B., 'Privacy and Data Protection in Africa: A State of the Art', International Data Privacy Law, 2012, Vol. 2, No. 3, pp. 163-178.

³¹ Makulilo, A.B., *Twenty-Two Years of Scholarly Research on Data Privacy in Africa: Content and Trend Analysis*, article manuscript2022, (on file with the author).

³² Ndabambi (et al), "Privacy and Confidentiality in the Management of Patient Records at the Princess Marina Hospital, Botswana", European Journal of Academic Research :2014, Vol 2

Professions Act of 2001, Nurses and Midwives Act of 1995, and the Public Service Act of 2008), there were no policies in place to regulate the management of patient records in Botswana. The authors conclude that inadequate patient record storage, access, and security may violate patient privacy and confidentiality.³³

Floyd³⁴ presents a private management framework for personal electronic health records. He explains the importance of personal electronic health records and the easier communication they can bring between patients and healthcare providers in South Africa. He argues that despite South Africa's law protecting personal information, it is limited in terms of protection. Accordingly, health data may be accessed, thereby infringing patients' privacy. He proposes establishing a privacy management framework for patients using mobile devices to access sensitive health records. This is important as it is an essential responsibility for organizations to protect personal data and ensure the privacy of patients' records.

Modi discusses the importance of mobile health technology in developing countries. He uses Tanzania as a case study.³⁵ He posits that in healthcare delivery, mobile phones seem to play a significant role and a massive contribution in delivering healthcare information to many people, particularly those living in remote areas. The author presents that mobile phones are cheap, portable, easy to use, and are becoming

³³ Ibid.

³⁴ Floyd E., (et al), "A privacy management framework for personal electronic health records", *African Journal of Science, Technology, Innovation and Development*: 2018, Vol 10.

³⁵ Modi, S., "Mobile health technology in developing countries: The Case of Tanzania," *Pepperdine Policy Review*: 2013, Vol. 6.
Article 5.

readily available. He further argues that rural areas are poor and unable to travel to healthcare centres; thus, mobile health makes it easier for many people to receive healthcare information at an appropriate time. However, the study does not provide a framework for evaluating m-Health interventions in protecting the privacy of the information transferred from one device to another.

Mbiki³⁶ discusses health regulation in Tanzania. She posits that Tanzania has no harmonized legislation governing e-Health in Tanzania. The author argues that the absence of robust data protection legislation that specifically incorporates conditions for processing personal health data in the context of e-Health does not guarantee data protection. The paper further argues that Tanzania's constitutional right to privacy remains inadequate in offering a regulatory framework for protecting health-related data.

Like Msumi, Merle, *et al.*, provide a comparative analysis of the e-Health systems in Tanzania and Germany, focusing on protecting personal data in the health sector. The author discusses the legal frameworks, technical infrastructure, and data protection mechanisms in both countries and identifies the strengths and weaknesses of each system.³⁷ The authors invoked theoretical analysis only to provide a broad picture of the German and Tanzanian law in the e-Health sub-sector.

³⁶ Mbiki M. M., "An Overview of eHealth Regulations in Tanzania" DuD • Datenschutz und Datensicherheit: 2018, Vol 6.

³⁷ Merle, F., (et al), "Strengthen protection of personal data in the health sector: a comparative analysis of the Tanzania and German eHealth system", Datenschutz und Datensicherheit-DuD: 2020, Vol 6.

Sampat, *et al.*,³⁸ discuss privacy risks and security threats in mHealth applications. The authors reveal how mobile health applications have transformed the relationship between doctor and patient.³⁹ The authors posit that while the apps provide convenient access to healthcare, a lot of personal and sensitive patient data is collected, stored and shared with doctors and the patient's insurance company, lifestyle coaches, family, and friends, which raises many privacy concerns. The authors argue that little is known about the privacy and security concerns in the applications of these apps and that adopting these apps poses a risk. This is because the apps can collect a wide range of personal data from the users; some information is collected with permission, and some is not. The author concludes that, despite the number of benefits these apps offer, little attention has been given to the information security and privacy policies and practices of mHealth apps to safeguard personal information.

Townsend⁴⁰ assesses the regulatory framework that governs privacy and data protection in the effective implementation of electronic health in Africa. The author considers whether the general data protection regulation in South Africa is sufficient to secure health data privacy in the electronic environment. She argues that such a law would need to be supplemented by other measures, such as adopting multiple layers of regulatory measures around the data protection regime. Those measures include

³⁸ Sampat, B., (et al), "Privacy risks and security threats in mHealth apps," *Journal of International Technology and Information Management*: 2017, Vol. 26: Iss. 4, Article 5.

³⁹ Ibid

⁴⁰ Townsend, B.A., "Privacy and data protection in eHealth in Africa: an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking?" *Doctoral Thesis, University of Cape Town*, 2017, pp. 199-200.

self-regulation and technological measures.⁴¹ From the author's point of view it is important to consider multi-layered regulatory approach in Tanzania. Such as Tort/common law, Constitution, PDPA, contract, hospital policy/regulation, Hospitals/Doctors' Associations Code of Conduct, and consumer protection agencies, to the protection of persona data generally. Regarding the e-Health approach, Tanzania has been making efforts to integrate technology into its healthcare systems to improve efficiency, accessibility, and quality of care. This may involve initiatives such as electronic medical records, telemedicine, mobile health applications, and other digital tools aimed at enhancing healthcare delivery and patient outcomes. Combining these legal, regulatory, and technological approaches creates a comprehensive framework aimed at ensuring effective and equitable healthcare services for the population of Tanzania.

Olufunke⁴² considers the need to use the EU Regime for Data Protection as a Conceptual Model for Reforming Nigeria's Privacy Legislation. The author investigates data protection privacy and the use of mobile health in Nigeria. He does so by examining the inadequacies of the present framework relevant to mHealth privacy protection in Nigeria. The examination inquires whether the existing privacy framework protects mHealth users in collecting, using, and transferring their health information. He argues that although a privacy protection framework exists, its

⁴¹ Townsend, B.A., "Privacy and data protection in eHealth in Africa: an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking?" Doctoral Thesis, University of Cape Town, 2017, pp. 199-200.

⁴² Olufunke O. S., "Privacy Protection for Mobile Health (mHealth) in Nigeria: A Consideration of The Eu Regime for Data Protection as A Conceptual Model for Reforming Nigeria's Privacy Legislation", Master Thesis, Dalhousie University, 2015, pp. 4-6.

provisions for processing health information are not clearly defined. He further considers the prospect of adapting the European regime for privacy protection to regulate mHealth privacy in Nigeria.⁴³ The EU data protection regime is a general law not specifically intended to regulate the e-Health sub-sector. The Tanzania's Data Protection Act borrows heavily from the GDPR as well.

Mulder, *et al.*,⁴⁴ examine the legal and practical challenges surrounding the cross-border transfer of health data in the context of the EU's GDPR. The scholars further examine the discrepancies between the marketing statement “your privacy is important to us” and the actual privacy policies. The author argues that data transfer is not necessarily bound by country or EU due to the rapid growth and the very nature of modern technology. The GDPR framework stipulates privacy rights for the users of e-Health technologies and their obligations to it. When one looks into the cross-border transfer of personal data, it is observed that in the EU and its member states, rules are somehow clear, and some institutions oversee the implementation of the law. In particular, the authors observe the role of privacy policies in ensuring compliance with the GDPR's requirements for transparency and informed consent.

Yi-Chin⁴⁵ discusses privacy concerns and the continued use of telemedicine during COVID-19. The study investigates the risk to privacy during the pandemic. The study

⁴³ Olufunke O. S., “Privacy Protection for Mobile Health (mHealth) in Nigeria: A Consideration of The Eu Regime for Data Protection as A Conceptual Model for Reforming Nigeria's Privacy Legislation”, Master Thesis, Dalhousie University, 2015, pp. 4-6.

⁴⁴ Mulder, T., (et al), “Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law”, 2019, Vol 28.

⁴⁵ Yi-Chin K., (et al), “Privacy Concerns and Continued Use Intention of Telemedicine During COVID-19”, Mary Ann Liebert, inc., 2022, Vol 28.

provides an opportunity to understand consumer privacy concerns under personal or environmental risk while utilizing Telemedicine as a treatment option. The study argues that telepatients have greater privacy concerns than repeat users. The authors further argue that in risks such as the COVID-19 Pandemic, privacy concerns do not negatively impact the user's continued use intention.

Muhammad⁴⁶ provides an overview of patients' Privacy Rights Protection in Telemedicine in Indonesia During the COVID-19 pandemic. The author argues that despite regulations and guidelines on the implementation of telemedicine or online health services, personal data leakage still occurs. The author believes that no regulations regulate strict sanctions when patient's sensitive data are being misused. The author recommends special regulations protecting patients' privacy when using online health services.

Tecklenburg⁴⁷ discusses telemedicine in terms of the chances and challenges of medical genetics in Germany. The author posits that Telemedicine has been gaining popularity in Germany in recent years due to its benefits in improving healthcare accessibility, reducing healthcare costs, and improving patient outcomes. The application of telemedicine in Germany has been particularly important during the COVID-19 pandemic, as it has helped to reduce the risk of infection and maintain continuity of care. Numerous regulations and complex reimbursement structures play

⁴⁶ Muhammad F., "Telemedicine in Indonesia During the Covid-19 Pandemic: Patients Privacy Rights Protection Overview", *FIAT JUSTISIA*: 2022, Vol 16.

⁴⁷ Tecklenburg, J. Telemedicine – chances and challenges for medical genetics in Germany. *Medizinische Genetik*, 2021, Vol. 33 (Issue 1), pp. 53-59.

a role in the application of Telemedicine in medical genetics in Germany. The author is concerned that discipline- and technology-specific challenges complicate the integration of technical solutions into the medical genetic practice.

In previous studies, teleconsultations and virtual consultations in medical genetics have proven their value, as indicated by high satisfaction levels in the users and showing no inferiority to in-person consultation in terms of psychosocial outcomes. The author worries that the coming years will bring increasing demand for genetic counselling, which the limited number of specialists in Germany can hardly meet. In this context, telemedicine can help close these gaps in standard care while strengthening the field by ensuring comprehensive medical genetic care. However, there are still some challenges to the widespread adoption of Telemedicine, such as the need for reliable internet connectivity and privacy concerns related to the transmission of health-related data.

Walzer⁴⁸ provides an overview of digital healthcare in Germany. He maintains that digitization in the healthcare sector is a complex process with cross-sectoral influences in which the interests of all stakeholders must be considered. Digital healthcare in Germany has seen significant growth in recent years. The German government has been actively promoting the digitization of healthcare services to improve patient outcomes and increase efficiency in the healthcare system. The concept influences the communication between the actors, diagnosis and treatment options, and the control

⁴⁸ Walzer, S. "Digital Healthcare in Germany: An Overview. In: Walzer, S. (eds) Digital Healthcare in Germany. Contributions to Economics." Springer, 2022.

of the individual health status, and it positively influences organizational and documentary needs.

Influenced by demographic change, the increased demand for health services already poses significant challenges for the health system. The shortage of skilled nurses and medical professionals further reinforces this. The author emphasised that the increasing digitalization in the healthcare system is associated with high costs but offers better healthcare opportunities. The author expresses his concern about the incentives and market access pathways for digital solutions and the price effects of the new regulatory framework in Germany. However, there is still work to address the challenges and ensure that digital health solutions are effective, secure, and accessible to all patients. Garte⁴⁹ presents understanding and using computerized medical records and the importance of having Processes that foster innovation and better-quality healthcare, such as clinical trials or mobile health. He argues that computerized need robust data protection safeguards to maintain individuals' trust and confidence in the rules designed to protect their data.⁵⁰

According to the author, the use of computerized medical records has increased in Germany in recent years. EHRs are becoming more common, with many hospitals and medical practices using electronic systems to manage patient information. The German government has been promoting the use of EHRs to improve the efficiency and quality

⁴⁹ Garte, R. *Electronic Health Records: Understanding and Using Computerized Medical Records*: Pearson Education, p 45, 2012.

⁵⁰ Garte, R. *Electronic Health Records: Understanding and Using Computerized Medical Records*: Pearson Education, p 45, 2012.

of healthcare services. One major issue here is the lack of interoperability between different systems. This can make it difficult for healthcare providers to share patient information and coordinate care. The author is further concerned with the security and privacy of patient data. Although Germany has stringent data protection laws, there have been many debates on ensuring that patient data is kept secure while still allowing healthcare providers to access the required information.

Zeeb, *et al.*,⁵¹ point out that the COVID-19 pandemic worldwide and Germany, in particular, contributed to developing new technologies and accelerated the digitization of various domains of daily lives worldwide. One such domain focuses on digital aspects of public health. Digital public health describes the entire field of development and application of digital technologies in public health, especially concerning prevention and health promotion. The study further reveals that widespread internet access and, in particular, the introduction of smartphones and other mobile devices since 2009 have contributed significantly to the digitization of health. Among others, digitization affects services, increases the availability of information, simplifies communication, and allows individual monitoring and self-measurement. Despite all these advantages, most system users and patients express concerns about their data and privacy online.

The literature does not cover Tanzania's personal data protection in e-Health. Most of these literatures cover developed countries and a few African countries. Literature in

⁵¹ Zeeb, H., (*et al.*), "Digital Public Health Bremen Digital public health-an overview." Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz: 2020.

this context touches on personal data protection but not electronic health-related data. Although the social economics between Germany and Tanzania are not similar, the standards and principles governing personal data protection are the same.

Patient records, by their nature, are very sensitive. As discussed by different authors above, confidentiality shows the relationship between patient and doctor. But again, it is the concern of this study that confidentiality alone is not a guarantee of protection of privacy, especially of patients' sensitive information in the digital world. This study intends to establish appropriate measures to safeguard issues of privacy and confidentiality of patients' records. One trend demonstrated in the available literature about protecting privacy in the context of e-Health in Africa is that the scholars have not explicitly investigated the issue. The discussion has been general and confined to one jurisdiction.

In the latter case, replicating the findings in other jurisdictions is difficult. Particularly important, different jurisdictions have different legal cultures. Moreover, the existing legal protection varies significantly from jurisdictions with comprehensive data protection laws, such as South Africa, to jurisdictions that only recently adopted data protection legislation, like Tanzania. The present study seeks to bridge the gap in understanding the law's role in regulating the processing of personal data in the context of e-Health in Tanzania. This study, therefore, intends to cover the existing gaps by providing how best e-Health legal framework can be established to protect personal data, e-Health data, and e-healthcare delivery systems.

1.7 Research

Methods are the tools, instruments, techniques, and procedures - by which science gathers and analyzes information.⁵² Like tools in other domains, different methods can do different things.⁵³ Each method should be regarded as offering potential opportunities that are not available by other means but also as having inherent limitations.⁵⁴ To be precise, the study employs doctrinal and complemented by comparative legal research.

1.7.1 Doctrinal Legal Research

Doctrinal legal research is a common method legal scholars and practitioners use to understand and interpret the law. It is beneficial for analyzing legal issues that require a detailed understanding of legal principles and doctrines. This is traditionally the sole methodology of legal research. It primarily focuses on the law instead of what it should be. Under doctrinal methodology, a researcher's main goal is to locate and collect the law (legislation or case law) and apply it to a specific set of material facts to resolve a legal problem.⁵⁵

This method involves the analysis of legal propositions and case laws through legal reasoning and rationale deducting. This is because the major assumption of doctrinal research is that the character of legal scholarship is derived from the law itself.⁵⁶ With

⁵² Mcgrath, J.E., 'Methodology Matters: Doing Research in the Behavioural and Social Sciences', in R. M. Baecker *et al.*, (eds), *Readings in Human-Computer Interaction: Toward the Year 2000*, Morgan Kaufmann Publishers, 1995, p. 154.<http://pages.cpsc.ucalgary.ca/~saul/wiki/uploads/HCI Papers/mcgrath-methodologymatters-bgbg95.pdf>.

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ Chui, W.H and McConville, M (eds), *Research Methods for Law*, Edinburgh University Press, 2010, p.4.

⁵⁶ Ibid.

this limitation, it is imperative to note that doctrinal methodology cannot be used for legal analysis beyond an existing legal rule. This method only applies where existing laws are interpreted, or at least a bill is required. Doctrinal legal research is helpful to the proposed project as it will give room to analyse the mentioned sources while linking them to this project and coming up with tentative conclusions regarding the healthcare delivery system.

The primary data sources for this research method are domestic legislation, case laws, and international instruments. Primary legislation in the field of data protection was collected and reviewed. Similarly, case law and treaties were analysed. Decisions of quasi-judicial bodies were collected and analysed. Policies, Hansard's, reports, travaux préparatoires, journal articles, commentaries, reference books, newspapers, and magazines were part of the sources for the doctrinal research because commentaries of legal and non-legal academics provide opinions on the law. Such sources are considered secondary data.

Data analyses of information gathered in doctrinal legal research are done through interpretive constructs of deductive, analogical, inductive, and policy reasoning. A deductive approach involves “developing a hypothesis (or hypotheses) based on existing theory and then designing a research strategy to test the hypothesis.”⁵⁷ The inductive approach, also known as inductive reasoning, starts with observations, and theories are proposed towards the end of the research process as a result of

⁵⁷ Wilson, J “Essentials of Business Research: A Guide to Doing Your Research Project” SAGE Publications, p.7. 2010.

observations.⁵⁸ Analogical reasoning is a kind of reasoning that is based on finding a common relational system between two situations, exemplars, or domains. When such a common system can be found, then what is known about one situation can be used to infer new information about the other. The basic intuition behind analogical reasoning is that when there are substantial similarities between situations, there are likely to be further similarities.⁵⁹

Data analysis for doctrinal legal research involves examining and interpreting the information gathered from legal sources to identify patterns, trends, and relationships that may inform legal theories, principles, and arguments. The researcher collects all the legal materials relevant to the study and organizes them accordingly. This may include cases, statutes, regulations, legal commentaries, and other relevant sources. From there, the researcher reviewed the collected legal materials to gain a comprehensive understanding of the legal principles and theories relevant to the study.

Further, the researcher analyzes the legal materials to identify the existing legal gap and the relationships between them and the collected materials. Again, the researcher evaluates the legal materials to assess their quality and reliability for the study. This may involve considering the authority and credibility of the legal sources, as well as any biases or limitations that may affect their interpretation. Another task is interpreting the legal materials to develop legal arguments and theories based on the analysis conducted. This may involve the information gathered from the legal

⁵⁸ Goddard, W. & Melville, S., "Research Methodology: An Introduction" 2nd edition, Blackwell Publishing, 2004.

⁵⁹ D. Gentner, L. Smith, in *Encyclopedia of Human Behavior* (Second Edition), 2012.

materials into a coherent narrative and identifying any inconsistencies or contradictions in the existing legal literature. Based on the analysis and interpretation of the legal materials, the researcher concludes and makes recommendations for future legal research or practice.

1.7.2 Comparative Legal Research

The comparative research method in social sciences and humanities includes legal research to compare different cases, societies, or phenomena to identify patterns, similarities, and differences. The technique involves selecting two or more cases with common characteristics and systematically analyzing them to determine why they differ or resemble one another. It is often employed to answer questions about why certain societies or groups behave differently, why particular policies work in some contexts and not others, and how historical events shape contemporary societies.

In this study the comparative legal research was applied in a way to establish comparison of the legal framework in Tanzania to that of Germany. The comparative legal research method was beneficial to this study as it assisted to analyze the Tanzania legal and policy framework including institutions that are based in the e-Health Data Protection and compare them in similarities and differences from the German Perspective so as to establish a need for the development of the law in the mentioned subject matter by adopting the legal practice in Germany into the Tanzanian domestic legal framework. Also the comparative legal research method was applied in the collection of data in the e-Health Personal Data Protection sector in Tanzania in the light of German sectors so as to identify the weakness in the Tanzania sector and fill

the gaps by applying the strengths from the German sectors.

The most important question to pose is on why the researcher decided to apply the comparative legal research method by choosing Germany. It is important to note that Germany has the strongest data protection law in the world. This has also been important in selecting Germany as the best practice for the proposed comparative study. Due to this, a comparative analysis of the legal and regulatory systems for protecting personal data in the e-Health sector will be necessary for this research. It is also important to note that this study is all about transfer of healthy data from one healthy facility to another.

1.8 Ethical Consideration

Personal data protection is also an ethical consideration. Researchers are responsible for protecting participants' data and not using it for purposes beyond what is outlined in the informed consent. Personal data protection ensures that the research does not harm patients and their rights are respected. In this context, ethical issues were taken into very high consideration. Among the main ethical issues considered were maintaining confidentiality, ensuring that respondents participate voluntarily, adhering to agreements with the respondents on what to be collected and reported, and providing full explanations of the details and results of the research to respondents.

1.9 Significance of Study

Studying personal data protection in e-Health certainly contributes to the broader discourse on privacy in several ways, e-Health data often includes highly sensitive

personal information. Exploring how individuals provide informed consent for the collection, use, and sharing of their health data online expands our understanding of autonomy and the nuances of consent in digital contexts. It raises questions about how individuals can make meaningful decisions about their data when faced with complex privacy policies and technical jargon.

e-Health data protection operates within a complex landscape of legal and regulatory frameworks. Analyzing these frameworks and their practical implications for stakeholders provides insights into the effectiveness of current privacy laws and regulations. It also highlights areas where legal protections may be lacking or inadequate, driving discussions around the need for updated legislation to address emerging privacy challenges in e-health. e-Health data protection raises ethical considerations related to privacy, confidentiality, fairness, and equity. Researching into these ethical dimensions helps identify potential risks and unintended consequences associated with the collection and use of health data in digital contexts. It fosters discussions about ethical guidelines, principles, and frameworks for guiding responsible data practices in e-Health.in Tanzania.

It is expected that findings on existing e-Health legal frameworks and regulations in Africa and Tanzania in particular, will increase public understanding of the protection of sensitive health-related information when using e-Health technologies and be able to enforce their rights but also appreciate potential liabilities that come between the health-related data transactions.

The study also improves the literature on e-Healthcare delivery systems in the African

context. On the other side, this study identify and analyze the strengths and weaknesses of the laws, policies, and regulations and suggest the possible implementation mechanism for maintaining this important relationship between patients and the healthcare delivery system in the health industry in Tanzania. Recommendations provides for possible consideration as a guide to the strategic development and implementation of e-Health information technologies while abiding by basic personal data protection and privacy norms.

1.10 Scope of Study

The study focuses on personal data protection in e-Health: comparative analysis between Tanzania and Germany. For this case, this study chose Tanzania and Germany to enable this study to be conducted with minimal hurdles efficiently. Secondly, Germany was picked as a platform because it is the pioneer of data privacy and one of the states in Europe with a fast-growing pace of Internet subscribers, which has recently been influenced by the explosion of personal computers, smartphones and tablets supported by increased Internet capacity and with robust data protection regime thus likely to provide proper insights of the e-Health technologies regime which will serve as an eye opener to the Tanzanian e-Health technologies regime.

Therefore, this study will concentrate more on personal data protection, particularly health-related data, because of many issues ushered in by the fast growth of technology or digital health technology across diverse jurisdictions. Thus the focus of the thesis argument is to asses and makes proposals regarding the protection of personal data in health-related matters in Tanzania.

1.11 Limitation of Study

Despite the success of this study, some limitations were a challenge to the researcher. The main limitation being methodological. The researcher embarked in applying the Comparative legal study as a research method. This method negatively affected the undertaking of the study and obtaining the required data because there was a compulsory need to have the German laws, regulations and policies on hand. Though the researcher was able to obtain the said legal instruments from Germany, but it was a very difficult affair in analysing the laws as they are from a different jurisdiction with a different legal system from that of Tanzania.

CHAPTER TWO

CONCEPTS AND THEORIES OF PERSONAL DATA PROTECTION IN e-HEALTH

2.1 Introduction

Chapter two discusses concepts and theories underlying personal data protection in general and their application to protecting personal data under e-Health delivery mode. Keywords such as personal data, privacy, e-Health concept and its evolution, guiding principles, and their roles in e-Health concerning the research problem are discussed. The chapter also provides theories underlying personal data protection in the context of e-Health privacy. These are no intrusion, seclusion, control, limitation theories, and restricted access/limited control. The chapter concludes by providing theories that guide the study and rationale of that choice.

2.1.1 Personal Data

Personal data is a key concept in data protection law. In case law, personal data is often the subject of legal disputes and can be interpreted and applied in various ways. Generally, personal data has no hard and singular definition. Personal data has always been defined according to the particular context in use. Personal data means information that can be used to identify an individual, such as a name, address, date of birth, Social Security number, or medical record number.⁶⁰ In e-health, the increasing use of EHRs and other digital technologies enables the vast sharing of patient

⁶⁰ Mary, D. B., "Information Privacy in the Evolving Healthcare Environment" Journal of AHIMA, , 2015 , Vol 86(7), 28-33.

information across different platforms and systems, likely improving health service provision. In contrast, it also increases the risk of data breaches and unauthorized access to sensitive medical information.

In this context, protecting patient information in digital healthcare is important. This is sought to be achieved by implementing robust data security measures, adopting policies and procedures to safeguard mobile devices, and complying with privacy regulations. The healthcare providers can protect patients' privacy rights and maintain trust in the healthcare system. It's important to note that personal data is subject to privacy laws and regulations. Thus, it is essential to ensure that personal data is collected, used, and stored in a manner that protects individuals' privacy and rights.

Internationally, various instruments provide the term personal data. The EU's GDPR defines personal data as information about an identifiable natural person.⁶¹ An identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.⁶² Likewise, the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) defines personal data as any information relating to an identified or identifiable natural person. An identifiable natural person can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific

⁶¹ Article 4(1) of the GDPR.

⁶² Article 4(2) of the GDPR.

to his physical, physiological, mental, economic, cultural or social identity.⁶³ This definition is similar to personal data in the GDPR. Both instruments emphasize the importance of protecting individuals' privacy and personal information from unauthorized access, use, or disclosure. This position is in line with the requirement of human rights, which requires that no one be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation.⁶⁴ In this context, everyone has the right to protect the law against such interference or attacks.

The German data protection law⁶⁵ defines personal data as any information relating to an identified or identifiable natural person. This includes data such as names, addresses, email addresses, photographs, social security numbers, financial information, and other information that can be used to identify an individual.⁶⁶ The Act also recognizes sensitive personal data, which includes information about an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, criminal convictions or offences, and genetic data.⁶⁷ Protecting personal data is a fundamental right under German law, and data controllers are required to take appropriate measures to protect the privacy of individuals and ensure that their data is processed per legal requirements.

In Tanzania, as a recognition of the right to privacy and personal security enshrined

⁶³ Article 2(e).

⁶⁴ United Nations Universal Declaration of Human Rights: Article 12.

⁶⁵ The Federal Data Protection Act (Bundesdatenschutzgesetz or BDSG), which was last updated in 2018.

⁶⁶ Ibid, Section 3.

⁶⁷ Ibid, Section 9.

under Article 16 of the Constitution of the United Republic of Tanzania, 1977 as amended. According to the law, personal data is information about an identifiable natural person.⁶⁸ It includes information such as name, identification number, location data, online identifier, or any other factors that can identify a person directly or indirectly.⁶⁹ The law further outlines sensitive personal data as a subset of personal data, which includes information related to an individual's health, race, ethnicity, political affiliation, religious beliefs, sexual orientation, criminal history, biometric data, or any other data that is classified as sensitive by the relevant data controller.⁷⁰ Generally, The Personal Data Protection Act seeks to protect the privacy rights of Tanzanian citizens by regulating the collection, use, and disclosure of their data.

An understanding of the personal data concept reveals that the concept is broadly defined to encompass personal data used in the e-health system. Although some concepts touch on e-health-related issues, they are limited to the effect of using technology in e-health rather than providing a meaning of personal data to be protected by the law. To this extent, it is essential to define personal data in the context of health. Globally, personal data plays a crucial role in e-Health, enabling healthcare stakeholders to deliver more personalized, efficient, and effective care. However, it is essential to balance the benefits of using personal data with the need to protect individual rights and freedoms and ensure transparency, accountability, and trust in the e-Health ecosystem.

⁶⁸ Section. 1(1) of Personal Data Protection Act No 11 of 2022

⁶⁹ Ibid, section 1(2).

⁷⁰ Ibid Section. 2.

Personal data in e-Health context refers to any information identifying an individual, such as their name, address, date of birth, medical history, and other information related to their health or well-being.⁷¹ It includes sensitive information, such as genetic data, mental health records, and sexually transmitted disease diagnoses, among other diseases. These personal data require the protection of the law. This is because of the increased use of technology and digital platforms. Personal data has become more vulnerable to theft, misuse, or unauthorized access. Therefore, it is essential to protect personal data to prevent abuse of personal data and protect a person's privacy.

To this extent, personal data protection refers to the measures and practices safeguarding individuals' personal information. Personal data includes any information that can be used to identify a specific person, such as their name, address, email address, phone number, social security number, or other unique identifiers. Personal data have become commodities; unrestricted access to one's personal information may sometimes cause harm to the data subject. This being the case, there are several reasons for protecting personal data.

The basic principle underlying the data protection laws in different countries is the requirement of consent by the data subject and the stated purpose. These laws require organizations to obtain consent from individuals before collecting, using, or disclosing their data and to implement security measures to protect them. Data is information or data that is linked or can be linked to individual persons. Examples include explicitly

⁷¹While there is no specific article in the GDPR that defines personal data in the context of eHealth, the regulation as a whole applies to the processing of personal data, including that which is related to an individual's health or well-being.

stated characteristics such as a person's date of birth, sexual preference, whereabouts, religious affiliation, and the IP address of your computer or metadata about these kinds of information.

In addition, personal data can also be more implicit in the form of behavioural data, such as social media, that can be linked to individuals.⁷² Information forms the intellectual capital from which human beings craft their lives.⁷³ Information is essential for the functioning of contemporary society.⁷⁴ The information, or data, may be used for various economic, political, and social purposes and collected, handled, stored, and distributed by frequently unknown and unidentifiable persons or organizations.⁷⁵

The overall objective of personal data protection is to protect a person's privacy. In this context, protection of personal data and privacy are related concepts. However, the term privacy is broad and includes the protection of the privacy of the patient. It is in this context that the privacy-related concepts are discussed below. Ordinarily, no one would wish his personal information or data to be shared with everyone without a good cause. The discussion focuses on privacy-related concepts in connection to e-Health. The rationale for using privacy concepts is to protect individuals' personal information, maintain confidentiality, build trust, comply with regulations, and respect human rights. Privacy concepts protect an individual's personal information from unauthorised access. This includes sensitive information such as financial details,

⁷² DeCew, J., "Pursuit of Privacy: Law, Ethics, and the Rise of Technology" Ithaca, NY: Cornell University Press: 1997.

⁷³ Mason, R.O., "Four Ethical Issues of the Information Age," 10 (1) MIS Quarterly, 1986, p. 5.

⁷⁴ Ibid.

⁷⁵ Ibid.

medical history, and contact details.

The privacy concept helps maintain confidentiality when sensitive information is shared. This includes legal proceedings, medical consultations, and financial transactions. This is because when individuals know that their personal information is being protected, they are likely to trust organizations and institutions with their information. This can improve customer loyalty and help organizations build a positive reputation. Privacy concepts, such as data protection laws, are often used to comply with legal and regulatory requirements. Organizations that do not comply with these regulations can face legal penalties and damage to their reputation. Privacy concepts are based on the principle that individuals have a right to privacy and that their personal information should be protected. Using privacy concepts helps to respect this fundamental human right.

For this study, defining personal data in the context of e-Health is to understand the types of data to be protected by the law. Personal data is a crucial component of e-Health systems, as it allows healthcare professionals to make informed decisions about patients' treatment and care. However, using personal data in e-Health also raises significant privacy concerns, as this information must be protected from unauthorized access, use, and disclosure. For this reason, personal data protection regarding e-Health entails protecting a person's privacy. From the jurisprudential point of view, personal data protection results in privacy. In this context, the privacy-related concepts are discussed.

2.1.2 Privacy

There is no hard and fast rule defining the term 'privacy'. This term has been defined differently by different scholars depending on the context. Privacy has been conceptualized in various contexts from century to century and is used to protect the citizens' needs. It is a valuable concept and will forever remain so with the development of technology. From an international perspective, privacy is probably the most difficult to define among all human rights. There are challenges in determining the scope of this concept because different interests and theories have sought to explain the intended scope to provide a compelling, consistent account of what privacy is, why it matters when violated, and the related consequences.

Privacy is a valuable aspect of personality. Every person has a fundamental need for privacy. Human beings value their privacy and the protection of their sphere of life. They value some control over who knows what and to what extent about their affairs. No individual wants their personal information, in this case, to be accessible to anyone at any time. Several countries see the importance of protecting their citizens' information privacy from a legal perspective with meaningful enforcement policies. It is commonly assumed that in a society, life and enjoyment for all people are connected with their privacy. Everyone is entitled to protection regarding their personal life, particularly sensitive personal information. Privacy is considered the fundamental right of every individual, and it supports freedom of association, expression, and thought, basically being free from any interference. Privacy plays a vital role in protecting society and individuals, particularly fundamental human rights in the era of science and technology.

Traditionally, privacy is defined as the ability of an individual or group to control or limit access to their personal information and to be free from unwanted intrusions or surveillance.⁷⁶ It is the right to keep certain information about oneself confidential and the freedom to make decisions about how and with whom that information is shared. Defining privacy is crucial as it sets the boundaries for private information and how it can be used, shared, or accessed. It also helps establish legal and ethical guidelines for how individuals, companies, and governments should collect, store, and share personal information.

Alan⁷⁷ defines privacy as the feeling that others should be barred from things that concern him and acknowledging that others have a right to do the same. He suggested that a person's privacy is seen in three dimensions: emotions and physical images, possible unwanted intrusion, and contexts that may affect what a person feels is private to them. The author defines privacy concerning control of personal information as the ability to lay claim to the extent to which information about individuals, groups or organisations is communicated to others. In this context, a person has privacy when they can control the availability of information about themselves to others.

David defines privacy as a state or condition of limited access to a person.⁷⁸ The notion of limited access to a person's information or physical presence is an essential aspect of privacy. However, only one dimension of a broader concept encompasses many

⁷⁶ This definition of privacy is a commonly accepted one and can be found in various sources. One possible source is the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, presented at the 17th session of the Human Rights Council in 2011.

⁷⁷ Alan, P. B., 'Privacy A Useful Concept?', 42 Social Forces, 1964, at pg 429, 429.

⁷⁸ David, O.' B., "Privacy, Law, and Public Policy", New York: Praeger Publishers: 1979 at pg 16.

other elements, such as confidentiality, anonymity, and autonomy. Likewise, privacy has to do with intimacy to protect sensitive aspects of an individual's personal life.⁷⁹ Accordingly, privacy is a complex and multifaceted concept encompassing many aspects of an individual's life. While intimacy is certainly one aspect of privacy, it is not the only one. Privacy also includes the right to control how personal information is collected, used, and shared by others, the right to be left alone and make choices about one's life, and the right to maintain boundaries around personal space and possessions.

To this extent, privacy proclaims that the individual is at liberty to avoid unsanctioned intrusions in his life and personal affairs and pre-supposes that the individual will have unqualified control over the information about him. This is because privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity, and integrity.⁸⁰ It encompasses freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.⁸¹

The fact that personal data is protected to provide privacy to persons is a fundamental human right and one of the core principles of human dignity. Any risk assessment conducted to enhance the privacy of individuals' data is performed from the

⁷⁹ Julie, C. I., "Privacy, Intimacy and Isolation", New York: Oxford University Press: 1992 at pg 140.

⁸⁰ Kahn, J., "Privacy as an Aspect of Human Dignity". New York University Law Review: 2003, Vol 39.

⁸¹ Ruth, G., "Privacy and the Limits of Law" Yale Law Journal : 1980, Vol 89.

perspective of protecting the rights and freedoms of those individuals.⁸² Risk assessments can help prevent privacy breaches and the misuse of personal information, which can seriously affect individuals. Thus, It is crucial that any organization or individual responsible for handling personal data recognizes the importance of privacy as a fundamental human right and incorporates this principle into all risk assessments and decision-making processes related to personal data handling.

Furthermore, privacy is a state of affairs where information regarding an individual's life and private conditions is beyond the reach and knowledge of others.⁸³ However, privacy is not absolute, and different individuals and cultures may have varying expectations of what constitutes private information. For example, some may consider their medical history private, while others may be more open about sharing it. Therefore, privacy is a complex and multifaceted concept that can differ from person to person and from culture to culture.

From an international perspective, privacy is a complex issue that involves balancing the need for security and law enforcement with the fundamental right to privacy. One of the critical aspects of the GDPR is its recognition of the right to privacy.⁸⁴ Under the GDPR, individuals have the right to have their data processed fairly, lawfully, and transparently.⁸⁵ They also have the right to access their data.⁸⁶ Data subjects have the

⁸² This statement is written in Article 35(1) of the General Data Protection Regulation (GDPR) of the European Union. The GDPR is a comprehensive data protection law that sets out rules for the collection, processing, and storage of personal data of individuals in the EU.

⁸³ Gavison, R., "Privacy and the Limits of Law". Yale Law Journal :1980, Vol 89.

⁸⁴ Which is enshrined in Article 8 of the European Convention on Human Rights.

⁸⁵ Covered under Article 5 of the GDPR.

⁸⁶ Covered under Article 15 of the GDPR.

right to rectify and erase their data,⁸⁷ as well as the right to restrict or object to its processing in certain circumstances.⁸⁸ However, the GDPR does not explicitly define privacy in a single article, nor does it define privacy in a single term.⁸⁹ Rather, it provides a comprehensive framework for protecting individual's personal data and privacy rights. The GDPR protects the fundamental rights and freedoms of natural persons, particularly their right to protect personal data.⁹⁰

The European Court of Justice's decision in *Schrems*⁹¹ defined privacy as a fundamental right under the EU law. The case addressed the legality of the transfer of personal data from the EU to the United States, and the court found that the current mechanisms for such transfers did not provide sufficient protection for the privacy rights of EU citizens.⁹² The ruling highlights the importance of protecting personal data and the privacy of individuals in an increasingly digital world.

The UDHR and ICCPR recognize privacy as a fundamental human right. Essentially, the ICCPR requires that no one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation and that everyone has the right to the protection of the law against such interference or attacks.⁹³ A similar position is emphasized under Article 17 of the ICCPR. The right

⁸⁷ Covered under Article 16 of the General Data Protection Regulation of 2018.

⁸⁸ Covered under Article 18 of the General Data Protection Regulation of 2018..

⁸⁹ See for example the General Data Protection Regulation of 2018 requires organizations to take certain steps to protect the privacy of individuals when processing their personal data. For example, organizations must implement appropriate technical and organizational measures to ensure the security of personal data and must notify individuals in the event of a data breach. Art 35

⁹⁰ Article 1 of the General Data Protection Regulation of 2018.

⁹¹ 2020.

⁹² Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximilian Schrems (Schrems II)*, ECLI:EU:C:2020:559, 16 July 2020.

⁹³ Article 12 of the UDHR.

to privacy has become increasingly important in the digital age, where new technologies have created new challenges for protecting privacy.

Governments and corporations collect and use vast amounts of personal data, often without individuals' knowledge or consent. Generally, protecting privacy requires a coordinated and collaborative effort between governments, international organizations, and other stakeholders. It is vital to ensure that privacy laws and regulations are consistent and effective while respecting the legitimate needs of law enforcement and national security.

The Tanzania Personal Data Protection Act No 11 of 2022 defines privacy as the right of an individual to be free from interference or intrusion into their private life or affairs.⁹⁴ The Act provides a legal framework for protecting personal data in Tanzania and establishes rights and obligations for data controllers and individuals. The Act is an important step towards ensuring that individuals' privacy rights are respected and that personal data is processed responsibly and transparently. This is a step in recognising the right to privacy and personal security enshrined under Article 16 of the Constitution of the United Republic of Tanzania, 1977 (RE 2008). The Act defines privacy as the right of an individual to control and protect their personal information and data.⁹⁵

The interest of the data subject is given paramount importance by giving certain rights

⁹⁴ Section 3(1) The Tanzania Personal Data Protection Act No 11 of 2022.

⁹⁵ Ibid section 33.

in the course of data collection and data processing. The Act also requires that individuals be given the right to access their data, request that their data be corrected or deleted, and object to processing their data.⁹⁶ Additionally, the Act imposes obligations on data controllers to protect personal data against unauthorized access, alteration, disclosure, or destruction.⁹⁷ The Act further prohibits processing personal sensitive data and, for this matter, including health-related data unless required under the law.⁹⁸

Many have criticized the concept of privacy, saying that the term privacy is so inaccurate that it may be considered useless in some cases because when privacy infringement is discussed, there is often the omission of stating why such infringement is considered damaging.⁹⁹ A person's right to privacy entails having control over their personal information and being able to conduct their affairs relatively free from unwanted intrusion.¹⁰⁰ Control over personal information helps a person decide whether or not to consent to use any related information.

It is essential to note that the world has progressed to the point where individuals who talk of a breach of their privacy always reflect the violation of their data. Many individuals' lives now operate on modern-day technologies, digital lifestyles, internet use, and online platforms. The unfortunate effect is that, with the increased prevalence

⁹⁶ Ibid Section. 33(1).

⁹⁷ Ibid, Section 22.

⁹⁸ Ibid, Section 30.

⁹⁹ Daniel, J., "The Meaning and Value of Privacy" in Beate Roessler and Dorota Mokrosinska (eds), 'Social Dimensions of Privacy: Interdisciplinary Perspectives' Cambridge University Press: 2015, at pg 73.

¹⁰⁰ Neethling, J. P., (et all), "Neethling's law of personality", Durban: Butterworths, 1996.

of dealing with personal data on many beneficial and convenient levels, society has become a 'privacy-unfriendly environment. The position of rapidly advancing information communication technology and conservative and underdeveloped informational privacy law has exacerbated sensitivities around potential privacy violations.¹⁰¹

Ordinarily, People treasure their privacy and data protection and are concerned about who knows what about them. As a result, they want to protect their personal information and make it unavailable to anyone. Yet, the advancement in information technology threatens privacy and control over personal data. In a descriptive sense, access has increased, which, in a normative sense, requires consideration of the desirability of this development and evaluation of the potential for regulation by technology.¹⁰²

One wishes to see the relationship between privacy and control. Privacy can be understood as the ability of individuals to control access to their personal information or data. In other words, privacy gives individuals the power to decide what information about them is shared and with whom. Critical issues include standardized, worldwide laws for privacy and ensuring the correct use of the most appropriate privacy-enhancing technologies such as encryption, reconfigurable access and privacy settings, time outs, and proximity tokens, to name just a few.¹⁰³

¹⁰¹Davies, S.G., 'Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in *Technology and Privacy: The New Landscape* PE Agre & M Rotenberg (eds), 1997 p. 143.

¹⁰² Lessig, L., "Code and Other Laws of Cyberspace", New York: Basic Books: 1999.

¹⁰³ Fontaine, P., (et all), "Systematic Review of Health Information Exchange in Primary Care Practices" *The Journal of the American Board of Family Medicine*: 2010, at pg. 31.

A certain degree of transparency is necessary as, ultimately, it is about trust, respect, and the expectations that patients have their healthcare team to provide them with the best possible care while ensuring their privacy and confidentiality of personal information.¹⁰⁴ It is also essential that any system be readily usable by all authorized individuals, who should only have access to the information they require. The correct information must be accessible where it is needed and when needed in an appropriate format.¹⁰⁵

Thus, privacy as a means of control entails individuals determining who can access their personal information and how that information can be used. For example, privacy laws and regulations give individuals the right to know what personal information is being collected about them, how it's being used, and who it's being shared with. They also give individuals the right to request that their personal information be deleted or corrected if it's inaccurate. The right to privacy has become a universal human right articulated in the International and Regional instruments and the Constitutions of various countries.

Numerous international organizations and legal systems recognize further privacy. The UDHR enshrines the right to privacy in Article 12, which states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." At the European level, the right to privacy is perceived as a notion of human dignity and plays a vital role in guaranteeing human independence and

¹⁰⁴ Ibid.

¹⁰⁵ Ibid.

dignity. International treaties and agreements, including the ICCPR, have further developed and reinforced this right. The concern over the privacy of health-related records is a critical issue in many countries. Patients need trust in the system when their sensitive medical information is considered from one destination or person to another. If proper systems of privacy and data protection in e-Health are not initiated, users and patients may be reluctant to use the e-Health application.¹⁰⁶ Privacy is an essential aspect of e-Health, particularly when it comes to the creation of knowledge.

E-Health leads to the creation of vast amounts of health-related data that can be used to generate new knowledge and insights. It's important to note that privacy must be balanced with the need for collaboration and open communication. Individuals often need a space free from outside influence or scrutiny to explore and develop their ideas fully. Without privacy, people may be hesitant to share their thoughts and perspectives, limiting the range of ideas brought to the table. The solution is to base protection measures on legal frameworks that are understood, trusted and enforced.¹⁰⁷ Additionally, privacy can protect people's intellectual property and prevent others from stealing their ideas.

Privacy and freedom are two important concepts that intersect in the context of eHealth. One way in which e-Health can promote freedom is by providing patients with greater access to health information and resources. For example, patients may access their medical records, communicate with their healthcare providers online, and

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

receive virtual consultations and diagnoses. In establishing trust, the requirement that health-related information be kept private is a central tenet of most doctor-patient relationships. It is commonly accepted as the basis of good ethical practice.¹⁰⁸

More than ever, data handling and sound, secure record-keeping should form part of this practice in light of advancements in medical testing, genetic profiling, and medical imaging, hugely increasing the volume and detail of digitally available health information.¹⁰⁹ Given that a need for privacy in most societies is well established, cultural variants of 'privacy' exist.¹¹⁰ Although privacy is universally essential, what is considered worthy of protection is variable.¹¹¹ Differences in interpretation are apparent between various regions, with differing societies presenting divergent ideas of what is tolerable within a particular society, for instance.¹¹²

It is essential to balance the need for privacy with freedom in e-Health. Patients must be able to make informed decisions about how their personal health information is used and shared while having the freedom to access the healthcare services and information they need. In this context, privacy in e-Health becomes the key connection to personal data protection. At this level, ensuring privacy in e-Health is crucial to maintaining the trust of individuals and communities and facilitating the creation of knowledge that can improve healthcare outcomes.

¹⁰⁸ Ibid.

¹⁰⁹ Ibid.

¹¹⁰ Gidron, T., 'Publication of private information: An examination of the right to privacy from a comparative perspective (part 2)' *Tydskrif vir die Suid-Afrikaanse Reg*, 2010, Pp. 271–287.

¹¹¹ Ibid p. 287.

¹¹² Ibid.

The challenge here is that patients have enough knowledge of the issues relating to privacy when giving out their personal information during the whole process, for example, in health card registration. There is a need to create awareness in this regard. Staventonn pointed out another challenge in this arena: security policies, procedures and measures, access control, stakeholder liability, and gaps in information and computer technology across various health organizations.¹¹³ A framework considering legislative requirements, human perspectives, and technological measures is useful in developing a measurable and accountable e-health system. Successful implementation of this approach would enable the possibilities, practicalities, and sustainability of proposed e-Health systems to be realized.¹¹⁴ Hence, the term privacy in the context of e-health is meant to protect a patient's privacy in all spheres under e-Health system.

2.1.3 e-Health Data Privacy

e-Health refers to using electronic and digital technologies to support and enhance healthcare delivery. It encompasses a wide range of applications, tools, and services that can improve the delivery and quality of healthcare services and enable better communication and collaboration between healthcare professionals and patients.¹¹⁵ Examples of e-Health applications include EMRs, telemedicine, mHealth, health information exchange (HIE), and personal health records (PHRs). These tools can improve access to healthcare services, enhance the quality of care, reduce costs, and improve health outcomes.¹¹⁶

¹¹³ Svantesson, D., 'Legal liability for Internet based cross-border provision of medical advice, information and products' *9th Greek Australian Legal and Medicine Conference Rhodes Greece*, 2003, p. 122.

¹¹⁴ Patience E., (et all), "Review of security issues in e-Healthcare and solutions", HONET-ICT 2016, pp. 118-121, 2016.

¹¹⁵ The General Data Protection Regulation of 2018.

¹¹⁶ Ibid.

In addition, e-Health serves as a generic umbrella term for using ICT in health-related services and processes. E-Health has become crucial for modern healthcare systems worldwide and covers various applications, including electronic health records, electronic medication overview, and telemedicine-related services.¹¹⁷ E-Health is also defined as using ICT for health. It involves applying various ICT solutions for healthcare, including telemedicine, health information systems, and mobile health.¹¹⁸

In Germany, e-Health is defined as using information and communication technology to improve healthcare.¹¹⁹ E-Health allows doctors to prescribe digital health apps and services to patients and establishes a framework for reimbursing such services. The processes of e-health-related activities require proper handling of patient data in e-Health applications. E-Health is a crucial component of Tanzania's healthcare system and is an important tool for improving access to quality healthcare services. In general, e-Health is a broad term that refers to using electronic technologies and communication systems in healthcare to improve the quality, accessibility, efficiency, and effectiveness of healthcare services.

In Tanzania, several tools define e-Health. The National e-Health Strategy 2019-2024 defines e-Health as using ICT for health, including EHRs, telemedicine, and health

¹¹⁷ Cabieses B., (et al), "The link between information and communication technologies and global public health", 2013

¹¹⁸ World Health Organization (WHO)

¹¹⁹ Digital Care Act of 2019

information systems.¹²⁰ The Health Sector Strategic Plan¹²¹ defines e-Health as using ICTs to improve health outcomes and the efficiency of health service delivery. The Electronic Health Records Standards and Guidelines 2019 defines EHRs as electronic health records that contain health information about an individual that can be created, managed, and consulted by authorized healthcare providers. Some other laws and regulations govern the use of e-Health in Tanzania, including the Health Act of 2019, the Medical Laboratory and Technicians Act of 2019, and the Pharmacy Act of 2011. These laws and regulations guide issues such as data privacy and security, professional standards, and the use of electronic medical records. However, they do not explicitly define EHRs.

Likewise, the Tanzania Health Sector Strategic Plan IV (2015-2020) identifies e-Health as a priority area for investment and sets out strategies for implementing e-Health initiatives in the country. Similarly, The Tanzania National e-Health Strategy (2019-2024) provides a framework for implementing e-Health initiatives in Tanzania, including developing electronic health records, telemedicine, and mHealth (mobile health) services.

The 2016 Tanzania mHealth Guidelines guide the development and implementation of mHealth applications, including SMS-based messaging, mobile applications, and

¹²⁰ Section 1.1 of Tanzania National eHealth Strategy June, 2013 – July, 2018 defines eHealth as defined as the cost effective and secure use of ICT in support of health and health-related fields, including healthcare services; health surveillance; health literature; and health education, knowledge, and research. The definition introduces a range of services such as electronic health records to ensure continuity of patient care across time, mobile health services (mHealth), telehealth, health research, consumer health informatics to support individuals in health decision making, and e-learning by health workers. In practical terms, eHealth is a means of ensuring that correct health information is provided in a timely manner, where it is needed and to whom it is needed, in a secure, electronic form for the purpose of improving the quality and efficiency of healthcare delivery and prevention programs.

¹²¹ Ibid, IV 2015-2020

other mobile technologies for health promotion, disease prevention, and treatment.¹²² Ordinarily, no one would wish his personal information or data to be shared with everyone without a good cause. In this context, therefore, the discussion focuses mainly on privacy-related concepts in connection with health-related data. The rationale for using privacy concepts, particularly personal data protection, is to protect individuals' personal information, maintain confidentiality, build trust, comply with regulations, and respect human rights. The concepts discussed here are important to protect an individual's personal information from being accessed by unauthorized parties. This includes sensitive information such as financial details, medical history, and personal contact details.

Privacy concepts help maintain confidentiality when sensitive information must be shared. This includes legal proceedings, medical consultations, and financial transactions. When individuals know that their personal information is being protected, they are more likely to trust organizations and institutions with their information. This can improve customer loyalty and help organizations build a positive reputation. These concepts are often used to comply with legal and regulatory requirements, such as personal data protection laws.

Organizations that do not comply with these regulations can face legal penalties and damage to their reputation. The global principle is that individuals have a right to privacy and that their personal information should be protected. Using privacy

¹²² Tanzania Digital Health Investment Road Map 2017-2023

concepts and personal data protection in e-Health helps to respect this sensitive fundamental human. Overall, health data privacy encompasses personal data protection, e-Health, and privacy and is essential in protecting sensitive health-related data from being misused, mishandled, or accessed by unauthorized parties. In this context, the relevant concept concerning health-related data that encompasses personal data protection, e-Health, and privacy is health data privacy.

In this context, the researcher establishes a new definition of e-Health Privacy to be the position of a patient to be protected from external disturbance and interference on the health information stored on electronic data that belongs to such a patient. This definition acts as an advocacy for the total exclusion of external forces not permitted by the patient to access or use the patient's e-Health information at the detriment of the patient or for economic gains. The patient's data should be protected and in case of interference, breach or disclosure the patient must be compensated by the Health Institution for the wrongdoing and the parties involved in the unauthorized access must be criminally responsible for the action of breach.

2.2 Theories Underlying Personal Data Protection in e-Health

The privacy concept is embedded in the theories underlying personal data protection. It is in this context. The theories underlying personal data protection are discussed in the context of privacy. These theories provide a framework for understanding the importance of personal data protection in e-Health and guide the development of policies and practices that encourage the privacy, confidentiality, trust, fairness, and ethical use of patient data.

The philosophical and legal theories of privacy discussed include the non-intrusion, seclusion, limitation, and control theories of privacy. Each theory contains one or more important understandings regarding privacy in general and e-Health contexts. Personal data protection in e-Health can be traced from privacy theories, which explain the reasons for personal data protection, its operations, and how the e-healthcare delivery system operates.

2.2.1 Non-intrusion Theory

Louis Brandeis and Samuel Warren advocate the non-intrusion theory concerning privacy.¹²³ They argued that individuals have a right to privacy based on the principle of non-intrusion, which means that others should not intrude on an individual's private affairs without their consent. This idea has since become a cornerstone of privacy law and has influenced legal and social attitudes toward privacy. The theory emphasizes the importance of minimum intrusion into individuals' private lives. In essence, it requires a person to be left alone from their affairs and not to be intruded upon without giving out their consent to related information. This is a way of respecting people's privacy and allowing them total control over their lives. The theory embraces individuals' ultimate right over personal information and their ability to decide how and when it is shared with a third party.

The theory emphasizes the importance of individual autonomy and self-determination, that people have a right to keep certain aspects of their lives private, and that others

¹²³ Warren, S. D. and Brandeis, L. D., "The Right to Privacy", Harvard Law Review, 1980, Vol 4

should respect this right. The critical focus is respecting people's privacy and allowing them to maintain their personal affairs. It is a vital principle in the privacy framework, particularly in the age of global digital surveillance and personal data collection. It highlights the importance of respecting people's privacy and protecting their independence in the face of increasing pressure to share personal information to access digital services and participate in online transactions of information in general and in e-Health delivery systems.

However, the theory does not explain why, let alone what amounts not to intruding. With the fast growth of technology, it has become easier for firms to collect and analyze personal data without physically interfering with someone's private space. This presents another challenge for the Non-intrusion theory, which primarily focuses on physical intrusions into private spaces. In some cases, the government may argue that certain intrusions into individuals' private lives are necessary for national security or other public interests. This also challenges balancing privacy with other societal values, such as security. Sometimes, it can be difficult to enforce the Non-intrusion theory in practice, especially in cases where privacy violations occur in the digital dominion or by units' exterior of the government. This can make it challenging to hold some organizations liable for privacy violations.

Nevertheless, applying the Non-intrusion theory in definite cases would depend on several factors, including the context in which the privacy issue arises, the nature of the intrusion or interference, and the competing interests. For example, when a person's private medical information was being disclosed without the patient's consent, the

Non-intrusion theory would likely support their right to keep their medical information private. A valid reason for the disclosure would be required. Likewise, in cases where the government would need to search for individuals suspected of terrorist involvement, the non-intrusion theory balances government interests, national security, and the need to protect society.

Case laws have also been based on the same opinions, for example, in *Olmstead v. U.S.*,¹²⁴ whereby a suspected bootlegger challenged the use of evidence obtained through wiretapping. The Court ultimately ruled against *Olmstead*, finding that wiretapping did not violate the Fourth Amendment's protection against unreasonable search and seizure because it did not involve physical trespass. The court had this to say: Is such a view of privacy adequate? It is important to note that some versions of the non-intrusion theory tend to confuse privacy's condition (or content) with a right to privacy.

However, the ruling was eventually overturned in 1967 in the case of *Katz v. United States*, one of the landmark United States Supreme Court cases that dealt with whether a person has a reasonable expectation of privacy in a public telephone booth. The case was decided in 1967 and is still considered pivotal in Fourth Amendment jurisprudence.¹²⁵ In the case, the FBI had placed a listening device on the outside of a public telephone booth that Katz was using to conduct illegal gambling operations. The FBI obtained evidence from the listening device, which was used to convict Katz

¹²⁴ 1928. 277 U.S. 438ff

¹²⁵ *Katz v. United States*, 389 U.S. 347 (1967).

of unlawful gambling. Katz argued that using the listening device violated his Fourth Amendment rights, which protect citizens from unreasonable searches and seizures.

The government argued that Katz had no reasonable expectation of privacy in the public telephone booth because he was in a public place. In this decision, the Supreme Court ruled in favour of Katz, stating that he did have a reasonable expectation of privacy in the telephone booth. The Court held that the Fourth Amendment protects people, not just places and that a person has a reasonable expectation of privacy in a place where he or she seeks to preserve his or her privacy. The Court established the reasonable expectation of privacy test, which became a standard for determining whether a search or seizure is constitutional under the Fourth Amendment. The test requires that a person have a subjective expectation of privacy and that the expectation be one that society is prepared to recognize as reasonable.

Similarly, in *Eisenstadt v. Baird*,¹²⁶ the Court struck out a Massachusetts law that prohibited the distribution of contraceptives to unmarried individuals. Justice Brennan wrote a concurring opinion arguing that the law violated the right to privacy. He asserted that this right was not limited to married individuals but also extended to unmarried individuals and that the state had no compelling interest in regulating the private, consensual sexual conduct of adults.

In the case of *Jamii Media*,¹²⁷ the issue revolved around freedom of expression and the

¹²⁶ *Eisenstadt v. Baird* in 1972.

¹²⁷ *Jamii Media Company Ltd v. The Attorney General* (2017) TLS LR 447.

right to privacy. Jamii Media, a Tanzanian online news outlet, challenged provisions 32 and 38 of Tanzania's Cybercrimes Act, which they argued restricted freedom of expression and violated the right to privacy. The court examined whether these provisions were in line with Tanzania's constitution and international human rights standards. Ultimately, the court ruled in favor of Jamii Media, declaring certain sections of the Cybercrimes Act unconstitutional. This decision was seen as a significant victory for freedom of expression and online media in Tanzania.

2.2.2 Seclusion Theory of Privacy

The seclusion theory posits that privacy is about having a personal space where one can be free from any interference or being private and significantly away from people rather than just protecting information or data. Accordingly, the seclusion theory defined privacy as “being alone.”¹²⁸ In describing privacy as being secluded from others, this theory seems to confuse privacy with solitude. It advocates that the more alone one is, the more privacy one has. One disparity of this theory can be found in remarks by Gavison, who describes a person as enjoying perfect privacy when that person is utterly inaccessible to others when no one has physical access to the individual.¹²⁹ In the case of *Deogras John Marando vs Managing Director Tanzania*,¹³⁰ it is about the matter that concerns with personality or invasion of right of privacy which plays a vital role in shaping celebrity rights. Personality is defined as the combination of characteristic or quantities that form an individual's distinctive

¹²⁸ Herman, T.T., “Philosophical Theories of Privacy: Implications For an Adequate online privacy policy”, *Metaphilosophy*, 2007, Vol 38.

¹²⁹ Gavison, R., “Privacy and the Limits of the Law.” *Yale Law Journal*, Vol. 89 1980, p. 421.

¹³⁰ Civil Appeal No 110 Of 2018

character. So, right to personality means inherent rights associated with the personality of an individual. It aims at controlling the commercial use or any other interference of his or her identity. One of the relief sought was that the defendant (respondent herein) be ordered to pay the plaintiff total amount to the tune of 200 million as a compensation for use for profit obtained from use of plaintiff's picture/likeness for promoting its services.

Another distinction of the seclusion theory can be observed in Westin's description of privacy as the voluntary and temporary withdrawal of a person from the general society through physical means in a state of solitude.¹³¹ Warren and Brandeis also suggest a variation of the seclusion theory when they describe privacy in terms of solitude and the necessity for individuals sometimes to retreat from the world.¹³² For example, a person may choose to be in a crowded coffee shop and maintain their privacy by not disclosing personal information to others. Conversely, a person may be in a secluded area but still have their privacy violated if someone eavesdrops on their conversations or accesses their data without their consent.

The seclusion theory of privacy is often criticized for equating privacy with solitude, which is not always true.¹³³ Solitude refers to being physically alone, while privacy refers to the ability to control who has access to information about oneself.¹³⁴

¹³¹ Weinstein, M. A., "The Uses of Privacy in the Good Life." In *Nomos XIII: Privacy*, edited by J. Roland Pennock and John W. Chapman, New York: Atherton Press, 1971, Pp. 88–104.

¹³² Warren, S., and Louis B., "The Right to Privacy. *Harvard Law Review* 14, no. 5, 1890, p. 193.

¹³³ Parent, W. A., "Recent Work On The Concept Of Privacy" *American Philosophical Quarterly* Volume 20, Number 4, October 1983

¹³⁴ Ibid

However, seclusion theory may only be helpful when managing violative or self-destructive behaviour is recommended. This theory is more advantageous for health care delivery and mostly ward nursing staff as one way of managing disturbances and ensuring the safe running of the intended ward, for example, in the psychiatric wards.

The seclusion theory avoids confusing privacy and liberty because it provides an account of privacy that is essentially descriptive. It avoids confusing the content or condition of privacy with a right to privacy. In describing privacy as being secluded from others, the theory tends to confuse privacy with solitude, as stated earlier. It suggests that the more alone one is left, the more privacy one has.¹³⁵ This arrangement follows that a person stranded on an island without human inhabitants would have complete privacy, or what Gavison refers to as perfect privacy.¹³⁶ The important question is whether a person in such a situation enjoys privacy in any expressive sense. It can also be asked whether one's ability to experience solitude is essential for an individual to have privacy. Contrary to what is implied in the seclusion theory, it is seen that one can enjoy privacy while not necessarily being isolated from others.¹³⁷

Both the non-intrusion and seclusion theories address privacy concerns that pertain to physical access to individuals or in the form of unnecessary intrusion into one's personal affairs through someone physically accessing one's personal papers, home, and so forth.¹³⁸ Other aspects of the non-intrusion theory pertain to concerns about

¹³⁵ Ibid.

¹³⁶ Gavison, R., "Privacy and the Limits of the Law." Yale Law Journal, Vol. 89 1980, p. 427.

¹³⁷ Weinstein, M. A., "The Uses of Privacy in the Good Life." In *Nomos XIII: Privacy*, edited by J. Roland Pennock and John W. Chapman, New York: Atherton Press, 1971, p. 91.

¹³⁸ DeCew, J. W., *Loc cit.*, p.76.

interference with an individual's ability to make certain decisions, which are sometimes analyzed under decisional privacy.¹³⁹

Privacy analysts note that in certain states, the concept of privacy has evolved, initially associated with intrusion of physical access, then with concerns about interference in decision-making, and more recently related to concerns about the flow of personal information.¹⁴⁰ So, perhaps not surprisingly, privacy theories have tended to analyze the concept of privacy in terms of conditions having to do with access to and control over personal information.¹⁴¹

Many authors now use informational privacy to describe privacy concerns, including access to personal information stored in computer databases. Thus, privacy is more than just being alone; it encompasses various aspects such as personal autonomy, control over personal information, and the ability to limit access to oneself by others.

2.2.3 Control and Limitation Theories of Privacy

Control and limitation theory entails that privacy is not simply an absence of information about us in the minds of others; instead, it is the control over the information we have about ourselves.¹⁴² This theory emphasizes the importance of informed consent, transparency, and individual autonomy in determining privacy practices. In other words, individuals should be able to choose whether or not to share

¹³⁹ Ibid.

¹⁴⁰ Ibid.

¹⁴¹ Ibid.

¹⁴² Fried, C., "Privacy: A Rational Context." In *Computers, Ethics, and Society*, edited by Ermann, M. D., Mary Williams, B., and Gutierrez, C., P50–63. New York: Oxford University Press, 1990, p. 54.

their personal information and be informed about how their information will be used. Miller embraces a version of the control theory when he describes privacy as the individual's ability to control the circulation of information relating to him.¹⁴³ A version of the control theory is also endorsed by Westin when he describes privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.¹⁴⁴

Rachel appeals to a version of the control theory of privacy by bringing out a connection between the ability to control who has access to information about a person and the ability of that person to create and maintain different sorts of relationships.¹⁴⁵ He believes that, unlike the non-intrusion and the seclusion theories, the control theory of privacy separates privacy from liberty and solitude. Perhaps the control theory's most important insight is recognizing the role of choice that an individual with privacy enjoys. He further considers the fact that someone who has privacy can grant, as well as deny, others access to information about themselves. However, the control theory is unclear concerning two important points. First, it is unclear which kinds of personal information one can expect to have control over. Secondly, how much control can one expect to have over one's personal information?

Regarding which kinds of personal information one can expect to have control over, it can be asked whether someone can reasonably expect to control all of their personal

¹⁴³ Miller, A., *The Assault on Privacy*. Cambridge: Harvard University Press, 1971, p. 25.

¹⁴⁴ Westin, A. F., *Privacy and Freedom*. New York: Atheneum Press, 1967, p.7.

¹⁴⁵ Rachels, J., "Why Privacy Is Important." *Philosophy and Public Affairs* 4, No. 4, 1975, p. 297.

information. For example, suppose an acquaintance sees a person while shopping at a certain grocery store. In that case, they have no control over whether their acquaintance has gained information about the fact that one shopped at this particular store. In this context, the kind of personal information over which one can expect control is limited to nonpublic personal information, including information about sensitive and confidential data, such as financial and medical records. This kind of information can be contrasted with public personal information, such as where a person works, lives, shops, and dines.

Control theory is also unclear concerning how much control one can expect. What are control theorists asserting when they say that one must have control over one's personal information to have privacy? Are they claiming that one must have total or absolute control over one's personal information as a necessary condition for privacy? If so, this would seem implausible on practical grounds. People must disclose certain information about themselves in ordinary daily transactions, especially those involving commerce. Control theorists need to specify how much control one has over one's personal information, particularly how much control one has over one's personal public information versus one's non-public information, so one can expect to enjoy privacy.

Control theorists can also be interpreted as holding a conception of privacy counterintuitive to the conventional understanding.¹⁴⁶ For example, many control

¹⁴⁶ Lundgren, B., "A dilemma for privacy as control. *The Journal of Ethics*." Vol 24 (2) 2020, p. 165-175

theorists seem to imply that one could reveal every bit of personal information about oneself and yet still enjoy privacy. However, the prospect of someone disclosing all of their personal information and somehow retaining privacy, merely because they had control over whether to reveal that information, would seem to be counter to the intuitions about what is required for privacy, as well as to the way the use that concept in ordinary discourse. Although one could exercise one's autonomy in disclosing every piece of one's personal information to others, it would be not easy to understand how one could still retain one's privacy.¹⁴⁷ It would seem that the control theory confuses privacy with autonomy.

Regarding the limitation theory of privacy, Gavison¹⁴⁸ posits that one has privacy when access to information about oneself is limited or restricted in certain contexts. Gavison embraces a variation of this theory when she describes privacy as limiting others' access to information about individuals.¹⁴⁹ The parent seems to endorse a version of the limitation theory when he defines privacy as the condition of not having undocumented personal knowledge about one possessed by others.¹⁵⁰

One feature of the limitation theory of privacy is that it correctly recognizes the importance of setting up contexts or zones of privacy to restrict others from accessing one's personal information. Another strength of this theory is that it avoids confusing privacy with autonomy, as well as with liberty and solitude. The limitation theory

¹⁴⁷So, one can have control over information without necessarily having privacy, and it is seen that one can have privacy even when one has limited control over one's personal information.

¹⁴⁸Gavison, R., "Privacy and the Limits of the Law." Yale Law Journal, Vol. 89 1980, p. 428.

¹⁴⁹*Ibid.*

¹⁵⁰Parent, W. A., 1983. "Privacy, Morality and the Law: Philosophy and Public Affairs 12, no. 4. 1983, p. 269.

seems to undervalue the role of control that is also required in one's having privacy; it does not consider that someone who has privacy can choose to grant others access to information about themselves and limit others from access to that information.

The limitation theory also seems to imply that one has privacy only to the extent that access to information about oneself is limited or restricted. The more one's personal information can be withheld from others, the more privacy one has. Thus, in the account of privacy offered in the limitation theory, privacy can easily be confused with secrecy.¹⁵¹ This theory emphasizes the need for legal and regulatory frameworks that limit the collection and use of personal information and provide remedies for individuals whose privacy has been violated. Both theories recognize the importance of privacy as a fundamental right and acknowledge the need to protect personal information. However, they differ in their approach to achieving this goal. The control theory emphasizes individual autonomy and empowerment, while the limitation theory emphasizes external constraints and regulation. The appropriate balance between control and limitation will depend on the specific context and the level of risk involved in collecting and using personal information.

2.2.4 The Restricted Access/Limited Control Theory (RALC)

RALC Theory guided this study by emphasising the importance of individuals determining who can access their personal information and under what circumstances. The researcher examined and defended a theory of privacy that incorporates elements

¹⁵¹For an interesting discussion of some ways in which concerns affecting privacy and secrecy overlap, see Thompson, P. B., "Privacy, Secrecy, and Security." *Ethics and Information Technology* 3, No. 1, 2001, Pp. 13–19.

of the classic theories into one unified theory. Therefore, the RALC theory is considered an approach to this study. RALC is designed to protect personal information from unauthorized access and misuse. RALC helps prevent identity theft, fraud, and other privacy violations.

Many industries and organizations are required by law to protect personal information. RALC provides a framework for meeting these legal and regulatory requirements by outlining best practices for controlling access to personal information and giving individuals control over their data. By implementing RALC, organizations can demonstrate their commitment to protecting their customers' privacy. This can help build trust with customers and improve the organization's reputation. By giving individuals control over their data, RALC can help improve the accuracy and completeness of data. Individuals are more likely to provide accurate information when they feel they have control over its use.

The RALC theory explains privacy as protection from intrusion and information gathering by others, not in terms of control over information.¹⁵² The RALC theory of privacy tries to combine both concepts. It distinguishes between the concept of privacy, defined in terms of restricted access, and the management of privacy, achieved via a system of limited controls for individuals.¹⁵³ The RALC sees restricted access and individual control as mutually constitutive. Individuals and society may

¹⁵² Tavani, H.T. (2008), "Informational privacy: concepts, theories, and controversies", in Himma, K.E. and Tavani, H.T. (Eds), *The Handbook of Information and Computer Ethics*, Wiley, Hoboken, NJ,

¹⁵³ Tavani, H.T. (2008), "Informational privacy: concepts, theories, and controversies", in Himma, K.E. and Tavani, H.T. (Eds), *The Handbook of Information and Computer Ethics*, Wiley, Hoboken, NJ, pp. 131-64

regulate privacy in certain ways, which is an aspect of subjectivity and action. Based on this action, a sphere of privacy for individuals protected from access to others may be set up to enable individuals to act in society, their private sphere, and the public based on privacy and data protection.¹⁵⁴

This theory provides a framework to analyze and understand privacy in information technology and online communications. The theory suggests that privacy is maintained by limiting access to personal information and giving individuals control over how their information is used and shared. It proceeds on the assumption that an adequate theory of privacy needs to differentiate the concept of privacy from its justification and management.¹⁵⁵ Accordingly, the RALC framework has three components: account of the concept of privacy, justification of privacy, and management of privacy.¹⁵⁶

The distinction mentioned earlier distinguishes between a loss of privacy and a violation or invasion of privacy. The question that arises is how exactly privacy is defined in this framework. Accordingly, an individual has privacy in a situation with others if, in that situation, the individual is protected from intrusion, interference, and information access by others.¹⁵⁷ In this context, the notion of a situation, which has a critical role in the definition of privacy, is left deliberately unspecified so that it can range over states of affairs that we usually regard as private.

¹⁵⁴ Ibid.

¹⁵⁵ Ibid.

¹⁵⁶ Ibid.

¹⁵⁷ Moor, J.H., "Toward an Approach to Privacy in Public: Challenges of Information Technology." In *Readings in CyberEthics*, 2nd Ed, edited by Richard A. Spinello and Herman T. Tavani, Sudbury, Mass.: Jones and Bartlett, Note that because RALC requires that one must have protection from intrusion *and* interference *and* information access, it addresses concerns not only about protecting informational privacy (as described in the control and the limitation theories) but also about protection against the kinds of threats described in the non-intrusion and the seclusion theories as well.

From a practical point of view, RALC theory can be applied to various situations, such as social media platforms, online shopping sites, and government surveillance programs. For example, social media platforms should allow users to control who can see their posts and personal information, and government surveillance programs should be subject to oversight and limitations to prevent abuses of power. RALC also draws an essential distinction between a naturally private situation and a normatively private situation. In the former, individuals are shielded or blocked from observation, interference, and intrusion by natural means¹⁵⁸, such as physical boundaries in natural settings, such as hiking or camping in the woods. The latter entails that privacy can be lost but not violated or invaded because there are no norms conventional, legal, or ethical according to which one has a right to be protected.¹⁵⁹

Since the RALC theory links privacy with protecting individuals by limiting or restricting access to persons or information about persons, RALC might initially appear to be simply a variation of the limitation theory. In his article,¹⁶⁰ Dag examines the European Union's Directive 95/46/EC and its approach to privacy rights. He argues that the Directive takes a "restricted access and limited control" approach to privacy, which means that individuals have the right to control access to their data, but only to a limited extent. However, the Directive acknowledges the importance of protecting personal data but does not give individuals complete control over how their data is used.

¹⁵⁸Moor, J.H., "Toward an Approach to Privacy in Public: Challenges of Information Technology." In *Readings in CyberEthics*, 2nd Ed, edited by Richard A. Spinello and Herman T. Tavani, Sudbury, Mass.: Jones and Bartlett, 2004, Pp. 450–61.

¹⁵⁹ *Ibid.* p. 462.

¹⁶⁰ Elgesem, D., "The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data. *Ethics and Information Technology*. 1999, p. 289.

RALC generally defines privacy as protection from intrusion and information gathering by others, not in terms of control over information. Literature shows that there are difficulties in defining the control theory of privacy in a way that requires one to control one's information on one side. On the other hand, one can have privacy without complete control and control over information without having privacy.

Control is also vital for the management of privacy. In managing one's privacy, one should not have absolute control over information about oneself. Instead, an individual must have some degree of control concerning choice, consent, and correction.

A person needs some control in choosing situations that offer others the level of access the person desires, which can range from total privacy to total publicity. One can also manage privacy through the consent process; for example, one can waive one's right to restrict others from accessing certain information about oneself. Regarding the role that correction of personal information plays in managing privacy, individuals need to be able to access and amend their information if necessary. For example, consumers need to be able to access information about their credit history and credit scores and challenge and correct any erroneous information. Limited controls such as choice, consent, and correction are made possible by adequate privacy policies.

Accordingly, RALC, an individual has privacy "in a situation with regard to others if in that situation the individual ... is protected from intrusion, interference, and information access by others." To see how the notion of control works in the RALC framework, consider the example of one's medical information. That information is private because a normative zone has been established to restrict people from accessing

the information, not because an individual has complete control over who has access to that information within a medical setting. Doctors, nurses, financial administrators, and insurance providers may access various pieces legitimately. But why does information included in one's medical records deserve normative protection? One justification is that individuals seek to avoid embarrassment and discrimination.

Another related justification is that individuals seek control over their lives. They need some degree of control, even if limited, over whom they associate with, what jobs they hold, and what insurance plans they select. Privacy policies that protect information in a particular situation by normatively restricting others from accessing that information provide individuals with limited controls.¹⁶¹ The notion of privacy as control and limited access implies that privacy operates as a limit to using one's personal information. Thus, individuals have the right to control access to their personal information.

It is perhaps worth summarizing some key features of RALC at this point. Because RALC differentiates the concept of privacy from both the justification and management of privacy, it has three important components. Privacy is protection from intrusion and information access by others in a situation. One has normative privacy when protected by explicit norms, policies, or laws established to protect individuals. Although privacy is defined as protection and restricted access, the notion of control

¹⁶¹ Privacy protection is justified, in part, because the protection it provides allows a person to plan his/her life in certain ways (e.g., to decide which projects a person will undertake and which risks he/she will assume). Private situations also allow for intimacy and close personal relationships. In effect, privacy offers individuals some control over their lives, which can lead to increased autonomy and happiness. It is important to note that the need for control provides only one justification for privacy policies. Moor notes that privacy protection is also justified because privacy expresses or articulates a "core value"—viz., security—which is essential to human flourishing and is increasingly threatened in computerized societies.

also plays an important role in the RALC framework in justifying and managing privacy. Part of the justification for framing privacy policies is that they provide individuals with the limited controls they need to manage their privacy. Let us apply RALC to a specific privacy issue involving information technology to determine how an adequate privacy policy can be framed. This theory presupposes that an adequate privacy theory must differentiate the concept of privacy from the justifications and management of privacy.

The processing of information is part and parcel of the provision of healthcare. At the simplest level, patients have information that they share with medical staff, and medical staff impart information to patients. At the most complex, it is seen that numerous institutions are sharing and generating information on the patients and medical staff to manage the provision of healthcare. It is true that the introduction of information and communication technology into the healthcare context multiplies and complicates the risks of outsider abuse of medical information.¹⁶² However, the fundamental problem is not technological but rather the legal framework within the health care institutions that guarantee patients' sensitive information privacy.

The individual control of personal information plays a vital role in managing privacy. This theory has been compelling. In the first place, viewing privacy as a right to control personal information is evident in rules prescribing that personal private information may only be used when the person has given their consent, especially with the

¹⁶²Thomas C. R., 'Privacy, Information Technology, and Health Care', CACM, Vol.40(8), 1997, Pp. 92-100.

processing of personal data as one of the binding nature of legal regulations of privacy and data protection. With this theory, an individual can also have a right to control places and locations, including physical access. One would wish to know if everyone is given this right to consent reasonably enough to use their personal information.

The situation may arise in some cases, let us say in health care, where, as an individual, one has to accept the consequences of denying or giving consent. The right to consent sometimes may give rise to a situation where an individual is left alone. These challenges may be due to one person's social and intellectual competencies. The privacy challenges should not overshadow the potential of the Internet to offer consumers greater privacy protections than in the offline world. E-Health companies have the potential to do better with privacy than their offline kin have done.

In the offline, paper-based healthcare world, photocopying medical records for patients is time-consuming and expensive; obtaining patients' authorization for specific disclosures and security may not be much more than a locked file cabinet. In contrast, e-Health companies now have the means to engage consumers up front in a meaningful dialogue about using and disclosing their personal information. Privacy-enhancing technologies such as encryption, online opt-in buttons, and e-mail and Web browsing anonymisers are readily available.¹⁶³

Data handling and good, secure record keeping should form the backbone of any e-

¹⁶³see: <http://www.healtfair.org/doi/full/10.1377/hltaff.19.6.140> (accessed on 27 April 2023)

Health practice to succeed in securing user confidence and gaining global momentum. This is particularly so in light of advancements in medical testing, genetic profiling, and medical imaging and the dramatic increase in the volume and detail of digitally available health information.

One of the greatest advantages of information technology in health care is that e-Health can create a platform and infrastructure for sharing and exchanging electronic health records. Personal medical information about a patient is recorded in a patient's medical record and may be kept in either paper or electronic form. Although these records may include extensive personal information regarding a patient, they usually include medical notes, historical reports, magnetic resonance images, clinical laboratory results, medical practitioners' letters, referrals, medication prescriptions, and treatment regimes. They may then be centrally recorded, located, and accessible to various medical healthcare practitioners.¹⁶⁴

An overview of the theories discussed above reveals that one of the main challenges with the non-intrusion theory is defining what constitutes an intrusion. The definition of an intrusion can vary widely depending on the context and cultural norms. For example, some individuals may feel that being observed in public is an intrusion, while others may not be bothered by it. Additionally, technological advances have made it easier to collect and analyze data on individuals, raising questions about what types of data collection constitute an intrusion.

¹⁶⁴ Ibid.

The seclusion theory is based on a reasonable expectation of privacy, which can be ambiguous and difficult to define. What one person considers private may not be the same for another person, making it difficult to apply the theory consistently. Advances in technology have made it easier for individuals and organizations to collect, store, and analyze personal data. This has created new privacy challenges that the seclusion theory may not be well-equipped to handle. One of the main challenges with control and limited theory is the difficulty in defining the boundaries of privacy.

Control and limitation mechanisms rely on clear definitions of what constitutes private information, but these definitions can be challenging to establish and can vary across cultures and individuals. Additionally, as technology advances, the types of data that can be collected and shared constantly expand, making it challenging to keep up with new privacy threats. The RALC suggests that privacy is maintained by limiting access to personal information and giving individuals control over how their information is used and shared. Thus, it is more relevant to personal data protection in e-Health because, if employed, it is likely to protect health-related data. There will be no direct intrusion, and it accommodates the establishment of e-health-related policies that will allow the establishment of regulations or relevant laws.

2.3 Conclusion

The concepts and theories discussed in this chapter provide this study's scope and conceptual and theoretical basis. The three concepts discussed are important in personal data protection in e-Health and data privacy. For this study, these concepts will be used repeatedly. RALC posits that individuals should be able to restrict access

to their personal information and have control over how that information is used. This means that individuals should have the right to determine who has access to their personal information and how it is used. Generally, the RALC theory provides a useful framework for understanding privacy in the digital age and highlights the importance of giving individuals control over their personal information.

Privacy and personal data protection, in many instances, complement each other. Protecting privacy may facilitate the individual's protection of their sensitive information. Therefore, it is necessary to understand the politics of the relationship between privacy and personal data protection, particularly in health-related information. The next chapter focuses on international and regional benchmarks for protecting personal data in e-Health.

CHAPTER THREE

LEGAL AND POLICY FRAMEWORK ON e-HEALTH PERSONAL DATA PROTECTION

3.1 Introduction

This chapter presents international, regional and sub regional instruments that provide benchmarks for protection of personal data in e-Health. In essence, it reviews standards enshrined under UN, European Union and Africa. The United Nations has developed a number of international instruments and agreements on personal data protection, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Additionally, the UN has adopted a number of resolutions and recommendations on the protection of personal data, including the Guidelines for the Regulation of Computerized Personal Data Files and the UN General Assembly's Resolution on the Right to Privacy in the Digital Age. These instruments and agreements provide a framework for the protection of personal data and privacy rights that can serve as a benchmark for countries and organizations seeking to establish their own data protection regimes. legislation. Apart from data protection standards, aspects of Human Rights instruments are also considered both at the international level and regional level.

Absolutely, data protection is a critical aspect of modern society, especially with the rise of digital technologies and the increasing amount of personal information being

collected and processed. There are indeed several international, regional and sub-regional instruments that aim to safeguard individuals' data privacy and ensure responsible handling of personal information. Internationally, the United Nations International Covenant on Civil and Political Rights (ICCPR)¹⁶⁵ enshrines provisions related to the right to privacy, including protecting personal data.¹⁶⁶ UN Guiding Principles on Business and Human Rights of 2011 guides how businesses can respect human rights, including privacy and personal data protection.

From a regional integration perspective, the European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016 and became enforceable in May 2018. The GDPR applies to any organization that processes personal data of EU residents, regardless of where the organization is based. The GDPR also sets out strict requirements for data processing, including consent, data minimization, and transparency. In this context, any challenges arising from e-Health management may require a transnational approach. It is worth noting that although not specific to Africa, the GDPR has an extraterritorial effect and applies to any organization that processes the personal data of individuals in the European Union, including African organizations.

In Africa, the AU Convention on Cyber Security and Personal Data Protection 2014 was adopted by the AU. This instrument aims at promoting cybersecurity and

¹⁶⁵ 1966.

¹⁶⁶ Article 17(1) ICCPR That no one shall be subjected to arbitrary or unlawful interference with his privacy, family, Everyone has the right to the protection of the law against such interference or attacks. home or correspondence, nor to unlawful attacks on his honour and reputation and article 17(2) that .

protecting personal data on the African continent.¹⁶⁷ Essentially, it outlines the principles of data protection, establishes the rights of individuals regarding their data, and sets out the obligations of data controllers and processors.¹⁶⁸

These instruments and agreements provide a framework for protecting personal data and privacy rights that can serve as a benchmark for countries and organizations seeking to establish data protection regimes. By referencing the UN's standards and recommendations, individuals and organizations can ensure they meet globally recognized standards for protecting personal data, which can help build trust with their customers or users.

At the regional level, the chapter focuses on AU, EAC and SADC framework on privacy because Tanzania is a member of these regional and sub-regional initiatives on data protection. Tanzania's membership in the African Union (AU), the East African Community (EAC), and the Southern African Development Community (SADC) implies its involvement in various regional and sub-regional initiatives, including those concerning data protection and privacy. While specific frameworks solely dedicated to privacy might not exist under these organizations, they often collaborate and share best practices on matters related to data protection and privacy.

3.2 International Legal and Policy Framework

The International legal framework on e-Health Personal Data Protection is very rich

¹⁶⁷ Article 8 of the African Union Convention on Cyber Security and Personal Data Protection 2014.

¹⁶⁸ Ibid, Article 9.

with a number of instruments to that effect which have been adopted by the states of Tanzania and Germany and become instrumental in the protection of data. Some of the Instruments are elaborated below;

3.2.1 The Universal Declaration of Human Rights, 1948 (Hard Law)

The UDHR is a long-term document that has been used in the history of human rights. The states of Germany and Tanzania are parties to this instrument. This international document was adopted and accepted by the UN Assembly as Resolution No. 217 of 1948. The document set out for the first time that fundamental human rights to privacy should be globally protected. The Declaration provides for the right to privacy thus;

*“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”*¹⁶⁹

Although UDHR is a non-binding declaration, it has considerable status as the foundational instrument of international human rights law. It has served as a benchmark in developing other human rights instruments across the World, which enshrine the right to privacy and data protection. The right to privacy is a fundamental human right that the law should protect. The UDHR recognizes that individuals have the right to be free from unreasonable intrusion into their personal and private lives, including their homes, families, and correspondence.¹⁷⁰

The right to privacy is essential for protecting other human rights, such as freedom of

¹⁶⁹ Article 12 of the UDHR.

¹⁷⁰ Article 12 of the UDHR.

expression and association, and helps individuals maintain autonomy and control over their lives. Governments and other entities are obligated to respect and protect the right to privacy, and any interference with this right must be based on clear legal grounds, be necessary for a legitimate aim, and be proportionate to the aim pursued.¹⁷¹ Any arbitrary or unlawful interference with the right to privacy violates international human rights law. In essence, the UHDR recognizes privacy as a basic human right and forms the basis for protecting personal data under the e-Health delivery system.

3.2.2 The International Covenant on Civil and Political Rights (ICCPR), 1966. (Hard Law)

The ICCPR was adopted by the UN General Assembly in 1966 and entered into force in 1976. The states of Tanzania and Germany are state parties to this Instrument. It is a key international human rights treaty that sets out the civil and political rights to be protected by state parties to the treaty.¹⁷² The ICCPR is legally binding and obligates state parties to respect and ensure the rights set out in the treaty, such as the right to life, freedom of speech, religion, and assembly, and the right to a fair trial. As of 2022, 173 state parties to the ICCPR are regarded as one of the most important international human rights instruments.

The ICCPR recognized the need for data protection laws to safeguard the fundamental right to privacy recognized as stipulated under Article 17 of the ICCPR. It states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family,

¹⁷¹ Ibid Article 19

¹⁷² Article 3 of the ICCPR.

home, or correspondence nor unlawful attacks on his honour and reputation. This article provides remedies for damages against such interference or attack.¹⁷³

The ICCPR recognizes and protects various civil and political rights, including privacy.¹⁷⁴ Although the ICCPR does not explicitly mention data protection, it contains provisions for protecting personal data under e-Health. This can be inferred from Article 17, which requires a person not to interfere with his privacy and attacks on his honour and reputation. This is because unauthorized collection, use, or disclosure of personal data in all spheres, including e-Health, interferes with privacy.

The UN General Assembly Resolution on privacy, specifically Comment 16 to Article 17 of the ICCPR, provides an essential framework for protecting privacy rights. Comment 16 emphasizes that protecting privacy is essential to enjoy other human rights, such as freedom of expression and association. It recognizes that the collection, use, and disclosure of personal data can pose risks to privacy and that safeguards are necessary to ensure that such activities are consistent with human rights principles. The focus is that laws specific to privacy and data protection shall regulate the gathering and holding of personal information on computers, data banks, and other devices, whether public authorities or private individuals or bodies demand such information. It makes it clear that the country shall take measures to ensure the safety of the said information so that it does not end up in the hands of persons who are not legally allowed to either receive, process or use it.

¹⁷³ Article 17 (2) of the ICCPR.

¹⁷⁴ Ibid Article 17 (1).

The provision clarified that every individual has the right to establish and be aware of what personal data is stored in automatic data files and for what purposes. In case such information has been collected or processed contrary to the provisions of the law, the data subject has all the right to request the modification or removal of the said information. Generally, the framework provided by the United Nations General Assembly Resolution on privacy, particularly Comment 16 to Article 17 of the ICCPR, highlights the importance of protecting privacy as a fundamental human right. This Article provides guidance for policymakers and stakeholders concerning collecting, using, and disclosing personal data. It emphasizes the need for safeguards to ensure these activities are consistent with human rights principles.

In addition, the UN General Assembly has recognized the importance of data protection in several resolutions, including Resolution 68/167, which calls for protecting privacy in the digital age. The UN also established the Office of the High Commissioner for Human Rights (OHCHR), which has taken a leading role in promoting the protection of privacy and personal data as a human right.¹⁷⁵

3.2.3 The UN Convention for the Protection of Individuals with Regards to Automatic Proccesing of Personal Data of 2018 (Hard Law)

This is a Convention in place to protect the automatic processing of personal data to individuals around the globe. The states of Tanzania and Germany are parties to this

¹⁷⁵ OHCHR has organized expert consultations and published reports to explore the challenges that the right to privacy and other human rights face in the digital age, as requested by relevant resolutions by the General Assembly and the Human Rights Council. See <https://www.ohchr.org/en/privacy-in-the-digital-age>

Instrument. The main purpose being to protect the respect to the right to privacy to personal data or information.¹⁷⁶ This instrument is essential to the patients as it advocates for the respect to the right to privacy and protection of their personal data. In the same footing, the Convention requires member states to ensure that all data processors take appropriate security measures against risks such as accidental or unauthorised access.¹⁷⁷ In case of any breach of personal data, the controller or processor is required to inform the owner of the data within a reasonable duration.¹⁷⁸ The above instrument basically protects the personal data of patients by ensuring that the privacy within the patients data is protected as against the third parties. It follows that the patients data should be well secured by the data processors and not otherwise. This is to ensure that the data of the patient is well secured against unauthorised access.

Therefore, the Convention provides three basic roles to the protection of personal data of a patient. The first role is to ensure that the privacy in the information belonging to the patient is well protected. In this role the most important aspect is the privacy issue and not otherwise, so if the information is not of privacy then it is not subject to protection. The second role is to ensure that all measures to prevent any risk of information breach is guaranteed. The third role is to ensure that the information is conveyed to the patient in case of any breach.

¹⁷⁶ UN Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of 2018, Provision of Article 1

¹⁷⁷ Ibid, the Provision of Article 7 (1)

¹⁷⁸ Ibid, the Provision of Article 7 (2)

3.2.4 WHO Declaration on the Promotion of Patient Rights in Europe of 1994.

(Hard Law)

This declaration was adopted by a special committee of the World Health Organization at Amsterdam. The state of Germany is a signatory to the declaration. The declaration was initiated for the purpose of ensuring that the rights of patients in various sectors are protected. In the aspect of information to health the declaration requires that everyone has the right to have respect to his or the privacy.¹⁷⁹ This is very essential that, the right to privacy of the patient in relation to the information of his or her health must be protected. The rationale of the declaration is that Health information is a private affair and should not be disclosed to the public without the consent of the patient. Although, the provision of Article 2 (1) of the declaration only permit disclosure of Health information to be conveyed from the public only for beneficial purposes and not for disclosing the patients health whereabouts.¹⁸⁰

3.2.5 Right to Privacy in the Digital Age (GA Res. 71/199) (Soft Law)

The UN General Assembly adopted Resolution No. 71/199 in December 2016. This non-binding instrument recognizes the increasing importance of protecting the right to privacy in the digital age. The resolution acknowledges the transformative role of digital technology and the internet in enhancing human rights but also highlights the challenges and risks to privacy posed by digital technologies and the need for a human rights-based approach to digital communications.

¹⁷⁹ WHO Declaration on the Promotion of Patients Rights in Europe of 1994 of Article 1

¹⁸⁰ Ibid, WHO Declaration of 1994

The resolution calls on states to review and update their laws and practices related to the interception, collection, and retention of personal data and to ensure that their surveillance activities comply with international human rights law.¹⁸¹ It also calls on all stakeholders to promote transparency and accountability in the use of digital technology and to respect individuals' right to privacy in the digital age. The resolution also emphasizes balancing privacy and other important values, such as national security and public safety. It calls on governments to ensure that measures taken to protect these values do not unnecessarily infringe upon individuals' privacy rights.¹⁸²

The resolution reflects a growing recognition of the importance of privacy and data protection in the digital age and the need for governments and other stakeholders to protect these rights. Globally, the resolution emphasizes the need for a human rights-based approach to digital communications and highlights the importance of protecting privacy in the digital age.¹⁸³ Although the resolution is not legally binding, it carries significant moral and political weight and is an important reference point for protecting privacy in the digital age.

3.2.6 General Assembly Resolution 45/95 and Guidelines for the Regulation of Computerized Personal Data Files of 1990 (Soft Law)

The guidelines were adopted by the UN in 1990 and they are non binding. They

¹⁸¹ A great discussion was that States urgently need to undertake a review their national law and where necessary adopt clear and precise legislation that both protects the right to privacy, including in internet and telecommunications, and regulates communications surveillance by law enforcement and intelligence agencies. Legislation should include anonymity protection for internet and telecommunications. State should also enact data protection laws. States should review their communications and data legislation on a regular basis to ensure that it keeps pace with technological advancements. See ReportThe Right to Privacy in the Digital Age (www.geneva-academy.ch).

¹⁸² Ibid.

¹⁸³ Ibid.

provide a framework for the regulation of personal data protection. These instruments recognize the increasing importance of protecting personal data and the need for privacy rights to be respected in the context of the growing use of electronic data processing.¹⁸⁴ They aim to promote the protection of personal data and privacy by establishing guidelines for collecting, processing, using, and disseminating personal data held in computerized files.

It is the cardinal principle of the guidelines that, information about persons must be collected and processed in regards to fairness and lawful ways.¹⁸⁵ This means personal data of a patient must be characterized by lawfulness and fairness at all times without any predjudice. This is supplemented by the requirement that, the information of a patient must be accurate and periodic checks must be made to ensure that the data processed and stored is accurate to its fullest length.¹⁸⁶ The security of the patients information is highly regarded by the guidelines. The guidelines require appropriate measures to be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorised access , fraudulent mis use of data or contamination by computer virus.¹⁸⁷

In essence, the guidelines provide a comprehensive framework for data protection that covers various aspects, including the lawful basis for data processing, the rights of data subjects, the obligations of data controllers, data security, and data transfer across

¹⁸⁴ Principle 1 of The General Assembly resolution 45/95 and Guidelines for the Regulation of Computerized Personal Data Files

¹⁸⁵ Ibid, Principle 1

¹⁸⁶ Ibid, Principle 2

¹⁸⁷ Ibid, Principle 7

borders.¹⁸⁸ The guidelines also emphasize the importance of obtaining informed consent from data subjects before processing their data and ensuring that data is accurate daily. The ingredient of consent is very important in ensuring that the data disclosed was permitted by the patient and not otherwise.

3.2.7 OECD Guidelines on the Protection of the Privacy and Transboundary Flaws of Personal Data RE 2013. (Soft Law)

These guidelines are non binding to the OECD member states . The guidelines intend to provide the proper methodology on the protection of the privacy of information or personal data. The guidelines require that the collection of Personal Data should be limited to the rule of lawfulness and fairness and should be collected in regards to the consent of the owner of the data.¹⁸⁹ This is very important that, that the collection of data should be subject to the consent of the patient to whom the personal data is required from. Also the guidelines require for the personal data to be relevant to the purpose for which it is sought or used and should be accurate.¹⁹⁰

This is essential to the patients personal data , due to the ground that, the data sought from the patient must be applied or used to the required purpose and not otherwise. Generally the guidelines require that, the purpose for which the personal data is collected should be specified before or during the time of collecting the data.¹⁹¹ This means that, before data of a patient is sought, the patient must be notified on the

¹⁸⁸ Ibid Principle 1-5

¹⁸⁹ OECD Guidelines on the Protection of the Privacy and Transboundary Flaws of Personal Data RE 2013, Para 7 of the Guidelines.

¹⁹⁰ Ibid, Paragraph 18 of the Guidelines

¹⁹¹ Ibid, Paragraph 9

purpose of collecting the data from him or her. Therefore, the guidelines advocate for the non disclosure of the personal data of a person without the consent of such a person or without authorization of the law.¹⁹² Thus personal data of a patient can only be disclosed by consent of the patient or by authorization of the law.

3.2.8 UN System of Privacy and Data Protection in the e-Health Subsector.

The UN system doesn't have a centralized framework for privacy and data protection specifically tailored to the e-Health subsector. However, several UN agencies work on issues related to privacy and data protection in the context of healthcare, including the World Health Organization (WHO), the United Nations Development Programme (UNDP), and the International Telecommunication Union (ITU). These agencies often collaborate with other international organizations, such as the World Bank and the World Trade Organization (WTO), as well as with national governments and non-governmental organizations (NGOs), to develop policies and guidelines for safeguarding privacy and protecting data in e-Health systems. The approach to privacy and data protection in the e-health subsector varies from country to country and depends on factors such as legal frameworks, technological infrastructure, and cultural norms.

The development of e-Health standards under the UN began in the late 1990s with the establishment of the WHO's e-Health unit.¹⁹³ The WHO was created to provide

¹⁹² Ibid, Paragraph 10

¹⁹³ WHO Global Strategy on Digital Health, 2020, retrieved from https://www.who.int/health-topics/digital-health#tab=tab_3, on 27/04/2024

guidance on using ICTs in healthcare and promote the development of e-Health standards. In 2005, the WHO established the Global Observatory for Health (GOe), which aimed to monitor and promote the development of e-Health standards and best practices.¹⁹⁴ The GOe works closely with other UN agencies, such as the International Telecommunication Union (ITU) and the United Nations Development Programme (UNDP), to develop and implement healthcare standards.

Today, there are several e-Health standards developed and promoted by the UN, including the Health Level Seven International (HL7) standard for electronic health records (EHRs) and the International Classification of Diseases (ICD) standard for health data coding and classification.¹⁹⁵ These standards help ensure interoperability between different health systems and facilitate sharing of health data across borders. Developing e-Health standards under the UN has been an ongoing process involving multiple UN agencies to promote using ICTs in healthcare and improve health outcomes worldwide.

The UN Principles on Personal Data Protection and Privacy set out a basic framework for processing “personal data” by, or on behalf of, the UN system organizations in carrying out their mandated activities.¹⁹⁶ They were created by the UN Principles on Personal Data and adopted by the UN system in 2018.¹⁹⁷ These principles include fair

¹⁹⁴ Ibid

¹⁹⁵ Ibid

¹⁹⁶ Personal Data Protection And Privacy Principles, Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018

¹⁹⁷ See <https://unsceb.org/privacy-principles> (accessed 1 April 2023)

processing of personal data.¹⁹⁸ This entails that personal information should be processed for a specific purpose relevant and limited to the intended purpose.

Accordingly, the time for retaining personal information should be specified. Others are the accuracy of personal information, confidentiality during the processing of such information should be of a high degree, risks available to disclosure of such information should be evaluated, and thus, security of personal information should be assured. These principles set out a basic framework for processing personal data, defined as information relating to an identified or identifiable natural person, by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.¹⁹⁹ Some policies and mechanisms observe these principles, as discussed below.

3.3 e-Health Personal Data Protection under Regional Instruments.

Below is a discussion on the regional instruments engaged in the e-Health Personal Data Protection under the Regional Instruments. The Instruments were from the European Union and the African Union where the states of Germany and Tanzania are member states.

3.3.1 The Convention 108+ of the Council of Europe, 2018

Convention 108+ is an updated version of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

¹⁹⁸ Personal Data Protection And Privacy Principles, Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018

¹⁹⁹ Ibid.

The convention aims at strengthening privacy and data protection rights in the digital age. Globally, the Convention 108+ is an important step towards protecting individuals' privacy and personal data in the digital age, and it provides a framework for international cooperation in this area. It establishes the principles for protecting personal data, including the rights of individuals, the obligations of data controllers, and the responsibilities of data protection authorities.

The Convention also includes provisions on the trans-border flow of personal data, ensuring that personal data can be transferred across borders while maintaining adequate levels of protection.²⁰⁰ When the recipient is subject to the jurisdiction of a State or international organization that is not Party to the Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.²⁰¹ This means that if personal data is transferred from a state that has ratified the Convention to a state that has not ratified the Convention, the data controller and processor must take appropriate measures to ensure that the data is protected per the Convention's provisions. Here, the Convention 108+ sets out the framework for international cooperation on data protection, facilitating the exchange of information and best practices among signatory states.

Convention 108+ of the Council of Europe, 2018 applies to the processing of personal data by public and private entities, thereby securing every individual's right to protect their data.²⁰² The Convention applies to all processing of personal data, including the

²⁰⁰ Article 12 (1), (2) and (3) of the Convention 108+

²⁰¹ Article 14(2) +

²⁰² Article 3 Ibid

collection, storage, use, and disclosure of personal data. It applies to all data subjects whose personal data is processed within the territory of a state that has ratified the Convention. It also applies to data controllers and processors established in a state that has ratified the Convention, regardless of where personal data processing occurs.

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular, his right to privacy, concerning the automatic processing of personal data relating to him.²⁰³ It establishes everyone's right to access the data concerning them and to obtain rectification or deletion of these data if they have been processed unlawfully.²⁰⁴ Concerning medical data or data concerning the data subject's health, the convention expressly prohibits such processing unless it is provided for by national law, and such law provides appropriate safeguards.²⁰⁵ As a result, it is unlawful to process medical information about a person unless one has a legal basis to do so, such as an existing doctor-patient relationship.

Convention 108+ lays down principles and guidelines for protecting personal data, which are particularly important in e-Health. The convention recognizes that e-Health systems can collect and process sensitive personal data, such as health data, and it sets out rules to ensure that such data is handled with appropriate safeguards. In this context, the Convention sets out the special categories of data, including racial origin, political opinions, religious or other beliefs, and personal data concerning health or

²⁰³ Article 1 Ibid

²⁰⁴ Article 8 © Ibid

²⁰⁵ Article 6 Ibid

sexual life, which may not be processed automatically unless domestic law provides appropriate safeguards.²⁰⁶

The Convention further provides that such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights, and fundamental freedoms of the data subject, notably the risk of discrimination.²⁰⁷ Every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on automated data processing without considering his or her views.²⁰⁸ Every individual under the Convention has the right to object at any time, on grounds relating to their situation, to the processing of personal data concerning them unless the controller demonstrates legitimate grounds for the processing that override their interests or rights and fundamental freedoms.²⁰⁹

Under the Convention, personal data must be processed fairly and lawfully, and individuals must be informed about how their data is used.²¹⁰ They must also have the right to access their data and have it corrected or deleted if it is inaccurate or incomplete. By providing a common framework for protecting personal data, Convention 108+ helps ensure that individuals' rights are respected and that their data is handled appropriately. This helps to build trust in e-Health systems and encourages their development and use.

²⁰⁶ Article 6(1) Ibid

²⁰⁷ Article 6(2) Ibid

²⁰⁸ Article 9(1)(a) Ibid

²⁰⁹ Article 9(1)(e) Ibid

²¹⁰ Article 5(1)(a)(b) Ibid

3.3.2 EU Data Protection Directive 95/46/EC

Directive 95/46/EC, commonly referred to as the Data Protection Directive, was a European Union law that aimed to protect the privacy rights of individuals in processing their data and to facilitate the free movement of such data within the EU.²¹¹

The EU Parliament and the Council of the EU adopted the Directive on 24 October 1995, which all EU member states implemented by 2000. The Directive 95/46/EC is repealed with effect from 25 May 2018 under Article 94 of the GDPR as law across the EU. However, these directives are important to their historical nature in protecting the rights and freedom of persons to process personal data and the right to privacy of personal information.

The Data Protection Directive's application sphere was quite broad and covered a wide range of activities related to processing personal data. Specifically, the directive applied to data controllers and processors. Also, the directive applied to any operation or set of operations performed on personal data, including collection, recording, organization, storage, retrieval, use, transmission, and erasure. The Data Protection Directive aimed to protect individuals' fundamental rights and freedoms concerning processing their data and ensuring the free flow of data within the EU.

The Directive set out various principles and rules for the processing of personal data, including requirements for obtaining consent, providing individuals with access to their data, and ensuring the security and confidentiality of the data.²¹² It also

²¹¹ Article 5 of The Directive 95/46/EC

²¹² Article 7 (a) of The Directive 95/46/EC

established national data protection authorities in each EU member state to enforce the Directive and handle complaints and breaches.²¹³ It applies to all data processing activities carried out by individuals or organizations, whether public or private, regardless of the technology used. The directives insisted on the protection of individuals concerning processing personal data and the free movement of such data within the EU.²¹⁴ While Directive 95/46/EC does not explicitly address electronic health data, its provisions regarding personal data protection apply to all sectors, including healthcare.

Regarding electronic health data, the directive stipulates that sensitive personal data, such as health data, can only be processed with the explicit consent of the data subject unless certain conditions apply.²¹⁵ The directive also requires appropriate measures to ensure the security and confidentiality of personal data, including health data.²¹⁶ However, this prohibition does not apply where the processing of health data is required, for example, for preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services, and where such data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional confidentiality or by another person also subject to an equivalent obligation of confidentiality.

With Directive 95/46/EC, personal data used in e-Health projects must be processed

²¹³ Article 5 of The Directive 95/46/EC

²¹⁴ Article 3 of The Directive 95/46/EC

²¹⁵ Article 8 of the Directive 95/46/EC

²¹⁶ Article 8 (2) (d) of the Directive 95/46/EC Ibid

fairly and lawfully.²¹⁷ Furthermore, data must be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible way.²¹⁸ The data must be adequate, relevant, and not excessive about the purposes for which they are collected and must be kept in a form that permits identification of data subjects for no longer than is necessary and only for the purposes for which the data was collected or is required for further processing. Data subjects also have to be informed about processing their data.²¹⁹

In connection to the transfer of data between Member States for treatment purposes, in the case of e-Health projects, a data controller established in the territory of one Member State can be sure that in transferring data to another controller established in another Member State, this data will be appropriately protected. This is because the second Member State will provide similar personal data protection.²²⁰ About the transfer of data to third countries, the Directive stipulates that the Member States shall provide that the transfer of personal data that are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with national provisions adopted under the other provisions of the Directive, the third country in question ensures an adequate level of protection.²²¹ This means that the receiving country must have laws and regulations that protect personal data essentially equivalent to the protection provided by EU law.²²²

²¹⁷ Article 6 (1) (a) of the Directive 95/46/EC Ibid.

²¹⁸ Article 6 (1) (f) of the Directive 95/46/EC Ibid.

²¹⁹ Article 6 (1) © of the Directive 95/46/EC Ibid.

²²⁰ Article 25 of The Directive 95/46/EC Ibid.

²²¹ Article 25 (2) of the Directive 95/46/EC Ibid

²²² Article 25 of the Directive 95/46/EC Ibid

Furthermore, the Directive entails that appropriate technical and organizational measures be taken to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, and all other unlawful forms of processing.²²³ However, the Directives allow exceptions to the requirements provided under Article 25 in certain circumstances. Such circumstances include if the data subject has given explicit consent to the transfer or if the transfer is necessary for the performance of a contract between the data subject and controller.²²⁴

The Data Protection Directive was superseded by the GDPR, which strengthened and expanded upon many of the Directive's provisions. However, the principles and rules in the Directive continue to be relevant and have influenced data protection laws and regulations worldwide.

3.3.3 EU's Medical Device Directive (93/42/EEC)

The Medical Device Regulation (MDR) is a European Union regulation that took effect on 26 May 2021. The MDR applies to medical devices placed on the EU market, including electronic health data systems that are considered medical devices. Medical devices may process personal data, such as patient information, during operation. In such cases, the processing of personal data must comply with the GDPR and other relevant data protection laws and regulations. The MDR is designed to ensure high safety and performance for medical devices while maintaining the free movement of medical devices within the EU.

²²³ Article 7 of the Directive 95/46/EC Ibid

²²⁴ Article 27 of the Directive 95/46/EC of the European Parliament and Council of 24 October 1995

The Medical Device Directives define a medical device as any instrument, apparatus, appliance, software, material, or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used especially for diagnostic or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for, among other things, the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease, injury or handicap and the control of conception.²²⁵ When used in an e-Health project, software for general purposes is not a medical device.²²⁶ However, when specifically intended by the manufacturer to be used for one or more medical purposes set out in the definition of a medical device, software is a medical device.²²⁷

In the context of the Directive, manufacturers are obliged to place on the market or to put into service only medical devices that do not compromise the safety and health of patients, users, and other persons when properly installed, maintained, and used per their intended purpose.²²⁸ The manufacturer must design and manufacture medical devices so that some essential requirements are met, such as considering the generally acknowledged state-of-the-art and eliminating or reducing risks as much as possible.²²⁹ The MDR substantially impacts electronic health data because it requires medical device manufacturers to contrivance specific data privacy and security requirements. These requirements apply to electronic health data systems that are measured medical

²²⁵ Article 1(2)(a) of The Medical Device Directive (Council Directive 93/42/EEC

²²⁶ Ibid

²²⁷ Article 1 Ibid.

²²⁸ Article 2 of The Medical Device Directive (Council Directive 93/42/EEC.

²²⁹ General requirement 1 of The Medical Device Directive (Council Directive 93/42/EEC Ibid.

devices, such as software as a medical device and standalone software for medical applied services.

One of the concerns of the MDR regarding electronic health-related data is the necessity for medical device manufacturers to implement a risk management system that includes assessing and mitigating data privacy and security risks. The MDR also requires medical device manufacturers to ensure their devices are designed to protect patient data's confidentiality, integrity, and availability.²³⁰ Generally, while the MDD does not explicitly address personal data protection, medical device manufacturers and distributors must comply with relevant data protection laws and regulations when processing personal data concerning their devices. In this context, the GDPR sets out the main rules and principles for processing personal data in the EU, and medical device manufacturers and distributors must comply with these rules when handling sensitive personal data.

3.3.4 The European Convention on Human Rights (ECHR), 1953

The ECHR is an international treaty established by the Council of Europe in 1950. It was created to protect and promote human rights and fundamental freedoms in Europe. The Convention was signed in Rome on November 4, 1950, and came into force on September 3, 1953. The ECHR is a binding legal instrument that guarantees certain fundamental rights and freedoms to all individuals within the jurisdiction of the Council of Europe. While the Convention does not explicitly mention the right to

²³⁰ Article 20 of the Medical Device Directive (Council Directive 93/42/EEC), *Ibid.*

privacy or personal data protection, it recognizes the right to respect for private and family life and freedom of expression and information.

The ECHR does not mention data protection, as it was drafted before modern data protection regulations began. Nevertheless, the right to respect for private and family life, home, and correspondence, as provided in Article 8 of the Convention, has been interpreted by the European Court of Human Rights (ECtHR) to include a right to data protection. The case against the Republic of Finland was lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by two Finnish limited liability companies. The applicant companies alleged, in particular, that their right to freedom of expression under Article 10 of the Convention had been violated and that the length of the domestic proceedings had been excessive, in breach of Article 6 of the Convention. The court held that under the terms of Articles 8 to 11 of the Convention, several legitimate aims are liable to justify interference in an individual’s manifestation of his or her freedom of expression.²³¹ Generally, the ECHR has played a crucial role in laying the foundation for protecting personal data in Europe, and its principles have been further developed through the adoption of instruments such as Convention 108 and the GDPR.

Under the Convention, any individual who believes that his or her rights in the convention have been breached or interfered with can refer the matter to the European

²³¹ Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, originated in an application (no. 931/13).

Court of Human Rights. The judgments of the Court are binding on the states which are obliged to execute them.²³² The Convention, creates a right to respect for private and family life:

*" Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*²³³

The ECHR has been the starting point of much litigation, with Article 8 being no exception. It is clear from even a simple reading of the Article that it is complex since paragraph 1 sets out the precise rights to be guaranteed, but paragraph 2 provides exceptions to that right. It immediately sets up the expectation that privacy, while central to human rights, is not absolute and must sometimes be balanced against other public interests.

Case law has established that medical records fall within the privacy rights. In this case, a medical advisor was ordered to disclose details from the applicant's medical file during the trial of her husband for manslaughter. According to the Court, it is a key principle that the confidentiality of health data is respected:

*"Any state measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny."*²³⁴

²³² Ibid.

²³³ Art. 8(1)(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

²³⁴ Z v. Finland (9/1996/627/811)

*Z v. Finland*²³⁵ presents a landmark decision in the area of privacy rights. The case involved a Finnish national, identified only as Z, who had been diagnosed with HIV. Z had applied for a job with the Finnish armed forces but was rejected due to his HIV status. Z argued that the decision violated his right to privacy under Article 8 of the ECHR. In its judgment, the ECtHR held that the Finnish government's decision to reject Z's job application violated his right to privacy under Article 8 of the ECHR. The Court noted that the right to privacy includes the right to control information about oneself and to decide whether to disclose it to others. The Court also emphasized that the disclosure of personal information, such as Z's HIV status, can have severe consequences for the individual concerned.

The Court further noted that the government's decision to reject Z's job application was not necessary in a democratic society, as there were other less intrusive means of protecting the health of the armed forces. The Court found that the Finnish government had violated Z's right to privacy under Article 8 of the ECHR. The case of *Z v. Finland* is an important precedent in privacy rights, particularly concerning protecting personal health information. It affirms the importance of the right to privacy in protecting individuals from unwanted disclosure of sensitive information. It highlights the need for governments to carefully balance their legitimate interests with the rights of individuals.

In *Colak and Tsakiridis v. Germany*,²³⁶ a case was brought by two German nationals,

²³⁵ (9/1996/627/811)

²³⁶ no. 77140 and 35493/05 (fifth Section) ECHR 2010/2.

Mr. Colak and Mr. Tsakiridis, who argued that German authorities had violated their privacy rights. The case stemmed from a criminal investigation into an attempted bombing in Cologne, Germany, in 2006. The authorities used covert surveillance measures, including wiretapping and video surveillance, to investigate the case.

Mr. Colak and Mr. Tsakiridis were both subjects of the surveillance measures, and they argued that their privacy rights had been violated. In its judgment on June 9, 2011, the ECtHR found that Germany had not violated the applicants' rights to privacy. The court held that the surveillance measures used by the authorities were necessary and proportionated in the context of a criminal investigation into a serious offence. The court also noted that the measures had been authorized by a judge and had been subject to judicial review.

The court acknowledged that the surveillance measures had interfered with applicants' right to respect their private and family life. Still, it found that this interference was justified by the need to protect the public and prevent crime. The court also noted that the surveillance measures had been limited in scope and duration and that the authorities had taken steps to minimize the impact on the applicant's privacy. Overall, the *Colak and Tsakiridis v. Germany* case highlights the tension between the right to privacy and the need for law enforcement authorities to investigate and prevent crime. The case demonstrates that surveillance measures may be justified in certain circumstances but must be necessary, proportionate, and subject to appropriate safeguards to protect an individual's right to privacy. This was a great decision regarding protection of privacy.

Generally, the European Union has been actively promoting the development of e-Health initiatives to modernize healthcare systems across its member states. By leveraging digital technologies, such as electronic health records, telemedicine, and health apps, the EU aims to enhance access to healthcare services, streamline processes, and empower patients to actively participate in managing their health. This push toward e-Health not only seeks to improve healthcare delivery and patient outcomes but also fosters innovation and collaboration among healthcare professionals and technology developers globally. Thus, this is taken as a great milestone in the development of e-Health regulation in the European Union.

3.3.5 The European Union Data Protection Regulation (EU) 2016/679 (GDPR)

The GDPR is a set of data privacy and protection regulations adopted by the EU in 2016 and came into effect on 25 May 2018. The GDPR replaced the Data Protection Directive of 1995 and is designed to give individuals greater control over their data and to unify data protection regulations across the EU. The EU has implemented one of the most comprehensive and strictest privacy and data protection systems worldwide.

The GDPR is the cornerstone of this system, and it applies to all organizations that process the personal data of individuals residing in the EU, including those involved in e-health. The focus was to make Europe fit for the digital age. The GDPR is directly applicable in all EU member states and also stipulates some opening clauses for local

laws and regulations of each EU member state.²³⁷ The GDPR introduces regulatory solutions that enable stakeholders to shape the exact implementation of privacy obligations based on their specific needs. For example, organizations from one specific sector can jointly define and concretize legal requirements in a Code of Conduct, which can serve as a compliance tool if all regulatory obligations are met.

The GDPR plays a significant role in the development of the law in protecting personal data in e-Health by providing a framework for processing personal data in a manner that protects the privacy and rights of individuals. It imposes strict obligations on organizations that process personal data, including requirements for obtaining valid consent, ensuring data accuracy, and implementing appropriate security measures.²³⁸ The GDPR applies to processing personal data such as health records, medical images, and genetic data.²³⁹ It also regulates data processing from wearable devices, health apps, and other digital health tools.

In this context, the GDPR provides a comprehensive framework for protecting personal data in the context of e-Health with specific provisions to ensure that sensitive health data is collected and processed legally, fairly, and transparently.²⁴⁰ For example, the GDPR requires that personal data be processed lawfully, fairly, and transparently. This means that individuals must be informed about processing their personal data and give their explicit consent before any data is collected or processed.²⁴¹

²³⁷ Article 3 (1) of the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

²³⁸ Article 13 (1) and (2) of the GDPR.

²³⁹ Ibid Article 9.

²⁴⁰ Ibid Article 6 (1) (a).

²⁴¹ Article 5(1)(a).

Further, the GDPR requires that personal data be collected for specified, explicit, and legitimate purposes.²⁴² This means that data collected for e-health must be limited to what is necessary for the specific purpose for which it was collected.²⁴³ It requires that personal data be adequate, relevant, and limited to what is needed concerning the purposes for which it is processed. This means that only the minimum amount of data necessary to achieve the purpose of e-health should be collected and processed.²⁴⁴ Further, the GDPR provides additional protections for sensitive personal data, including health data. This includes requiring explicit consent from individuals before their health data is collected and processed.²⁴⁵

The GDPR gives individuals the right to receive their data in a structured, commonly used, and machine-readable format. This means individuals can receive their e-health data and transfer it to another controller.²⁴⁶ The GDPR further requires that controllers implement appropriate technical and organizational measures to ensure that personal data is processed in a manner that ensures appropriate security.²⁴⁷ This means that e-health systems must be designed with privacy and security from the outset.²⁴⁸ Nevertheless, healthcare delivery systems are subject to strict guidelines on collecting, processing and storing sensitive personal data. The GDPR does not deal exclusively with health information but rather regulates standards for sensitive personal data, indirectly including health-related data.

²⁴² Article 6 (1) (f).

²⁴³ Article 5(1)(b).

²⁴⁴ Article 5(1)(c)

²⁴⁵ Article 9

²⁴⁶ Article 20

²⁴⁷ Article 24 (1)

²⁴⁸ Article 25

3.3.6 European Data Protection Commission, 2018

The European Data Protection Commission is a regulatory body that oversees personal data protection in the EU. It was established in 2018 with the implementation of the GDPR. It is a comprehensive data protection regulation for all EU member states. The main objective of the European Data Protection Commission is to ensure that individuals have control over their data and that it is protected against misuse, abuse, or unauthorized access.²⁴⁹ The commission is responsible for enforcing the GDPR and investigating any complaints or breaches of the law.²⁵⁰ The European Data Protection Commission is crucial in promoting and implementing these standards. It continues developing its policies and guidance to adapt to the changing nature of technology and data use.

The Data Protection Commission at the European²⁵¹ has adopted an interesting document on the processing of personal data relating to health in EHRs.²⁵² This document aims to guide applying the data protection legal framework to electronic health record systems. Analyzing the Data Protection Working Party is necessary since many healthcare deliverers do not always know how to comply with the Data Protection Directive.

²⁴⁹ Article 57 of The General Data Protection Regulation

²⁵⁰ Article 58 of The General Data Protection Regulation Ibid

²⁵¹ See Arts. 29 and 30, 'The 'Data Protection' Directive, Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 No. L281/31. Article 29 sets up a Working Party on the protection of individuals with regard to the processing of personal data, hereinafter referred to as 'the Working Party'. The Working Party advises and makes recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

²⁵² Article 29 Data Protection Working Party, 'Working document on the processing of personal data relating to health in electronic records', WP 131, 15 February 2007.

The data contained in electronic health records or e-health platforms are used increasingly for purposes other than treatment, and healthcare actors are becoming more global. Therefore, more opportunities exist to process health data among several Member States and third parties. There is also the risk that data may be more readily available to a broader circle of recipients.²⁵³ In compiling existing medical information about an individual from different sources, with the result of allowing easier and more widespread access to this sensitive information, EHR systems introduce a new risk scenario.

More categories of people may gain access to data if hospitals, pharmacies, laboratories, sickness funds, etc., that process health data become members of international groups. Article 8(3) of the Data Protection Directive,²⁵⁴ for example, allows for processing by a health professional subject to confidentiality rules for preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services. However, the Working Party believes that Article 8(3) cannot be the sole legal basis for processing personal data in an EHR system. EHR systems provide direct access to a compilation of existing documentation about a person's medical treatment from different sources, such as hospitals and health care professionals, throughout their lifetime.

These systems contravene the traditional boundaries of the patient's direct relationship

²⁵³ Ibid . p. 5 See also the recent European Commission, 'Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health records', C (2008) 3282 final, 2 July 2008, p. 18.

²⁵⁴ The article makes it clear that the compliance with data protection rules shall be subject to control by an independent authority.

with a healthcare professional. Therefore, it is not certain whether health data processing in an EHR system can be allowed without the patient's explicit consent if, under Article 29, a Working Party is not convinced that relying only on the obligation to practice professional confidentiality provides sufficient protection.²⁵⁵ Suppose more people are allowed access to records because European actors keep such records. In that case, more specific safety measures must be taken, and patients must be asked for consent regarding which categories of people may have access to their records.

3.3.7 The Council of Europe in Development of Right to Privacy and Personal Data Protection

The Council of Europe is an international organization that aims to promote and protect human rights, democracy, and the rule of law in Europe. The Council has been actively developing the right to privacy and data protection. The Council plays a vital role in shaping data protection law in Europe and beyond European borders and continues to be a key player in this fast-growing field. In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as the Data Protection Convention. This convention was the first international treaty to address the protection of personal data, and it established basic principles for protecting privacy and personal data, such as the need for consent, purpose limitation, and data quality.

The Council also oversees the work of the ECtHR, which has issued numerous

²⁵⁵ Art. 29 Data Protection Working Party, 'Working document on the processing of personal data relating to health in electronic records', WP 131, 2007 p. 12.

decisions related to the right to privacy and data protection. These decisions have helped to clarify and strengthen the legal framework for privacy and data protection in Europe. The Council of Europe likewise works on additional data protection initiatives, such as guiding on implementing data protection laws and promoting cooperation between data protection authorities. Generally, the Council of Europe plays a significant role in developing and protecting Europe's right to privacy and data protection.

3.3.8 The African Charter on Human and Peoples' Rights, 1981

The African Charter on Human and Peoples' Rights, also known as the Banjul Charter, is a regional human rights treaty adopted by the Organization of African Unity (now the African Union) in 1981. The Charter recognizes the importance of protecting the right to privacy and personal data protection, although it does not provide specific provisions on these issues. The Charter, however, does not have specific provisions that protect personal data under e-Health.

The Charter guarantees respect for private life, family, home, and correspondence.²⁵⁶ This provision encompasses the right to privacy and personal data protection as essential components of an individual's private life. The provision protects individuals from arbitrary or unlawful interference with their private life, including personal data. It requires states to ensure that their laws and practices respect and protect this right.

²⁵⁶ Article 8 of the African Charter on Human and Peoples' Rights, 1981.

The sphere of application of the African Charter on Human and Peoples' Rights includes all African countries that have ratified the Charter.²⁵⁷ As of May 2023, 54 out of the 55 AU member states have ratified the Charter, with only South Sudan being a non-signatory. Further, the Charter applies to individuals, groups, and organizations within African states that have ratified it and to refugees and stateless persons residing in those countries. It also applies to African states' interactions with other states and international organizations.

The Charter also establishes the African Commission on Human and Peoples' Rights.²⁵⁸ The commission is responsible for interpreting and monitoring the implementation of the Charter. It recognizes the right to privacy and personal data protection as fundamental human rights.²⁵⁹ In the context of commission, privacy includes the protection of personal data. It calls for states to ensure that their laws and policies provide adequate safeguards to protect personal data from abuse, misuse, or unauthorized access.

In recent years, some African countries have enacted laws and regulations to protect the right to privacy and personal data protection. For instance, the Tanzania Data Protection Act, no 11 of 2022, sets out the requirements for the protection of personal data in Tanzania, Nigeria's Data Protection Regulation 2019 in Nigeria, while Kenya's Data Protection Act 2019 establishes the legal framework for the protection of personal data in Kenya.

²⁵⁷ Article 1 of the African Charter on Human and Peoples' Rights, 1981 Ibid

²⁵⁸ Article 30 of the African Charter on Human and Peoples' Rights, 1981

²⁵⁹ General Comment No. 4 on the right to privacy in Africa, 2014

Although the African Charter on Human and Peoples' Rights does not have specific provisions on privacy and personal data protection, it recognizes the importance of protecting individuals' private lives, which includes their data. The Charter, coupled with the African Commission's General Comment No. 4, provides a basis for developing laws and policies on privacy and personal data protection across Africa. The increasing adoption of e-Health technologies in Africa, such as electronic health records, telemedicine, and mobile health applications, has led to the collection and processing of vast amounts of personal health information. Data protection laws have been put in place in many African countries to ensure that this information is collected and used in a manner that respects individual's privacy and human rights.

The African Charter on Human and Peoples' Rights plays an essential role in safeguarding the privacy and personal data of individuals in the context of eHealth. By recognizing the importance of privacy as a fundamental human right, the Charter ensures that ethical and human rights principles guide the development and implementation of e-Health technologies.

3.3.9 African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)

The Malabo Convention is a regional treaty adopted by the AU in June 2014 and entered into force in 2021. The treaty aims to promote cybersecurity and data protection across Africa.²⁶⁰ The Malabo Convention provides a framework for

²⁶⁰ Article 2 (1) of the Malabo Convention

protecting personal data and establishes principles and guidelines for processing personal data. One of the key objectives of the Malabo Convention is to ensure that African countries have robust legal frameworks and effective measures in place to combat cybercrime.²⁶¹

Concerning personal data protection, the established mechanism ensures that any form of data processing respects the fundamental freedoms and rights of natural persons.²⁶² The treaty calls for criminalising cybercrimes such as hacking, online fraud, and cyber terrorism and establishes procedures for investigating and prosecuting these crimes.²⁶³

The Malabo Convention provides a framework for African countries to harmonize their cybersecurity and data protection laws, regulations, and practices. The treaty includes provisions that address issues such as cybercrime, data protection, cyber terrorism, online child protection, and international cooperation on cybersecurity. Essentially, the Malabo Convention addresses certain cyber law uncertainties.²⁶⁴ It is the first treaty outside of Europe to regulate personal data protection comprehensively. The treaty calls for establishing national data protection authorities to oversee the handling of personal data and ensure that it is processed according to international best practices.

²⁶¹ Article 8 (1) Ibid

²⁶² Article 8 (2) Ibid

²⁶³ Article 2(2) Ibid

²⁶⁴ See the African Union Convention on Cyber Security and Personal Data Protection adopted during the 23rd Ordinary Session of the Summit of the African Union (2014) ('the Malabo Convention' or 'the Convention') and its predecessor, the Draft African Union Convention on the Establishment of a Legal Framework conducive to Cyber Security in Africa (2012), African Union Commission. The Malabo Convention replaces the provisions of the Abidjan Declaration adopted on 22 February 2012 and the Addis Ababa Declaration adopted on 22 June 2012 on the Harmonization of Cyber Legislation in Africa.

The Convention seeks to establish an appropriate normative framework consistent with the African legal, cultural, economic, and social environment for cyber security and personal data protection within e-commerce and e-transactions.²⁶⁵ In addition, it represents a shared, coordinated African position. It seeks to reflect current legal thinking on processing personal information and its impact on the human rights of privacy, dignity, integrity, personality, and autonomy. Recognizing the increasing interdependence of African states, it calls for concerted action to be taken to protect the rights of individuals and to ‘establish an appropriate normative framework.’²⁶⁶

The Convention requires AU member states to adopt laws and regulations on data protection, establish data protection authorities, and ensure that personal data is collected, processed, and used per the principles of transparency, proportionality, and purpose limitation.²⁶⁷ The convention also requires member states to take appropriate measures to ensure the security of personal data and to provide remedies for individuals whose data has been unlawfully processed or accessed.²⁶⁸

It is important to note that the Malabo Convention defines the objectives of an African information society and strengthens existing legislation in member states and within the regional economic communities. Its adoption seeks to maximize African and international experiences and expertise in cyber legislation and to accelerate relevant reforms in African member states. This will be accomplished by providing a normative

²⁶⁵ See for content on the draft convention of 2012, UJ Orji *Cybersecurity Law and Regulation*, 2012 p. 135.

²⁶⁶ Article 1 of The Malabo Convention.

²⁶⁷ Article 13 principle 3 and 5 Ibid

²⁶⁸ Article 11 (1) (b) Ibid

framework consistent with an African legal, cultural, economic, and social environment. The purpose is to balance the use of information and communication technologies with the protection of the privacy of individuals while guaranteeing the free flow of information across borders, including e-Health records.

The convention also includes provisions on cross-border data flows, data localization, and protecting children's data. It sets out specific obligations for data controllers and processors, including obtaining consent for data processing, ensuring data accuracy, and establishing appropriate technical and organizational measures to protect personal data.²⁶⁹ It outlines the obligations of data controllers and data processors concerning personal data protection. Its scope generally extends to the public and private sectors as well as automated and non-automated processing.²⁷⁰

Further, the Malabo Convention sets out a comprehensive framework for protecting personal data, ensuring that data controllers and processors process personal data fairly, transparently, and securely and that data subjects can exercise their rights concerning their data.²⁷¹ Moreover, the Convention prohibits any data collection and processing 'revealing racial, ethnic, and regional origin, parental affiliations, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject.'²⁷² Exceptions to this prohibition are contained in Article 14 (2) of the Malabo

²⁶⁹ Article 13 principle 1 of the Malabo Convention.

²⁷⁰ Article 20 Ibid.

²⁷¹ Article 13 principle 2 of the Malabo Convention.

²⁷² Article 14 (1) Ibid.

Convention. The categories of sensitive data appear to be limited to only those stipulated within the section.

Concerning data transfer by data controller, the Convention requires data controllers not to transfer personal data to countries outside the AU unless the recipient country can ensure adequate protection.²⁷³ The term adequate level is not defined in the Convention, nor is it determined how the adequacy findings are to be made. The adequacy requirement does not apply to AU member states, irrespective of whether or not they have ratified the Convention, but only to non-AU member countries. Thus, AU member states can adopt any data export provisions they choose regarding each other. Article 9 (1)(c), the Malabo Convention only applies to the processing of data undertaken within the territory of a member state of the AU. Thus, extra-territorial application is not required, but it is not forbidden. Concerning the international movement of personal data, the Convention is therefore consistent in only requiring minimum protection standards while allowing more extensive protections.

Overall, the Malabo Convention is an important step towards promoting cybersecurity and data protection in Africa. By harmonizing laws and regulations and establishing best practices, the treaty aims to ensure that African countries can effectively respond to the growing threat of cybercrime and protect their citizens' data and privacy.

²⁷³ Article 14 (6)(a) Ibid.

3.3.10 African Declaration on Internet Rights and Freedoms, 2014

The African Declaration on Internet Rights and Freedoms is a document that outlines the principles and values that African stakeholders believe should guide the use, access, and governance of the Internet in Africa. It was adopted in 2014 by a group of African civil society organizations, academic institutions, and individuals who came together to address concerns about internet rights and freedoms on the continent. The declaration recognizes that individuals have a right to privacy and that their personal data should be protected.²⁷⁴

The Declaration further recognizes the importance of data protection in promoting and safeguarding individuals' rights.²⁷⁵ The Declaration recognizes that the Internet has become an essential tool for social, economic, and political development in Africa and that its full potential can only be realized if certain rights and freedoms are respected. These include the right to access the Internet, the right to freedom of expression online, the right to privacy and data protection, the right to access information, and the right to participate in governance and decision-making processes related to the Internet.²⁷⁶ The objective of the Declaration is to promote a free, open, and accessible internet in Africa that respects and upholds the rights and freedoms of all individuals.

The Declaration sets principles and guidelines that outline the rights and freedoms that

²⁷⁴ Article 8 and Principle 8 of the African Declaration on Internet Rights and Freedoms, 2014: Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, and are necessary and proportionate in pursuance of a legitimate aim.

²⁷⁵ Ibid.

²⁷⁶ Article 7 of the African Declaration on Internet Rights and Freedoms, 2014

should be protected in the online space in Africa, including e-health delivery services. The sphere of application of the declaration is the entire African continent and all stakeholders involved in the development, deployment, and use of the Internet.²⁷⁷ It also applies to all individuals, including journalists, bloggers, other online content creators, civil society organizations, governments, and Internet service providers.²⁷⁸ Others are stakeholders involved in developing and using the Internet in Africa.²⁷⁹

Thus, the ADIRF is a framework developed to guide African countries in promoting and protecting human rights online. Although the ADIRF does not specifically focus on personal data protection in e-Health, it contains provisions that can be used to develop laws to protect personal data. This is because it recognizes the right to privacy in the digital space where e-Health is practiced.²⁸⁰ This can be used as a basis for developing laws that protect personal data. Accordingly, it recognizes the importance of informed consent in collecting, using, and disclosing personal data.²⁸¹ This can be used to develop laws that require organizations to obtain consent from individuals before collecting and using their data.

The ADIRF also recognizes the importance of security in protecting personal data.²⁸² This can be used to develop laws that require organizations to implement appropriate security measures to protect personal data. It recognizes the right to access

²⁷⁷ Article 2 Ibid.

²⁷⁸ Article 12 Ibid.

²⁷⁹ Ibid.

²⁸⁰ Article 3 Ibid.

²⁸¹ Article 5 Ibid.

²⁸² Article 9 of the African Declaration on Internet Rights and Freedoms, 2014.

information, including personal data.²⁸³ This can be used to develop laws that require organizations to provide individuals with access to their data and to allow them to correct or delete inaccurate information. Moreover, the ADIRF recognizes the importance of independent data protection authorities.²⁸⁴ This can be used to develop laws that establish data protection authorities with the power to enforce data protection laws.

In protecting personal data and privacy in the digital age, the convention sets out principles to guide governments and other stakeholders on the right to privacy protection. It states:

*"Everyone shall have the right to the protection of their personal data, including the right to know what data is being collected, processed, or held, the right to access their personal data, and the right to have it corrected, amended or deleted if it is inaccurate or processed in violation of this Declaration or other relevant national and international standards. Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or where required by law."*²⁸⁵

This article states that individuals have a right to know which personal data is being collected, processed, or held about them. Accordingly, individuals have the right to access, correct, amend, or delete that data if it is inaccurate or processed in violation of the declaration or other relevant national and international standards. To that effect, personal data should only be used for specified purposes, not disclosed or made available for other purposes, except with the data subject's consent or where required

²⁸³ Article 4 and 7 Ibid.

²⁸⁴ Article 11 Ibid.

²⁸⁵ Article 6 of the African Declaration on Internet Rights and Freedoms, 2014.

by law. Therefore, the convention represents a significant step towards ensuring that the internet in Africa is used to promote all users' rights and freedoms.

3.4 e-Health Personal Data Protection under Subregional Instruments.

Belowforth is a discussion on the e-Health Personal Data Protection under subregional instruments. The main subregional organizations were EAC and SADC to which Tanzania is a member. ECOWAS was included to provide practice on other subregional organizations unto which Tanzania is not a member.

3.4.1 e-Health Personal Data Protection under East African Community (EAC)

The EAC is a regional intergovernmental organization of eight (8) Partner States, comprising Burundi, the Democratic Republic of Congo, Kenya, Rwanda, the Federal Republic of Somalia, South Sudan, Tanzania, and Uganda.²⁸⁶ It was originally established in 1967 but collapsed in 1977 due to various challenges, including political differences among member states. However, the EAC was later revived, and the Treaty for establishing the East African Community was signed in 1999, officially coming into force in 2000. The EAC was established to promote economic, social, and political integration among its member states. The EAC has been developing a legal framework for privacy and personal data protection in the region.²⁸⁷

Regional organizations have tried to ensure the right to privacy through data

²⁸⁶Established in terms of the Treaty for the Establishment of the East African Community and later amended in December 2006 and August 2007.

²⁸⁷Established in terms of the Treaty for the Establishment of the East African Community and later amended in December 2006 and August 2007.

protection; nevertheless, the overall legislative framework is not harmonized. It is, however, possible to find some common ground in the legislation. For example, most countries require consent to data access as a necessary condition for data processing. On a legal basis, no references are made to the idea of a legitimate interest as a condition for data processing. Additionally, most statutes have provided for the establishment of a data protection authority reporting to the telecommunications or ICT regulator. Furthermore, there are similar features when data controllers are obliged to notify the regulator of any data processing activities and to seek authorization from the regulator to transfer personal data to third countries.²⁸⁸

Harmonizing the data protection statutory and privacy regulatory framework in East Africa is still on the agenda of regional organizations and some states. In addition to protecting individual's right to privacy, having a harmonized or, at best, a uniform framework is seen as an opportunity to promote the continent's development by allowing the free flow of data within East Africa and Africa in general, encouraging data transfers from other continents to Africa and thus boosting the use of African-based datacenters, outsourcing services, blockchain technology, e-government, and fintech services. The reformation of regulatory principles is based primarily on transparency, flexibility, regional harmonization, proportionality, and legal certainty as core concepts underpinning regulatory frameworks in other similarly integrated regions.²⁸⁹

²⁸⁹East African Community East African Legislative Assembly Report of the Committee on communications, trade and investments on the on-spot assessment of regional cooperation in ICT November 2013 p. 9.

The EAC has taken significant steps to protect the privacy of its citizens and promote the responsible use of personal data in the region. Adopting the Data Protection and Privacy Framework Law and the various awareness and education initiatives are essential to achieving this goal. The EAC has also increased public awareness and education on privacy issues through various initiatives, including workshops, training programs, and public campaigns. These efforts aim to empower individuals to exercise their privacy rights and make informed decisions about using their data.

Although EAC member countries have to ensure that their domestic legislation complies with the Community's Cyber Laws Framework, they have been at various stages in developing their national privacy and cyber legislation and have been slowly and steadily making progress at their own pace. Subsequently, harmonization has become a more pressing policy issue, with support from UNCTAD's e-Commerce and the Law Reform Programme focused on the East Africa Community. The EAC is increasingly interested in using e-Health technologies to improve regional healthcare delivery. As part of this effort, the EAC has been working to establish a legal and regulatory framework for e-Health that includes provisions for protecting personal data.²⁹⁰ The EAC has recognized that the use of e-Health technologies requires the collection and processing of personal data.

3.4.2 e-Health Personal Data Protection under SADC

The Southern African Development Community (SADC) is a regional

²⁹⁰ <https://www.eac.int/press-releases/147-health/2966-eac-set-to-develop-health-data-governance-in-foster-digital-transformation-of-the-health-sector-in-east-africa> accessed 26 December 2023

intergovernmental organization comprising 16 Member States in Southern Africa. SADC was established in 1980 and comprises Angola, Botswana, the Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Seychelles, Tanzania, Zambia and Zimbabwe.²⁹¹ Southern African Development Community (SADC) Model Law of 2012 provides a framework for protecting personal data in the region. These model law emphasize the importance of transparency, accountability, and the rights of individuals to control their data.²⁹² SADC aims to promote the harmonization and standardization of legal instruments within the region and improve cooperation between member states, including developing electronic technology.

SADC has recognized the importance of privacy and data protection in the region and has taken steps to promote and protect these rights. In the context of e-Health, the SADC has not yet established a region-wide guideline for implementing eHealth. However, individual member states of SADC may have their guidelines and policies related to e-Health.²⁹³

The strategy was developed in response to the increasing demand for better access to healthcare services, particularly in rural and remote areas where traditional healthcare delivery models are limited. The strategy includes strengthening health information systems, increasing telemedicine access, and promoting mobile health (mHealth)

²⁹¹ Declaration and Treaty of SADC as revised in 1992.

²⁹² Personal Data Protection Guidelines for Africa, See internetsociety.org

²⁹³ SADC Model Law on Data Protection 2012.

technologies.²⁹⁴ Since adopting the strategy, SADC has supported several e-Health initiatives, including developing EHR systems and establishing telemedicine networks. SADC has also collaborated with international organizations, such as the WHO and AU, to promote e-Health in the region.

SADC considers data protection fundamental to any individual's development by creating a synergy between data protection and privacy protection as the concern of every human being. This goes hand in hand with the development of technologies that process and store significant personal data. Data protection regulations among the SADC countries should work to ensure the benefits of using information and communication technologies do not at any point weaken the protection of personal data, particularly sensitive personal data like health-related information. In 2018, SADC adopted the SADC Declaration on Cyber Security of 2012. The declaration emphasizes the need for member states to develop and implement comprehensive cybersecurity policies and frameworks that include provisions for the protection of personal data and privacy.

The SADC Model Law on Data Protection provides a framework for member states to develop data protection laws consistent with international best practices. The model law includes provisions for the collection, use, and storage of personal data, the rights of data subjects and the obligations of data controllers and processors. SADC has also established the SADC Model Law on Data Protection 2012, which focuses on

²⁹⁴ Ibid

developing data protection and privacy regulations to facilitate cross-border data flows and promote regional integration.

Regarding privacy and data protection legislation, SADC member states, namely, Seychelles, Mauritius, Angola, Lesotho, and South Africa, have adopted comprehensive data privacy legislation.²⁹⁵ Model laws at the regional level ensure that the widespread use of ICT does not result in the concurrent weakening of personal data protection and privacy of such information. It seeks to give effect to the principles of data protection by limiting the processing of personal data. Moreover, its purpose is to combat violations of privacy arising from the unlawful or unfair collection, processing, transmission, storage, and use of data activities.

3.4.3 e-Health Personal Data Protection under ECOWAS

Although Tanzania is not a member of ECOWAS, but ECOWAS has been selected for the purpose of understanding how other regional organizations practice on matters of e-Health on Personal Data Protection. Within the ECOWAS space, it is prohibited to obtain and process data that reveals the racial, ethnic, or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sexual life, genetic data, or more generally data on the state of health of a data subject within the ECOWAS region.²⁹⁶ Economic Community of West African States ECOWAS is a regional economic union in West Africa consisting of 15 West African countries,

²⁹⁵ Makulilo, A.B., 'Myth and reality of harmonization of data privacy policies in Africa' 31 *Computer Law & Security Review*, 2015, p. 86

²⁹⁶ Article 30 Supplementary Act on Personal Data Protection within Ecowas, 2010.

which are Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.²⁹⁷ It was established to promote economic cooperation and integration among its member states. In recent years, ECOWAS has taken steps to develop the right to privacy and personal data protection within its member states.

In particular, each Member State must establish a legal framework for protecting personal data relating to collecting, processing, transmitting, storing, and using personal data.²⁹⁸ The Act aims to protect individuals' fundamental rights and freedoms concerning the processing of their data.²⁹⁹ The Act sets out principles and guidelines for collecting, using, storing, and disclosing personal data by public and private entities within the ECOWAS region.³⁰⁰

In addition, ECOWAS has established the ECOWAS Cyber Security Program to strengthen cybersecurity measures and protect personal data in the region. Each Member State should develop a qualified human workforce trained in different aspects of cybersecurity by introducing training courses in the various areas relating to cybersecurity technical and legal in its teaching programs, promoting the enhancement of cybersecurity skills among all information and communication technology professionals and promoting research and innovation in the field of cybersecurity.³⁰¹ The program includes initiatives such as capacity building, policy development, and

²⁹⁷ See <https://www.ecowas.int>.

²⁹⁸ Article 2 of the Supplementary Act on Personal Data Protection within ECOWAS, 2010.

²⁹⁹ Article 38 Ibid.

³⁰⁰ Article 23 to 30 Ibid.

³⁰¹ ECOWAS Regional Cybersecurity and Cybercrime Strategy, 2021 Sub-objective 2.7.

information sharing to improve cybersecurity practices across ECOWAS member states.

The Supplementary Act on Personal Data Protection within ECOWAS establishes a comprehensive framework for protecting personal data in ECOWAS member states, including collecting, processing, storing, and transferring personal data.³⁰² This includes e-Health records. The Act applies to any individual, government, local authority, or public or private legal entity that collects, processes, transmits, stores, or uses personal data, any automated or non-automated processing of data that is contained or may be included in a file, any processing carried out in a West African Economic and Monetary Union ('UEMOA') or ECOWAS Member State, and any processing of data related to public security, defence, investigation and prosecution of criminal offences or State security, subject to such exemptions as are defined by specific provisions stipulated in other legal texts that are in force.³⁰³

The Act states that the content of the data protection laws in individual states should be influenced very strongly by the EU Directive and that a data protection authority should be established.³⁰⁴ The data protection authority must be independent and responsible for ensuring that personal data is processed in compliance with the provisions of the Act.³⁰⁵ The data protection authority must ensure that ICTs do not threaten public liberties and privacy.³⁰⁶ It sets out the rights of individuals concerning

³⁰² Article 2 of the Supplementary Act on Personal Data Protection within ECOWAS, 2010.

³⁰³ Article 3 Ibid.

³⁰⁴ Article 14(1) Ibid.

³⁰⁵ Article 14(2) Ibid.

³⁰⁶ Article 19 Ibid.

their data, including the right to access, rectify, and delete their data.³⁰⁷ It also requires organizations to obtain consent from individuals before collecting and processing their data and to implement appropriate security measures to protect personal data from unauthorized access, use, and disclosure.³⁰⁸

The Act requires that personal data should not be kept longer than required for the purposes for which they were obtained or processed.³⁰⁹ It explicitly prohibits collecting and processing data revealing the racial, ethnic, or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sexual life, genetic data, or generally, data on the state of health of a data subject within the ECOWAS region.³¹⁰ In addition to the Supplementary Act, the ECOWAS has established the ECOWAS Cyber Security Program to enhance the capacity of member states to address cyber threats and protect critical information infrastructure. This program focuses on data protection and privacy, with initiatives aimed at promoting awareness and building the capacity of member states to implement effective data protection frameworks.

ECOWAS has taken significant steps to address the challenges posed by the rapid growth of digital technologies and the need to protect personal data in the region. The organization's initiatives in this area are essential for promoting privacy and security, fostering trust in the digital economy, and promoting regional integration and

³⁰⁷ Article 38 Ibid.

³⁰⁸ Article 24 of the Supplementary Act on Personal Data Protection within ECOWAS, 2010.

³⁰⁹ Article 25(3) Ibid.

³¹⁰ Article 30 Ibid.

economic development. Generally, West Africa has a developed legal framework for privacy protection at a sub-regional level, with the strongest developments in Africa emanating from ECOWAS.³¹¹ Compared to other sub-regions within Africa, ECOWAS is described as Africa's most vibrant and dynamic sub-regional.³¹² Of the 15 member states of ECOWAS, as of today, eight have adopted Data Protection Laws, namely, Benin, Burkina Faso, Cape Verde, Senegal, Togo Ghana, Nigeria, and Niger, with Ivory Coast and Mali having data protection legislations, which are in force and have established data protection regulators.³¹³

Generally, no specific and unified ECOWAS instrument is dedicated to e-Health data protection. However, it's essential to note that regional organizations like ECOWAS often collaborate with member states to address e-Health and data protection issues. Data protection and privacy issues in e-Health fall under broader regional and national legal frameworks. ECOWAS member states always have regulations and policies that address data protection in the context of electronic health records and healthcare systems. Additionally, some countries in the region align their legislation with global standards, such as the GDPR in the EU.

3.5 Foreign Practice from other Jurisdictions

South Africa,³¹⁴ has a robust e-Health policy aimed at leveraging technology to improve healthcare delivery and accessibility, as outlined in its National Health

³¹¹ Greenleaf, G., Ibid. p. 18

³¹² Banjo, A., 'The ECOWAS Court and the Politics of Access to Justice in West Africa' 32 (1) *CODESRIA Africa Development* 2007, p.70

³¹³ Data Guidance Africa Advisory 'Africa: Regional disparity in the adoption of privacy laws revealed' April 2015. p. 1.

³¹⁴ National Digital Health Strategy for South Africa, 2019-2024.

Normative Standards Framework for Interoperability in e-Health. Kenya's Vision 2030 places significant emphasis on e-Health as a means to achieve universal healthcare.³¹⁵ The country has implemented initiatives like the Kenya Health Information System to digitize health records and improve data management.³¹⁶ Nigeria's National Health ICT Strategic Framework aims to harness ICT for improved healthcare delivery, including initiatives like the National Health Management Information System and the National Electronic Health Policy.³¹⁷

Ghana's e-Health Strategy prioritizes the use of technology to enhance healthcare delivery and improve health outcomes, with initiatives like the District Health Information Management System in place.³¹⁸ Zambia,³¹⁹ focuses on addressing the health sector challenges and accelerating progress towards attainment of the national and global health goals, aimed at ensuring equitable access to quality healthcare to all in Zambia, as close to the family as possible, Leaving no one behind.

3.6 Conclusion

Protecting personal data has long been recognized as a fundamental aspect of the right to privacy. Privacy is a fundamental right that both international and regional benchmarks must protect. The GDPR is one of the most comprehensive and strict privacy laws globally, and it was adopted by the EU in 2018. The comprehensive regulation sets out the EU's rules for protecting personal data. It applies to all

³¹⁵ Kenya Health Policy, 2014-2030.

³¹⁶ Kenya National eHealth Policy, 2016-2020.

³¹⁷ National Health ICT Strategic Framework, 2015-2020.

³¹⁸ National e-Health Strategy, 2010-2015.

³¹⁹ National Health Strategic Plan 2022–2026.

organizations, including healthcare providers, that process the personal data of EU citizens. The GDPR provides individuals with several rights, including the right to be informed about the processing of their data, the right to access their data, the right to rectify inaccurate data, the right to erasure, and the right to object to processing.

The Africa regional benchmark on privacy and personal data protection emphasizes respecting individuals' privacy rights and ensuring they are protected in an increasingly digital world. Accountability should be in the law and regulations regulating the process of personal data and protecting individuals' rights, including the right to privacy and entailing the process of personal data. Any law, policy, or regulation that contradicts such right shall be considered null and void. Both instruments are important to the development of e-Health because they provide a legal framework for processing personal data in the healthcare sector. This framework protects individuals' privacy while allowing healthcare providers to use personal data to improve patient care. By providing clear rules for processing personal data, these instruments help build trust in e-Health services and facilitate the development of innovative digital healthcare solutions.

CHAPTER FOUR

PROTECTION OF PERSONAL DATA IN e-HEALTH IN GERMANY

4.1 Introduction

This chapter presents and analyses Germany's legal framework for e-Health personal data protection. It presents Germany's socio-economic context to explain how e-Health was established. The chapter focuses on Germany's legal framework for e-health data protection, designed to ensure the privacy and security of health-related data in electronic systems. It comprises various laws and regulations governing personal health information collection, storage, processing, and sharing. This chapter forms an important part of best practices and experiences that can be considered in crafting Tanzanian e-Health law.

4.2 The Context of Germany in the e-Health System

Germany is seen as a global pioneer in data protection for various reasons. It was the first European country to have passed a data protection act at the state level in Hessen in 1970 and the federal level in 1978 as the *Bundesdatenschutzgesetz* or BDSG.³²⁰ Once the GDPR was finalized in 2016, Germany was among the first countries in Europe to revise its local data protection law, the BDSG. An updated and reformed BDSG-Neu was introduced as early as July 2017—a year ahead of the 25 May 2018 deadline for the GDPR.³²¹

³²⁰ Kim, A., “Privacy and data protection in India and Germany: A comparative analysis”, WZB Berlin Social Science Center, 2020

³²¹ Ibid

The German medical device market is believed to be one of the most lucrative healthcare markets worldwide.³²² Germany had a strong economy, with a strong manufacturing sector and high levels of exports. It has a fine-established social welfare system, which includes universal healthcare, strong social protection programs, and a well-functioning social security system.³²³

Germany's socio-economic context is characterized by a strong economy, a functioning welfare state, a skilled workforce, and a commitment to sustainable development. These factors contribute to Germany's global competitiveness and reputation as a prosperous and socially responsible nation. In addition, it has a developed social market economy, combining elements of free market capitalism and a strong welfare state. Germany follows the principles of a social market economy, which aims to balance economic growth with social welfare.³²⁴ It combines a competitive market system with extensive social benefits and protections. The government plays an active role in regulating the economy, ensuring fair competition, and providing social security.

Germany's health care system originates from the mutual aid societies created in the early 19th century.³²⁵ The German social benefits system is based on the concept of social insurance as embodied in the principle of social solidarity.³²⁶ This principle is a

³²² Miriam, B., et al, "Germany Healthy system summary",2022

³²³ Ibid

³²⁴ Watrin, C., "The Principles of the Social Market Economy — Its Origins and Early History." *Zeitschrift Für Die Gesamte Staatswissenschaft / Journal of Institutional and Theoretical Economics*, vol. 135, no. 3, 1979, pp. 405–25. JSTOR, <http://www.jstor.org/stable/40750151>. Accessed 31 May 2023.

³²⁵ See <https://healthsystemsfacts.org/national-health-systems/bismarck-model/germany/germany-health-system-history>.

³²⁶ Nilmin, W., et al, "Critical Issues for the Development of Sustainable E-health Solutions" Springer, 2012.

firmly held belief that the government must provide a wide range of social benefits to all citizens, including medical care, old age pensions, unemployment insurance, disability payments, maternity benefits, and other forms of social welfare.³²⁷

Germany has a comprehensive social welfare system that provides its citizens with a wide range of benefits. This includes universal healthcare coverage, generous pensions, unemployment benefits, and various social assistance programs.³²⁸ The welfare system is financed through a combination of employer and employee contributions, as well as general tax revenues.³²⁹ Germany has a relatively low level of income inequality compared to many other developing countries like Tanzania. The government of Germany is implementing policies to ensure a fair distribution of wealth and promote social cohesion.³³⁰ Progressive taxation, minimum wage laws, and strong labour protections contribute to reducing income disparities.

In Germany, digital technologies play an essential role in the fast growth of the electronic healthcare delivery system. Since 2018, the German Ministry of Health has passed legislation to digitalize the country's healthcare delivery system. The legislation expands the possibilities for e-Health in Germany.³³¹ In this context, patients have seen several innovations that were new to them or even to the practising doctors. The innovations included healthcare apps, video chats between patients and doctors, and

³²⁷ Goran, R., (et al), "Comparisons of Health Care Systems in the United States, Germany and Canada", Masta Sociomed, 2012.

³²⁸ Freye, M., et al. 'Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzanian and German eHealth system.' *Datenschutz Datensich* 44, 393–397 (2020).

³²⁹ *Ibid*

³³⁰ *Ibid*

³³¹ *Ibid*.

electronic record databases.³³²

Accordingly, telemedicine services have gained momentum in Germany, especially after the COVID-19 pandemic. It allows patients to consult with healthcare providers remotely, reducing the need for in-person visits. Telemedicine offers benefits such as increased accessibility, convenience, and improved efficiency in healthcare delivery.³³³ In addition, Germany has seen the rise of various mobile applications designed to support health and wellness, manage chronic conditions, and promote healthy lifestyles.³³⁴ These apps can monitor vital signs, provide health information, remind patients to take medications and offer personalized recommendations.³³⁵ Efforts are underway to establish secure platforms for exchanging health data among healthcare providers, laboratories, pharmacies, and other stakeholders.³³⁶ The aim is to improve care coordination and enable timely access to patient information across different healthcare settings. From the foregoing, Germany's health is digital and is set to transform its healthcare delivery system from reactive to predictive care. In general, there is great progress in the e-Health framework in Germany. However, the main concern is protecting patients' data privacy under e-Health.

To address this concern, the government of Germany introduced a nationwide

³³² Zakim, D., "Development and significance of automated history-taking software for clinical medicine, clinical research and basic medical science", *Journal of Internal Medicine*, Volume 280, 2016.

³³³ *Ibid.*

³³⁴ Thomas, F., "Home care in Germany during the COVID-19 pandemic: A neglected population?", *Journal of Nursing Scholarship*, Volume 29, 2022.

³³⁵ Rosenlund M., "The Use of Digital Health Services Among Patients and Citizens Living at Home: Scoping Review". *J Med Internet Res*. 2023.

³³⁶ Cao W., "A mobile health application for patients eligible for statin therapy: app development and qualitative feedback on design and usability". *BMC Med Inform Decis Mak*. 2023.

electronic health record system known as the "*Elektronische Gesundheitsakte*" (ELGA).³³⁷ The system aims to centralize patients' health data, including medical history, diagnoses, prescriptions, and other relevant information, accessible to authorized healthcare professionals. In Germany, personal data protection in healthcare is an essential component of confidence building between patients and service providers. To this extent, protecting patients' data is a crucial requirement. This is because e-Health data contain highly personal information about the patient, which is associated with an enormous potential for discrimination.

More importantly, telemedical care involves a large number of service providers who are considered third parties in the processing of the data.³³⁸ Thus, it is the patient, doctor, and service providers as a third party. Medical confidentiality, also known as doctor-patient confidentiality, is a legal obligation in Germany. Medical confidentiality is rooted in ethical standards and protected by law. Confidentiality is one of the core duties of any medical practitioner. It makes clear that any medical practitioner has a mandatory duty to keep a patient's personal health information private unless consent to give out the particular information is sought and provided.³³⁹

Medical confidentiality is all about privacy and respecting patient's personal health

³³⁷ September 2021.

³³⁸ Weichert, in: Kühling/Buchner (eds.), DSGVO/BDSG (2nd edition 2018), Art. 9 marginal no. 38.

³³⁹ Maehle AH., et al., "Medical confidentiality in the late nineteenth and early twentieth centuries: An Anglo-German comparison". *Medizinhist J.* 2010. The similarity of German and English doctors' attitudes to the issue of confidentiality may be explained by similar notions of medical professional honour. Clearly, doctors were keen to preserve medical secrecy as an integral part of their professional identity. At the same time, they were committed to protecting their patients' honour by guaranteeing the privacy of the doctor-patient encounter. Conflicts of duty, and of honour, occurred when disclosure served to protect a third party, e.g. the spouse and children of patients with VD. In such a situation the honorable path, at least for some doctors, could be to breach confidentiality and to warn contacts.

information. The starting point for the personal data protection framework concerning e-Health is that personal and medical information given to a healthcare provider will not be disclosed to others unless the individual has given specific consent for such release. This legal duty of the professional is reflected in section 9 of the Professional Code for Physicians and section 203 of The German Criminal Code (*Strafgesetzbuch*). This provision gives German doctors the right to refuse to give evidence in court about their patients' information.

These exceptions usually occur when there is a significant public health risk or a patient's life is in danger. In such cases, healthcare professionals may have a legal and ethical duty to disclose relevant information to the appropriate authorities. Confidentiality generally encourages open and honest communication between patients and healthcare providers. Patients are more likely to provide accurate and detailed information about their health condition, symptoms, and lifestyle choices if they know their information will remain confidential.

As e-Health technologies continue to advance, ensuring the protection of personal health data is of paramount importance. Health data contains sensitive information about individuals' medical conditions, treatments, and genetic information. Thus, protecting privacy is essential to maintaining patient trust and complying with data protection regulations. More importantly, e-Health systems and networks need secure security measures to prevent unauthorized access, data breaches, and cyberattacks.

Safeguarding data integrity and confidentiality is vital to maintaining the

trustworthiness of digital health platforms. Patients should have control over their health data and be able to provide informed consent for its use. Clear policies and mechanisms for obtaining and managing consent are necessary to ensure transparency and respect for individuals' autonomy. E-Health data are subject to legal and ethical regulations, including compliance with data protection laws such as the GDPR in the EU. Protecting e-Health data helps ensure compliance with these regulations and avoids potential legal issues. A robust data protection framework enhances trust in e-Health technologies among patients, healthcare providers, and other stakeholders. Trust is crucial for the widespread adoption and effective utilization of e-Health solutions, leading to improved healthcare outcomes.

Germany has established an infrastructure of outstanding hospitals, research centres, and specialized clinics.³⁴⁰ This infrastructure provides an ideal environment for testing and implementing innovative medical technologies and treatments. Additionally, Germany has a regulatory framework that ensures the safety and efficacy of medical devices and treatments. The German government recognizes the importance of innovation in healthcare and provides significant support and funding for research and development activities.³⁴¹ Public funding agencies, such as the Federal Ministry of Education and Research (BMBF) and various research grants and initiatives, encourage innovation and help drive advancements in medical technology and treatment.

³⁴⁰ Cologne, Germany: Institute for Quality and Efficiency in Health Care. Health care in Germany: The German health care system. 2015 (accessed 17/8/2023).

³⁴¹ Ibid.

As one of Europe's leading economies, Germany has a solid socio-economic context characterized by a highly developed healthcare system, advanced technological infrastructure, and a robust data privacy and protection focus.³⁴² The country places great importance on maintaining the privacy and security of personal data, especially in the context of e-Health protection. E-Health protection is not viewed as a stand-alone issue but as an integral part of the broader general privacy and data protection framework. This approach recognizes the sensitivity and significance of personal health data while enabling the benefits of digital healthcare technologies. This approach ensures that individuals can trust the healthcare system and have confidence in the confidentiality and integrity of their data. In this context, general data protection is discussed to provide the basis for developing e-Health personal data.

4.3 e-Health Card System

The rapid growth of information and communication technologies in the past years has led to the increased use of the internet and electronic devices to search and monitor health-related data, communicate with health professionals, and manage personal health records. The development of e-Health in Germany has been a significant focus driven by the need for efficient healthcare delivery, improved patient outcomes, and cost containment to ensure the community is connected and patients are empowered and encouraged. Germany introduced the electronic health card, the "*Elektronische Gesundheitsakte*" (eGK), as a central element of its e-Health infrastructure.

³⁴² Ibid.

The eGK stores patient data, including insurance and medical information, and facilitates secure and interoperable data exchange among healthcare providers. Until 2004, the health insurance card in Germany typically included basic information about the insured individual and their health insurance coverage.³⁴³ This card served as a credential for patients to access healthcare services within the German healthcare system. Germany has a social health insurance system that requires all residents to have health insurance coverage. Individuals can choose between statutory or private health insurance depending on their income and other factors.³⁴⁴

Due to limitations in the storage and application of these insurance cards, the government proposed the extension of the insurance cards to the electronic health card (EHC), which was finally implemented in 2006. Insured individuals received a health insurance card that contained basic information about the person and their insurance coverage. This card is presented when seeking healthcare services from doctors, hospitals, and pharmacies. The goal is to provide health services and patient information access through information technology.³⁴⁵ It is noted that Germany strongly emphasises the development of e-Health, an ongoing process with various stakeholders working to address technical, regulatory, and cultural challenges. The COVID-19 pandemic has accelerated some aspects of digital transformation in healthcare, and it will be interesting to see how these trends continue to evolve in the coming years.

³⁴³Tugce, S., 'New governance of the digital health agency: a way out of the joint decision trap to implement electronic health records in Germany?' *Healthy Economics Policy and Law*, 2023.

³⁴⁴*Ibid.*

³⁴⁵*Ibid.*

4.4 Legal and Regulatory Framework in Germany

The legal framework for e-Health data protection in Germany comprises a combination of EU regulations, national laws, and specific healthcare acts. These regulations emphasize the importance of protecting health data, ensuring patient consent, and maintaining data security standards. The framework provides a comprehensive structure for data protection in the digital healthcare landscape, enabling the secure and responsible use of health information.

4.4.1 Europe

4.4.1.1 The European Data Protection Regulation (EU) 2016/679 (GDPR)

The GDPR is a set of data privacy and protection regulations adopted by the EU in 2016 and came into effect on 25 May 2018. The GDPR replaced the Data Protection Directive of 1995 and is designed to give individuals greater control over their data and to unify data protection regulations across the EU. The EU has implemented one of the most comprehensive and strictest privacy and data protection systems worldwide.

The GDPR is the cornerstone of this system, and it applies to all organizations that process the personal data of individuals residing in the EU, including those involved in e-health. The focus was to make Europe fit for the digital age. The GDPR is directly applicable in all EU member states and also stipulates some opening clauses for local laws and regulations of each EU member state.³⁴⁶ The GDPR introduces regulatory

³⁴⁶ Article 3 (1) of the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

solutions that enable stakeholders to shape the exact implementation of privacy obligations based on their specific needs. For example, organizations from one specific sector can jointly define and concretize legal requirements in a Code of Conduct, which can serve as a compliance tool if all regulatory obligations are met.

The GDPR plays a significant role in the development of the law in protecting personal data in e-Health by providing a framework for processing personal data in a manner that protects the privacy and rights of individuals. It imposes strict obligations on organizations that process personal data, including requirements for obtaining valid consent, ensuring data accuracy, and implementing appropriate security measures.³⁴⁷ The GDPR applies to processing personal data such as health records, medical images, and genetic data.³⁴⁸ It also regulates data processing from wearable devices, health apps, and other digital health tools.

In this context, the GDPR provides a comprehensive framework for protecting personal data in the context of e-Health with specific provisions to ensure that sensitive health data is collected and processed legally, fairly, and transparently.³⁴⁹ For example, the GDPR requires that personal data be processed lawfully, fairly, and transparently. This means that individuals must be informed about processing their personal data and give their explicit consent before any data is collected or processed.³⁵⁰

³⁴⁷ Article 13 (1) and (2) of the GDPR.

³⁴⁸ Ibid Article 9.

³⁴⁹ Ibid Article 6 (1) (a).

³⁵⁰ Article 5(1)(a).

Further, the GDPR requires that personal data be collected for specified, explicit, and legitimate purposes.³⁵¹ This means that data collected for e-health must be limited to what is necessary for the specific purpose for which it was collected.³⁵² It requires that personal data be adequate, relevant, and limited to what is needed concerning the purposes for which it is processed. This means that only the minimum amount of data necessary to achieve the purpose of e-health should be collected and processed.³⁵³ Further, the GDPR provides additional protections for sensitive personal data, including health data. This includes requiring explicit consent from individuals before their health data is collected and processed.³⁵⁴

The GDPR gives individuals the right to receive their data in a structured, commonly used, and machine-readable format. This means individuals can receive their e-health data and transfer it to another controller.³⁵⁵ The GDPR further requires that controllers implement appropriate technical and organizational measures to ensure that personal data is processed in a manner that ensures appropriate security.³⁵⁶ This means that e-health systems must be designed with privacy and security from the outset.³⁵⁷ Nevertheless, healthcare delivery systems are subject to strict guidelines on collecting, processing and storing sensitive personal data. The GDPR does not deal exclusively with health information but rather regulates standards for sensitive personal data, indirectly including health-related data.

³⁵¹ Article 6 (1) (f).

³⁵² Article 5(1)(b).

³⁵³ Article 5(1)(c)

³⁵⁴ Article 9

³⁵⁵ Article 20

³⁵⁶ Article 24 (1)

³⁵⁷ Article 25

Germany has integrated the GDPR into its national law through the Federal Data Protection Act (*Bundesdatenschutzgesetz* - BDSG). This act complements and specifies the GDPR's provisions, ensuring alignment with German legal principles. Germany has a strong emphasis on data protection and privacy rights. It has a Data Protection Authority (DPA) in its federal states, overseeing compliance with data protection laws. Generally, Germany's approach to privacy issues aligns with the stringent requirements of the GDPR, reflecting a strong commitment to protecting individuals' data and privacy rights.

The GDPR significantly emphasizes transparency, accountability, and the responsibility of organizations when handling personal data.³⁵⁸ Such data must be processed lawfully and legally, transparently and fairly. In addition, the data processed must have a purpose limitation, be accurate, and be for minimum use. Accordingly, data must be kept for a certain period when necessary, and confidentiality must be observed.³⁵⁹ The processing of data and further processing of data already collected are generally prohibited unless the data subject has effectively consented to the processing.³⁶⁰ Since Health data is a special personal detail collection, processing is generally prohibited unless certain measures have been taken.³⁶¹

A data subject is entitled to request access to and obtain a copy of their data, with prescribed information about how the controller has used the data.³⁶² Data subjects

³⁵⁸ Article 3(2) of the GDPR.

³⁵⁹ Article 5 (1) Ibid.

³⁶⁰ Article 6 (1) Ibid.

³⁶¹ Article 9 (2) Ibid.

³⁶² Article 15 Ibid.

further enjoy a right to restrict the processing of their data in defined circumstances. These include where the accuracy of the data is contested, where the processing is unlawful, where the data are no longer needed to save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.³⁶³

In particular, extra caution should be taken when health data is being processed. These companies have a responsibility towards their consumers to protect their data and to inform them in an intelligible and easily accessible form of what data is being processed, why it is being processed, and by whom. Additionally, Germany's national laws and regulations complement the GDPR and address specific aspects of patient data protection. These may include laws related to healthcare, medical confidentiality, and data protection in healthcare settings.

4.4.2 General Law

4.4.2.1 The Basic Law for the Federal Republic of Germany, 1949

The German Constitution does not explicitly address privacy and personal data protection in the same way as some other national constitutions or international treaties. However, it provides a framework the German courts interpret to guarantee certain privacy rights and serves as a general basis for personal data protection laws. In this context, the Constitution establishes the transparency of human dignity as the highest constitutional principle. This principle has been interpreted to include the

³⁶³ Article 18 Ibid.

protection of privacy, which forms the basis for the fundamental right to informational autonomy.³⁶⁴ To this juncture, people have all the right and the power to decide when and, how and to what extent their personal information, particularly sensitive information, is published. Electronic health comprises services like health information networks, electronic health records, telemedicine services, consumer health informatics, healthcare information systems, and health knowledge management.

The German Constitution laid the foundation for privacy and data protection in e-Health. It establishes the framework for legislation and legal principles that promote individual rights, including the right to privacy, the protection of personal data, and medical confidentiality.³⁶⁵ These constitutional provisions, subsequent laws, and court decisions have shaped the development of privacy and e-Health in Germany. This right has been interpreted to encompass privacy and personal data protection in the digital age.³⁶⁶

The Constitution grants individuals the authority to collect, store, and use their data, including health data.³⁶⁷ This provision establishes human dignity as inviolable. It forms the foundation for protecting an individual's privacy and personal integrity, including their health-related information.³⁶⁸ The Constitution further safeguards the confidentiality of correspondence, posts, and telecommunications. It protects the

³⁶⁴ Article 1 of German Constitution.

³⁶⁵ Article 3 Ibid.

³⁶⁶ Article 2 Ibid.

³⁶⁷ Article 2, Paragraph 2 Ibid.

³⁶⁸ Article 1, Paragraph 1 Ibid.

privacy of electronic communications, including e-Health systems and platforms.³⁶⁹ Medical confidentiality is a vital aspect of privacy in healthcare. The German Constitution recognizes the importance of medical confidentiality and further protects the secrecy of correspondence, posts, and telecommunications. The Medical Confidentiality Act obligates healthcare professionals to maintain patient confidentiality.³⁷⁰ This provision protects the occupational freedom of individuals, including healthcare professionals. It is relevant to developing e-Health by protecting professional autonomy and confidentiality obligations in the healthcare sector.

The Federal Constitutional Court of Germany (*Bundesverfassungsgericht*) has significantly developed privacy and e-Health through its decisions. The Court is known for its emphasis on protecting fundamental rights and ensuring the constitutionality of laws and regulations. In the context of privacy and e-Health, the Court's decisions have profoundly impacted how these issues are addressed in Germany. For example, in 1983, the Constitutional Court ruled that the 1983 census law was unconstitutional because it violated the right to informational self-determination.

The Court held that individuals can control their data, and data collection must be proportional and legitimate.³⁷¹ With this decision, the Federal Constitutional Court created a constitutional right to informational self-determination. This landmark

³⁶⁹ Article 10 Ibid.

³⁷⁰ Article 12 Ibid.

³⁷¹ Hornung, G., "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", *Computer Law & Security Review* 25, 2009.

development resulted from an equally significant civil movement against mass data collection of citizens in the 1980s. In these anti-census protests in West Germany, protestors questioned the need for the number and kind of questions posed in the census. Some protesters resorted to not answering the questions, while others accidentally damaged the forms or wrote illegibly.³⁷²

This decision laid the foundation for protecting privacy in the digital age and has implications for data collection in e-Health systems. The court placed constitutional protection over personal data in Germany and recognized individual control over the amount and extent of use of their data. It prohibited the creation of citizen profiles with unique identifiers and even the sharing of data between government departments after a one-time collection. The decision led to the amendment of the BDSG in 1990, where the court's decisions and observations were taken into account in the form of building consent requirements, transparency, and prevention of abuse by government agencies.³⁷³

The Court further ruled on the constitutionality of telecommunications surveillance measures. The Court emphasized the importance of protecting private communications and held that surveillance measures must adhere to strict legal criteria to prevent abuse. This decision is relevant to protecting medical data and patient confidentiality in e-Health systems.³⁷⁴ In 2015, the Court addressed the issue of storing patient data in

³⁷² Hannah, G., "Dark Territory in the Information Age: Learning from the West German Census Controversies of the 1980s, 2010.

³⁷³ Volkszählungsurteil (Census Decision) – 1983.

³⁷⁴ Telecommunications Surveillance Decision – 2008.

electronic health cards. It ruled that patients have the right to informational self-determination, and any collection and storage of medical data must be voluntary and transparent. This decision influenced the design and implementation of e-Health systems in Germany to ensure patient privacy and data protection.³⁷⁵

The Federal Constitutional Court (*Bundesverfassungsgericht*) in Germany has significantly shaped the country's approach to privacy and e-Health. One landmark ruling by the German Constitutional Court was the Patient Data Protection Act case of 2020.³⁷⁶ In this case, among other issues, the Federal Constitutional Court examined the constitutionality of certain provisions of the Patient Data Protection Act, which aims at facilitating the use of patient data for research purposes while safeguarding individual privacy rights.³⁷⁷ The law allowed the transfer of patient data to centralized databases for research purposes without obtaining explicit patient consent.³⁷⁸ The court ruled that the provisions of the law were unconstitutional because they violated the right to informational autonomy protected under the German Constitution.³⁷⁹ The court emphasized that individuals have the right to decide whether and to what extent their health data is used for research purposes and that any interference with this right must be justified by a legitimate purpose and be proportionate.

The decision significantly impacted the development of privacy and e-Health in Germany. It strengthened the importance of individual privacy rights in the context of

³⁷⁵ Patient Data in Electronic Health Cards Decision – 2015.

³⁷⁶ *Emmett v. Eastern Dispensary and Casualty Hospital*, 396 F.2d 931 (1967).

³⁷⁷ *Ibid.*

³⁷⁸ *Ibid.*

³⁷⁹ *Ibid.*

healthcare data. It emphasized the need for unambiguous and informed consent from patients when their data is used for research. The ruling encouraged policymakers to return to and revise the legislation to ensure stronger protection of patient privacy while enabling responsible data use for medical research and advancements in e-Health. These constitutional provisions and accompanying legislation collectively form the legal framework that guides the development of privacy and e-Health in Germany. They aim to balance facilitating technological advancements in healthcare while safeguarding individuals' privacy rights and ensuring the security and self-control of their sensitive personal data.

4.4.2.2 German Federal Data Protection Act, 2017

The German Federal Data Protection Act (BDSG), revised in 2017, was a significant update to the country's data protection laws. It was developed in response to the EU's GDPR, which aimed to harmonize data protection laws across the EU member states.³⁸⁰ The BDSG provides a legal framework for private and public entities to process personal data, ensuring that individuals have control over their personal information and that their rights are respected.³⁸¹ The Act applies to the processing of personal data within the territory of Germany, regardless of whether the processing entity is located within or outside the country.³⁸²

The Act incorporates the principles of the GDPR, including lawfulness, fairness,

³⁸⁰See https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html accessed January 6, 2024.

³⁸¹ Section 45 of Federal Data Protection Act 2017.

³⁸² Section 1 Ibid.

transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.³⁸³ The Act includes regulations regarding the processing of sensitive personal data,³⁸⁴ including medical diagnosis, the provision of health or social care or treatment, or the management of health, and that appropriate and specific measures shall be taken to safeguard the interests of the data subject.³⁸⁵ The Act stipulates that health-related data should be treated with particular care and imposes strict requirements on its processing, storage, and transmission.³⁸⁶ This Act establishes basic data protection principles, such as the requirement of legal permission or the data subject's consent for any processing of personal data.³⁸⁷

The Act defines electronic health data as any information concerning the patient's personal or material circumstances of an identified or identifiable natural person. Consequently, personal electronic health data exists if the information is related to a named individual and if the individual's identity can only be concluded from the circumstances.³⁸⁸ The Act encourages the collection and processing of only the necessary personal data. Data controllers should ensure that the data they collect is adequate, relevant, and limited to what is necessary for the intended purposes.³⁸⁹ The Act emphasizes the importance of obtaining informed and voluntary consent from individuals before processing their data.³⁹⁰ Personal data should be collected for specified, explicit, and legitimate purposes and should not be further processed in a

³⁸³ Section 47 (4) and (5) Ibid.

³⁸⁴ Section 22 Ibid.

³⁸⁵ Section 48 (1) and (2) Ibid.

³⁸⁶ Section 22 (2) of Federal Data Protection Act 2017.

³⁸⁷ Section 51 Ibid.

³⁸⁸ Section 46 (14) Ibid.

³⁸⁹ Section 47 (2) and (3) Ibid.

³⁹⁰ Section 51 Ibid.

manner incompatible with those purposes.³⁹¹ The Act further requires such personal data to be processed to ensure appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.³⁹²

Data controllers are required to provide individuals with information about collecting, processing, and using their data. This includes details about the purposes, recipients, and duration of data processing.³⁹³ Organizations must implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, destruction, or alteration.³⁹⁴ The Act grants individuals certain rights, including access to personal data,³⁹⁵ rectifying inaccurate data, deleting data under certain circumstances,³⁹⁶ and objecting to or restricting data processing.³⁹⁷ In some instances, organizations must appoint a data protection officer (DPO) to ensure compliance with data protection laws and act as a point of contact for individuals and supervisory authorities. The DPO oversees data protection compliance and acts as a point of contact for data subjects and supervisory authorities.³⁹⁸

Additionally, the Act stipulates that the Data Protection Officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified unless they are released from this obligation by

³⁹¹ Section 47 (2) Ibid.

³⁹² Section 47 (6) Ibid.

³⁹³ Section 55 Ibid.

³⁹⁴ Section 45 of Federal Data Protection Act 2017.

³⁹⁵ Section 57 Ibid.

³⁹⁶ Section 58 Ibid.

³⁹⁷ Ibid.

³⁹⁸ Section 5 Ibid.

the data subject and have the right to refuse to give evidence under certain conditions.³⁹⁹ The DPO must maintain secrecy and confidentiality regarding the identity of individuals whose personal data is being processed. This means the DPO cannot reveal data subjects' identities to anyone without proper authorization or legal grounds.

Germany's national legislation implements the GDPR within the country's legal framework. While the BDSG largely aligns with the principles and standards the GDPR sets, it also includes specific provisions to address Germany's legal and cultural context. These provisions help to ensure a more tailored approach to data protection that reflects the country's unique circumstances. It is important for organizations operating within Germany or processing individuals' data in Germany to be aware of the Act's requirements in addition to the GDPR. This dual framework ensures that data protection regulations are effective and suitable for the country's specific needs while maintaining consistent personal data protection across the European Union and Germany.

4.4.2.3 Telecommunication Telemedia Data Protection Act, 2021

In addition to the GDPR and other laws, the Telecommunication Telemedia Data Protection Act, which became effective on 1 December 2021, governs communication services and networks. It merges the data protection regulations in Telemedia and telecommunications law, previously scattered across a wide range of German laws.

³⁹⁹ Section 7 Ibid.

The provisions of the Telemedia Act (TMG) and the Telecommunications Act (TKG) have been repealed and combined into the new Act.⁴⁰⁰

The Act protects confidentiality and privacy when using internet-ready terminal infrastructure such as websites, messenger services, or smart home devices. It also focuses on regulating privacy in electronic communications, addressing various aspects such as ambiguities regarding cookies, data retention, interception of communications, and confidentiality of communication services. The Act addresses the use of cookies and tracking technologies on websites. It requires website operators to inform users about the use of cookies, provide options for consent, and offer mechanisms for users to control tracking preferences.⁴⁰¹ The Act is designed to complement and clarify the implementation of EU Privacy directives within Germany, particularly concerning cookies and related technologies. The provisions covering cookies and similar technologies are also covered.⁴⁰² They apply to any storage of information on the end equipment of users as well as any access to such information. As a general rule, the Act states that such storage or access is only permitted if the end-user gives consent based on clear and comprehensive information. GDPR shall apply for such consent and the information provided.⁴⁰³

The Act contains definitions for data types related explicitly to providing telecommunications and telemedia services to inventory and usage data.⁴⁰⁴

⁴⁰⁰ Section 25 the Telecommunication Telemedia Data Protection Act of 2021.

⁴⁰¹ Section 26 Ibid.

⁴⁰² Section 25 of the Telecommunication Telemedia Data Protection Act of 2021.

⁴⁰³ Section 26(1) Ibid.

⁴⁰⁴ Section 1 (3) Ibid.

Telecommunications laws typically require service providers to obtain users' explicit consent before collecting, processing, or disclosing their data.⁴⁰⁵ The consent should be freely given, specific, informed, and revocable. Personal data collected by telecommunications providers should be used only for specific and legitimate purposes. It mandates that users be informed about collecting, processing, and using their data. Users must also give explicit consent for using their data, and they have the right to access, correct, and delete their data. Providers should not retain data longer than necessary to provide services unless required by law.⁴⁰⁶

The Act requires that special information be provided in the case of commercial communications. In the case of commercial communications, which are Telemedia or parts of Telemedia, service providers must observe that the commercial communications must be identifiable.⁴⁰⁷ The Act further regulates who is obligated to respect the secrecy of telecommunications. In addition to publicly available telecommunications services, the section also includes providers of telecommunications services offered wholly or partly on a business basis.⁴⁰⁸ The Act requires telemedia service operators to provide clear and easily accessible information about their identity and contact details on their websites or platforms. This ensures transparency and enables users to identify and contact the service provider easily.

⁴⁰⁵ Section 25 (1) Ibid.

⁴⁰⁶ Section 25 (2) Ibid

⁴⁰⁷ Section 6(1) of the Telecommunication Telemedia Data Protection Act of 2021.

⁴⁰⁸ Section 3(2) Ibid.

4.4.3 Specific Legislation

4.4.3.1 Development of e-Health Law

Recognizing the importance of health digitalization, Germany passed the first e-Health law of its history in 2015.⁴⁰⁹ The objectives of the Law were to promote the use of EHRs and improve data protection in the healthcare sector. While the law primarily focused on facilitating the digitization of healthcare processes, it also incorporated provisions to safeguard privacy and protect personal data. Its primary focus was advancing digital healthcare services in Germany while ensuring personal data protection and compliance with data protection regulations, including the GDPR.

The law aims to promote digital tools and technologies in healthcare to enhance patient care and improve the efficiency of healthcare services. It includes provisions that address various aspects of digital health, such as electronic health records, telemedicine services, and digital prescriptions, all while upholding strict data privacy and security standards. This emphasis on data protection is crucial to maintaining patient trust and ensuring that sensitive medical information remains confidential and secure.

With the introduction of e-Health law, Germany tried to create an appropriate framework to balance health benefits and data protection issues. The law outlines a roadmap to build a nationwide digital infrastructure, aims to facilitate access to health information, and governs the introduction of new digital applications. While the first

⁴⁰⁹ Weeks, L. C., et al “‘A scoping review of research on complementary and alternative medicine (CAM) and the mass media : looking back, moving forward.’ BMC Complement Altern Med, 3.

new services, such as remote consultation, emergency data storage, electronic medication plan, and electronic physician's letter, have been rolled out, the most significant changes are imminent.⁴¹⁰ In Germany, as in many other countries, the digitalization of healthcare systems has led to the need for robust legal frameworks to protect individuals' privacy and personal data in the context of e-Health services.

Germany is known for its strong data protection laws, which have had significant implications for e-Health services. The emergence of the GDPR, which applies across the European Union, sets stringent standards for collecting, processing, and storing personal data. E-Health laws in Germany must align with GDPR requirements to ensure patient data is handled lawfully and transparently. In Germany, the concept of moving from paper-based health records to electronic records is not an old concept. The recent idea is due to the fast development of computers and technologies. However, the use of electronic health records is voluntary. This means that healthcare providers and patients can choose whether or not to adopt EHRs.

However, as the benefits of EHRs become more apparent, many healthcare organizations and professionals are recognizing the advantages of making the switch. It became certain that using paper-based health records (data) may generate an extensive paper trail. Hence, there is great interest in moving from paper-based health records to EHRs.⁴¹¹ The transition from paper-based health records to EHRs has been relatively recent, driven by advancements in computer technology and the desire to

⁴¹⁰ Van der Haak, M., et al ' Data security and protection in cross-institutional electronic patient records.' *International Journal of Medical Informatics*, 2003, 70(2).

⁴¹¹ Ibid.

streamline healthcare data management. This transition has been observed not only in Germany but also in many other countries around the world. EHRs allow for quicker and easier access to patient information.

Healthcare providers can retrieve patient data instantly, reducing the time spent searching through physical files. It enables seamless sharing of patient data between different healthcare facilities and providers, leading to better coordination of care. This is especially important in cases where multiple specialists treat a patient. Over time, the costs of managing and storing paper-based records can become significant. EHRs can potentially reduce these costs by eliminating the need for physical storage space and reducing administrative tasks.

Indeed, digitalization is having a significant impact on the field of medicine and healthcare around the world. Like many other countries, Germany has been experiencing the effects of this digital revolution in healthcare. E-Health is gaining increasing importance in Germany. As a result, this concerns awareness of patient rights and more transparency, as well as essential questions of personal data protection and the technical-organizational security of data processing. The German legislature published the draft Patient Data Protection Act in April 2020 to deal with this process.⁴¹² The digitization of patient records allows for better information sharing among healthcare providers and reduces the risk of errors due to illegible handwriting or lost paperwork.

⁴¹² Available at: <https://www.bundesgesundheitsministerium.de/pdsg.html> (last accessed February 6, 2022).

4.4.3.2 Digital Health Care Act, 2019

Given the increasing importance of data security and privacy in the healthcare sector, it would not be surprising for governments to introduce regulations emphasising data protection standards for healthcare providers and digital health companies. Many countries worldwide have been working to update their healthcare and data protection laws to address the unique challenges of digital health technologies and collecting and storing sensitive health-related data.

Germany's healthcare system has made significant progress, thus bringing in the legislative framework for digitalising the healthcare delivery approach, basically with the electronic patient record. Germany has also played an important role in e-Health. It is the first country in the World to have a combination of regulatory and reimbursement processes for e-Health applications.⁴¹³ Germany has invested in digital healthcare infrastructure to improve patient care, data exchange, and healthcare efficiency. The country has been working on establishing a secure electronic network called the Telematics Infrastructure to connect healthcare providers, hospitals, pharmacies, and health insurance companies. This infrastructure aims to facilitate the secure exchange of patient data and improve care coordination.

One notable piece of legislation related to digital health in Germany is the Digital Healthcare Act, which was passed in November 2019 and came into effect on January 1, 2020. The law was designed to catalyze the digital transformation of the German

⁴¹³ McKinsey, T., 'Digitizing Healthcare Opportunities for Germany.', 2018.

healthcare system, which has historically been a laggard in that area among peer countries. In addition to promoting the use of telehealth and ensuring better usability of health data for research purposes, the new law entitles all individuals covered by statutory health insurance to benefits for certain digital health applications.⁴¹⁴ The Act encourages the digitization of healthcare delivery services in Germany while addressing personal data protection concerns.⁴¹⁵ The Act further emphasizes the importance of data security and requires healthcare providers and digital health companies to comply with strict data protection standards. The Act introduced a dedicated pathway enabling reimbursement of digital health offerings in Germany, bringing more transparency into the approval process for manufacturers, patients, and physicians.⁴¹⁶

Digital health applications are being prescribed by healthcare professionals and reimbursed by health insurance companies.⁴¹⁷ These applications can range from mobile apps to wearable devices, and they must meet specific criteria to be eligible for reimbursement. The goal is to improve patient care, support remote monitoring, and enhance access to healthcare services. Digital health applications become essential in the hands of patients. With the fast development of digital apps, doctors can collect patient data quickly and make disease treatments more quickly. The legal framework is designed so DiGA can support aspects of patient-centred care, such as strengthening

⁴¹⁴ Dittrich F., 'Digitalisierung: Back DA. The Digital Healthcare Act - a Turning Point in the German Digitization Strategy?' *Z Orthop Unfall*. 2021.

⁴¹⁵ *Ibid*.

⁴¹⁶ Lorenzo D'Angelo., et al '2 Years After Germany's Regulation for Digital Health Apps, What Can We Learn?', Guest Column; 2022.

⁴¹⁷ Lauer, W., '[Digital health applications (DiGA): assessment of reimbursability by means of the "DiGA Fast Track: procedure at the Federal Institute for Drugs and Medical Devices.' *Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz*. 2021.

self-management, health literacy, and adherence, and optimize treatment procedures and interactions between patients and service providers in many ways. Digital applications are eligible for a fast access way, in which data protection, data security, transparency, and ease of use are evaluated.⁴¹⁸ It focuses, in particular, on developing the electronic health card and the corresponding electronic patient file for statutory health and insured people. The protection extends to data stored in such files against unauthorized use, creating a secure telematics infrastructure, improving healthcare IT systems' interoperability, and providing telemedical services.⁴¹⁹

The Act also promotes the implementation of electronic patient records to enable secure and comprehensive sharing of patient information among healthcare providers. It gives patients the right to decide which healthcare professionals can access their data.⁴²⁰ The provision ensures the protection of patient data in the context of digital health applications. It emphasizes the importance of data privacy and security and requires manufacturers to comply with strict data protection standards. Patient consent and control over personal health data are central to the legislation.⁴²¹ The Act enables statutory health insurance funds to cover the costs of certain digital health applications if they meet the required safety, quality, and efficacy criteria. This inclusion in health insurance coverage aims to make digital health tools more accessible and affordable for patients.⁴²² The Act expanded the telematics infrastructure within the health sector.

⁴¹⁸ Ibid.

⁴¹⁹ Mittermaier M., '[Practical use of digital health applications (DiGA) in internal medicine].' *Internist (Berl)*. 2022.

⁴²⁰ Section 4(1) of the Digital Health Care Act, 2019.

⁴²¹ Section 4 Ibid.

⁴²² National Association of Statutory Health Insurance Physicians. Coronavirus: videosprechstunden unbegrenzt möglich. https://www.kbv.de/html/1150_44943.php (2020).

According to the new act, patients should be able to use digital services such as electronic patient files nationwide. Therefore, the new Act obliges pharmacies to connect to the telematics infrastructure by the end of September 2021 and hospitals by 1 January 2022. Midwives, physiotherapists, and nursing and rehabilitation facilities may join the ‘telematics infrastructure’ and be reimbursed for that voluntary connection.⁴²³

Moreover, the Act strengthens the use of remote/video consultations by patients, which have been legal in Germany since 2017. The German Act on Advertising for Therapeutic Products will be amended to allow patients' use of remote/video consultations. This amendment will allow patients to find doctors who offer remote/video consultations more easily. The Act aimed to facilitate the digital exchange of patient data between healthcare providers, health insurance companies, and other relevant stakeholders. However, there were concerns about the potential misuse or inadequate protection of sensitive patient data. The act did include provisions for data protection, but there were still worries about data breaches or unauthorized access.⁴²⁴

A comprehensive digital healthcare system requires significant infrastructure, technology, and training investments. The Act, however, did not address the potential challenges that healthcare providers and institutions might face during the transition to digital systems. Insufficient funding and lack of clarity on responsibilities for

⁴²³ Section 134(2) of the Digital Health Care Act, 2019.

⁴²⁴ Section 291 (4) Ibid.

implementation could hinder the successful adoption of digital healthcare solutions. Accordingly, the Act aimed to involve patients in their healthcare decisions and provide them access to their health data. However, there were concerns that the act did not emphasize sufficient patient involvement in developing and implementing digital health solutions. A lack of user-centric design and limited patient empowerment could undermine the effectiveness and acceptance of digital healthcare services.⁴²⁵ In 21st-century healthcare delivery services, there has been a growing emphasis on patient-centred care, shared decision-making, and the use of EHRs to facilitate access to health data. Various initiatives and regulations in Germany have been implemented to promote these principles.

4.4.3.3 The German Patient Data Protection Act, 2020

On 3 July 2020, Germany's Federal Parliament, the Bundestag, passed the Patient Data Protection Act or *Patientendaten-Schutz-Gesetz* (PDSG). The Act is a specific law in Germany that focuses on protecting patient data in the healthcare sector, and its application includes hospitals, doctors, health insurance providers, and pharmacies using services the applications and components of the German healthcare systems which process patients' information.⁴²⁶ It covers various aspects of data protection, including electronic health records, telemedicine, and health data exchange. The Act states that insured persons can also choose to have access to data to retrieve the prescription provided to them by the doctor as a printout on paper.⁴²⁷

⁴²⁵ Section 303 (5) Ibid.

⁴²⁶ Section 306(2) and section 307 of the German Patient Data Protection Act, 2020.

⁴²⁷ Section 342 (1) Ibid.

The Act came out as a way of pushing further the digitalization of the German healthcare delivery system. The Act introduces several innovative digital applications, clearly points out the importance of protecting the patient's personal health information stored in an electronic format, and emphasizes patients' sovereignty regarding their health-related information.⁴²⁸ The Act further marks the comprehensive telematics infrastructure regulations and their application.⁴²⁹

The service providers are responsible if they use components of their decentralized infrastructure for authentication and secure data transmission to the central infrastructure if they are involved in deciding on means of data processing. This also applies to properly commissioning, maintaining, and using the components. The service providers who have to use certain services, applications, and components of the Telematik to process e-prescriptions or access the electronic patient record must take appropriate technical and organizational measures where necessary.⁴³⁰

The application of the Act has introduced several changes. For instance, health insurance providers must offer clients electronic patient files, whereas patients will have the power to decide which information to store in the files and who can have access.⁴³¹ According to the Act, service providers are responsible if they use components of their decentralized infrastructure for authentication and secure data transmission to the central infrastructure and if they are involved in deciding on means

⁴²⁸ Section 340 Ibid.

⁴²⁹ Ibid.

⁴³⁰ Section 307 (1) Ibid.

⁴³¹ Section 342 (1) Ibid.

of data processing.⁴³² Some documents are provided in hard copies. By applying the Act, all these documents will be digitalized and added to the German digital healthcare system that supports communication between patients and healthcare providers. However, doctors can create electronic prescriptions, sign them, and add them to the telematics system. With this application, patients can access electronic prescriptions from their doctors and medicine at the pharmacy of their choice.⁴³³

For processing personal data with the coming specialist applications, the PDSG clarifies data protection responsibility. To this end, the Telematic infrastructure is broken down into decentralized, central, and application infrastructure.⁴³⁴ The service providers are responsible if they use components of their decentralized infrastructure for authentication and secure data transmission to the central infrastructure if they are involved in deciding on means of data processing. This also applies to proper commissioning, maintenance, and use of the components.⁴³⁵

The providers who must use certain services, applications, and components of the Telematic to process e-prescriptions or access the electronic patient record must take suitable and appropriate technical and organizational measures where necessary. The justification for the legislation draft mentions, for example, securing Telematic connectors against unauthorized access and appropriate state-of-the-art encryption standards.⁴³⁶ The Act marks a milestone in the digitalization of the healthcare system

⁴³² Section 307 (1) Ibid.

⁴³³ Section 361 Ibid.

⁴³⁴ Section 306 (2) Ibid.

⁴³⁵ Ibid.

⁴³⁶ Section 307 (1) Ibid.

in Germany. It also means a huge amount of highly sensitive data will be made available in an electronic format for the first time. It will likely attract the attention of malicious outsiders and tempt insiders to sensitive data. Healthcare institutions must face the challenges of this large-scale digitalization and be prepared to protect patient information as it goes virtual.

4.5 Personal Data Protection Institutions in Germany

In Germany, several institutions are dedicated to protecting e-Health data. Federal Ministry of Health This ministry sets the legislative framework and guidelines for e-Health data protection in Germany. It oversees healthcare policies and regulations, including those related to data protection in the health sector. The GDPR created the concept of the lead supervisory authority. In a situation where the cross-border exchange and processing of personal data is involved, the starting point for enforcement is that processors and controllers are regulated by and answerable to the supervisory authority for their involvement in personal data transactions.⁴³⁷ However, there must be a corporation with other concerned authorities in other member states.⁴³⁸

Germany does not have one centralized supervisory authority for data protection law, but authorities in every federal state are competent in respective states and specific areas such as religious communities.⁴³⁹ Each German state has its data protection authority responsible for enforcing data protection laws within its jurisdiction. These

⁴³⁷ Article 56(1) of the General Data Protection Regulation.

⁴³⁸ Article 56(2) Ibid of the GDPR.

⁴³⁹ DLA Piper's Data Protection Laws of the World Handbook, 2023. This is twelfth edition and now provides an overview of key privacy and data protection laws across more than 100 different jurisdictions.

authorities oversee compliance with data protection regulations, including those related to e-Health data. The Ministry of Health is responsible for formulating and implementing healthcare policies in Germany. They play a role in regulating e-Health systems and ensuring data protection in the healthcare sector. Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests are met. It is a public authority that processes operations that, by their nature, scope, or purposes, require regular and systemic monitoring of data subjects on a large scale; its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings can appoint a single data protection officer responsible for multiple legal entities.⁴⁴⁰ Further, the data protection officer must be easily accessible from each establishment⁴⁴¹ and have expert knowledge⁴⁴² of data protection laws and practices. However, it is possible to outsource the Data Protection Officer role to a service provider.⁴⁴³ Another good example is the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The restructuring above of an independent supreme federal authority comes at a time of immense challenges for data protection. The legal framework for data protection will undergo serious modification based on the agreement on the European Data Protection Regulation.⁴⁴⁴ This is an independent federal authority responsible for overseeing data protection in Germany.

⁴⁴⁰ Article 37(2) of the GDPR.

⁴⁴¹ Ibid.

⁴⁴² Article 37(5) Ibid.

⁴⁴³ Article 37(6) Ibid.

⁴⁴⁴ Andreas, F., 'German Federal Commissioner for Data Protection and Freedom of Information.' 2015: <https://www.linkedin.com/pulse/german-federal-commissioner-data-protection-freedom-fillmann>.

They monitor compliance with data protection laws and guide on data protection issues related to e-Health.

Since the e-Health care system relies heavily on exchanging sensitive medical information, ensuring data privacy and security is crucial. Strong measures are implemented to protect patient data, comply with privacy regulations, and maintain the confidentiality of personal health information. Hospitals' implementation of e-health systems has increased rapidly over the past several years. As the healthcare industry was digitized to keep up-to-date, the healthcare industry could not acquire electronic security features at the same speed, leading to vulnerabilities in e-health systems.⁴⁴⁵ If patients lack trust in EHRs and health information exchanges (HIEs), feel that the confidentiality and accuracy of their electronic health information are at risk, and may not want to disclose health information,⁴⁴⁶ Withholding their health information could have life-threatening consequences. This is one reason why ensuring the privacy and security of health information is so important.

The trust between patients and health information technology plays a significant role in improving healthcare outcomes. When patients feel comfortable and confident in sharing their health information through technology, healthcare providers can access a more comprehensive view of their health history, treatments, and ongoing care. In addition, health information breaches can have serious consequences for

⁴⁴⁵ Gabriel M. H., 'Data Breach Locations, Types, and Associated Characteristics Among US Hospitals,' *American Journal of Managed Care*, vol. 24.

⁴⁴⁶ Section 28(b) of the Digital Provision Act.

organizations, including reputational and financial harm or harm to your patients. Poor privacy and security practices increase the vulnerability of patient information in your health information system, also increasing the risk of a successful cyber-attack.

It is important to maintain accurate information in patients' records, to make sure patients have a way to request electronic access to their medical records and know how to do so, carefully handle patients' health information to protect their privacy, ensure patients' health information is accessible to authorized representatives when needed. In this context, protecting patients' privacy and securing their health information stored in an EHR is a core requirement of the Medicare and Medicaid EHR Incentive Programs.⁴⁴⁷ EHR developer is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR. Effective privacy and security measures help you meet meaningful use requirements while supporting the clinical practice to meet the required personal data protection measures.

It has been observed that providing access to EHRs is a vital next step in activating patients in their care and improving the health system.⁴⁴⁸ However, this opens new security threats. There is a genuine concern about people's and entities' access levels to patients' EHRs. A patient's EHR might be fragmented and accessible from several sites by visiting different doctors' offices, hospitals, providers, etc. Security defects in some of these systems could cause the disclosure of information to unauthorized

⁴⁴⁷ Anckar, C., 'On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research.' *International Journal of Social Research Methodology*, 2008.

⁴⁴⁸ *Ibid.*

persons or companies, and health data need protection against manipulations, unauthorized accesses, and abuses, which includes taking into account privacy, trustworthiness, authentication, and responsibility and availability issues.⁴⁴⁹

Despite all the benefits, EHRs also have difficulties maintaining data privacy to the extent that administrative staff can access information without the patient's explicit consent and how and to what extent information about them is communicated to others.⁴⁵⁰ Hackers, viruses, and worms can seriously threaten security and privacy in EHRs. Many reports of accidental loss or the theft of sensitive clinical data have appeared recently.⁴⁵¹ Knowing the security and privacy features of EHR systems could be critical if these risks are to be confronted and measures to increase the data protection of EHRs are to be adopted. These modernisation efforts aim to improve healthcare outcomes, enhance patient experience, and increase the efficiency and effectiveness of healthcare delivery services in Germany and globally. This is highly achieved in Germany by using information and communication technologies in the fast-growing e-healthcare delivery system that aims to transform the healthcare landscape and meet the changing needs of patients and healthcare practitioners.

4.6 Conclusion

The GDPR, the EU regulation enacted in 2018, governs personal data protection in Germany. In addition to the GDPR, Germany has national data protection regulations

⁴⁴⁹ Blank, R. H., 'Comparative health policy (4th ed. ed.).' Basingstoke: Palgrave Macmillan. 279. 2014.

⁴⁵⁰ Ibid

⁴⁵¹ Ibid

regulating privacy and personal data. These regulations aim to protect the privacy and rights of individuals concerning their data and set high standards for data handling and processing by organizations and businesses operating in Germany.

Organizations must implement data protection principles from the design stage of any new processes, systems, or services that involve the processing of personal data. Germany has a rich history of prioritizing research and development, especially in the healthcare sector. The country boasts a strong infrastructure for innovation, with prominent universities, research institutions, and a collaborative environment between academia and the medical industry. This commitment to Research and Development has led to various advancements in medical technology, pharmaceuticals, and healthcare services. It is reflected in Germany's contributions to medical discoveries, drug development, and pioneering healthcare delivery services.

Germany has a highly skilled workforce in the medical and scientific fields. The country strongly emphasises education, offering comprehensive programs in medicine, engineering, and related disciplines. This skilled workforce contributes to developing and implementing innovative medical technologies and treatments. On the other hand, Germany has made significant advances in adopting e-Health solutions in recent years, and its healthcare system is known for its high standards and strong regulations.

e-Health data systems hold great promise for improving healthcare delivery services not only in Germany but around the globe, but consequently, they have not yet fulfilled

their potential in the privacy protection of sensitive personal data. Questions about privacy and the technical-organizational security of data processing have raised many concerns from observers, affecting patients' confidence and trust in the systems regarding whether there will be adequate personal data protection to protect patients' information privacy. This is a crucial area that needs more consideration when implementing the new digital health arena in the healthcare delivery system.

CHAPTER FIVE

PROTECTION OF PERSONAL DATA IN e-HEALTH IN TANZANIA

5.1 Introduction

This chapter presents the development of protection of personal data in e-Health in Tanzania an important aspect to consider to ensure the privacy and security of individuals' health related information. It is in this context that, The President of Tanzania Her Excellency Samia Suluhu Hassan once said, “In the digital era, there is no room for a country to prosper economically and in social service delivery without the application of the information and communication technology”⁴⁵²

This chapter focus further on the implementation of electronic health in Tanzania. Basically, on Social economic context of Tanzania in healthcare delivery services and implementing the e-Health technology, giving and receiving health information in Tanzanian Hospitals, approach to new era of e-Health system and the impacts on its implementation, legal and regulation of e-Health, bring to light Health Insurance Companies as they usually collect, proceess and store health data thus they have access to hospital's databases currently hosted or stationed at several hospitals in Tanzania, for example Masana Hospital, Kairuki Hospital and TMJ Hospital. This practice has as increased the links between patients and healthcare providers in delivering health services in the country. As a result there is an increase of sharing information where personal data are shared between patients, doctors and service providers.

⁴⁵² Daily newspaper, Thursday, April 7, 2022.

5.2 The Context of Tanzania in e-Health System

Tanzania's context in e-Health systems is dynamic, reflecting the broader trends in healthcare digitization across Africa. The development of e-Health in Tanzania has been gradually progressing over the years, driven by various factors such as advancements in technology, government initiatives, and the need to improve healthcare access and delivery in the country. The adoption of electronic health records is increasing in Tanzania, with efforts to digitize patient records and streamline healthcare processes. This can improve the efficiency of healthcare delivery, reduce errors, and facilitate data-driven decision-making. Mobile technology, particularly mobile phones, is widely used across Tanzania, even in remote areas. This presents an opportunity for leveraging mobile health (mHealth) solutions to overcome infrastructure limitations and improve healthcare delivery. Telemedicine is gaining traction in Tanzania, allowing healthcare providers to reach patients in remote areas and provide consultation and diagnosis remotely. However, challenges such as internet connectivity and the availability of trained personnel need to be addressed for telemedicine to reach its full potential.

Information Communication Technology infrastructure, mobile technologies are highly embraced in Tanzania to deliver healthcare services and information. Mobile phone applications are used for health awareness, appointment reminders, disease surveillance, and remote patient monitoring,⁴⁵³ for example, the introduction of the M-MAMA App. The app M-MAMA is essentially an emergency transport system meant

⁴⁵³ <https://www.trade.gov/market-intelligence/tanzania-ict-healthcare> accessed 19/7/2023.

to help women get transport, and in Tanzania, it helps pregnant women get transport and receive emergency care. It is a conduit between pregnant women and healthcare services, especially for those who cannot access quick and quality healthcare. Data security, privacy and trust remain key concerns in the data protection regime and digital healthcare platforms. Examples of these applications include Doctorlib, Dr. Blood Pressure, Afyacheck, Mobile Afya, and Jambo Mama.⁴⁵⁴

To embrace the use of technology in the health delivery system, the government of Tanzania has taken initiatives to improve healthcare access, quality, and efficiency across the country.⁴⁵⁵ For example, internet connectivity in Tanzania is expanding with slight gaps between urban and rural areas. The government and private sector have been working to improve internet infrastructure and access. This is crucial for successfully implementing e-Health initiatives that rely on online platforms, telemedicine, and electronic health records. In addition, in collaboration with various stakeholders, the government is working towards expanding the use of digital health technologies to benefit the population and strengthen the healthcare system.⁴⁵⁶ Regarding expanding digital health technologies, various stakeholders play crucial roles in the process.

These stakeholders include government agencies,⁴⁵⁷ which include departments or

⁴⁵⁴ JamboMama:New Health Mobile App for Tanzanian Women, <https://www.healthynewbornnetwork.org/blog/jambomama-new-health-mobile-app-tanzanian-women/> retrieved on 29/04/2024

⁴⁵⁵ Renggli, S., Mayumana, I., Mboya, D. et al. 'Towards improved health service quality in Tanzania: contribution of a supportive supervision approach to increased quality of primary healthcare.' *BMC Health Serv Res* 19, 848 2019.

⁴⁵⁷ Ibid

ministries of health at various levels (national, regional, and local) that set policies and regulations and provide funding for digital health initiatives. Healthcare providers encompass hospitals, clinics, and healthcare professionals such as doctors, nurses, and allied health workers. They use digital health technologies to provide care, manage patient data, and communicate with patients. Again, there are technology companies that are important stakeholders. These organisations develop and provide digital health tools and platforms like EHR systems, telemedicine platforms, mobile health apps, wearable devices, and health information exchange networks.

This is evidenced by ongoing health sector reforms on legislation and policies that intend to improve health outcomes with an initial emphasis on improving access, quality and efficiency of healthy service delivery throughout the country. This includes but is not limited to establishing the National e-Health Strategy of 2019-2024 to guide the implementation of digital health initiatives.⁴⁵⁸ This strategy aims to harness ICTs' potential to strengthen health systems, improve healthcare delivery, and enhance health outcomes. The Ministry of Health developed the Tanzanian Health Enterprise Architecture (THEA) to guide the national integrated Health Information System (HIS) development.⁴⁵⁹ The THEA is used to design a hospital system called Electronic Facility Management System (eFMS), which connects all government hospitals in Tanzania, all referral hospitals, and government health centres.⁴⁶⁰ The eFMS is meant to centralize information from all government hospitals to the Ministry. This means

⁴⁵⁸ 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.

⁴⁵⁹ Ministry of Health and Social Welfare. Tanzania National eHealth Strategy June, 2013– July, 2018.

⁴⁶⁰ Ibid.

that the government data of particular patients are required can easily be accessed via the application eFMS.

The eFMS has improved patient care by enhancing communication between healthcare providers and patients. In addition, the health information systems in Tanzania hospitals generally use ICT, 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 dataset), and Support Health Facilities in service delivery management.⁴⁶¹

From the foregoing, it is posited that Tanzania has made efforts to digitize healthcare delivery systems and establish electronic medical record systems in healthcare facilities. The healthcare delivery systems enable healthcare providers to access and manage patient information electronically, improving the efficiency of healthcare delivery and continuity of care. Further, the country has implemented health information systems to collect, manage, and analyze health data. These systems help monitor disease trends, track healthcare service utilization, and support evidence-based decision-making among healthcare practitioners.⁴⁶² Generally, the Tanzania Ministry of Health recognizes the importance of ICT in transforming healthcare delivery by enabling information access and data collection and supporting healthcare

⁴⁶¹ Neema, E.S., 'Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulations' East African Journal of Education and Social Sciences, Vol 4, 2023.

⁴⁶² Mashoka R, J, (et all), "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective. Afr J Emerg Med. 2019.

operations, management, and decision-making.

The Government encourages the digitalization of medical records and the use of technology in health care delivery. On the other hand, health practitioners consider technology's benefits to offset its possible difficulties and shortcomings within the health industry. The e-Health system has merged many aspects of the healthcare system. The introduction of computers and technology has helped improve the efficiency of healthcare delivery and patient care.⁴⁶³ This is because e-Health allows access to health resources and healthcare electronically.⁴⁶⁴ It provides an opportunity to preserve or improve healthcare quality more cost-effectively. It allows healthcare services to be reinvented to make them more dynamic and able to adapt to technological changes.

5.3 Analysis of the Country's Policy Framework on the Health Sector

5.3.1 Tanzania National Health Policy, 2003

The Health policy was introduced in 2003 and serves as a directorial document for the general health sector in Tanzania. It includes provisions or guidelines related to the incorporation of fast-growing technology and the use of e-health technologies to improve healthcare delivery services, as well as the consequences. The policy emphasizes delivering equitable and quality healthcare services from the district to the regional level.⁴⁶⁵ The policy sets a vision for developing the health sector in Tanzania.

⁴⁶³ Ailey D, (et all). "Systematic review of evidence for the benefits of telemedicine", J TelemedTelecare. 2002.

⁴⁶⁴ WHO: <http://www.telehealthcode.eu/glossary-of-terms.html>. Accessed 13 March 2022.

⁴⁶⁵ Section 3.1 National Health Policy, 2003.

The objectives of the health policy are as follows. First, to improve the health and well-being of all Tanzanians and to reduce the burden of disease while raising the life expectancy of the people of Tanzania.⁴⁶⁶ Second, the health status of all Tanzanians, particularly the vulnerable groups, should be improved through a comprehensive and integrated approach. It emphasizes promoting community-based health care, improving health infrastructure, strengthening the health workforce, and increasing access to essential health services.⁴⁶⁷

The development of national health policies is crucial for poverty eradication and economic development. It is 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, so that they can participate more fully in the workforce. This increased productivity contributes to economic growth.⁴⁶⁸ 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 delivery services.⁴⁶⁹

The policy focused on implementing various health sector reforms to improve the efficiency and effectiveness of service delivery, health financing, and management. The policy clearly states that the Ministry of Health, as a technical Ministry, is

⁴⁶⁶ Section 2.1 Ibid.

⁴⁶⁷ Section 4 Ibid.

⁴⁶⁸ Section 1 National Health Policy, 2003.

⁴⁶⁹ Section 2 Ibid.

responsible for all matters about health in the country.⁴⁷⁰ 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.⁴⁷¹ The policy encouraged collaboration between the public and private sectors to improve the quality and accessibility of health services.

Advancements in health information technology can potentially transform healthcare delivery services within the Country. Policies that promote the adoption of EHRs and telemedicine in health systems can lead to better coordination of care, improved patient outcomes, and increased efficiency in healthcare delivery services. Adequate and well-trained healthcare professionals are essential for the functioning of the electronic healthcare system.

Equally important, preparedness for public health emergencies like pandemics or natural disasters is critical to health-related policies. In this context, the government must have contingency plans, allocate resources for emergency response, and strengthen healthcare infrastructure to handle such situations effectively. For example, during the COVID-19 pandemic, there was no policy or regulation on how to deal with the situation. Surprisingly, the existing health policy is poorly articulated on the e-

⁴⁷⁰ Section 1.2 Ibid.

⁴⁷¹ Section 5 Ibid.

health mode of health service delivery.

Instead, Tanzania has developed specific Tanzania National e-Health Strategies of 2013-2018 provides as one of its strategic principles that provision of e-Health should guarantee patient information rights, integrity and confidentiality. 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.⁴⁷² The strategy outline the country's approach to leveraging ICTs' in the health sector.⁴⁷³

The review process followed a participatory approach driven by HSSP III strategic objectives. The National e-Health Strategy provides an appropriate basis to guide the development of e-Health in Tanzania. It adopts an enterprise architecture (EA) - driven development approach to developing e-Health capabilities. Leverage what currently exists in the Tanzanian e-Health landscape, understand the new components and where they fit in existing structures, define information structures to fit current needs and support anticipated ones, and demonstrate how technology and resource constraints dictate both the feasible and the path forward. These strategies focus on 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, and the second is the Health

⁴⁷² Neema, E.S., 'Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulations' East African Journal of Education and Social Sciences, Vol 4, 2023.

⁴⁷³ 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.

Sector Strategic Plan 2015–2020. However, the government’s ongoing efforts ensure that digital health systems are implemented in well-coordinated and standardized data formats and communication protocols.

Health-related policies incorporate many regulations, laws, and guidelines that aim to improve public health, healthcare access, and people's overall well-being. These policies address various healthcare challenges and ensure healthcare services are delivered efficiently and equitably. One of the primary objectives of many health policies is to ensure that all citizens have access to affordable and quality healthcare services. This may involve expanding healthcare coverage, reducing out-of-pocket expenses, and improving the distribution of healthcare facilities to underserved areas. These policies can be affected at various levels, including local, regional, national, and international. Health-related policies must be evidence-based, considering the latest scientific research and best practices. These policies often involve partnerships between government agencies, healthcare providers, advocacy groups, and other stakeholders to achieve the best possible outcomes for its people's public health and well-being. These policies are essential for building a strong trust among the system users (electronic health-related data applications) and an inclusive healthcare system.

5.3.2 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.⁴⁷⁴

The effective use of ICT is becoming the most critical factor for rapid economic growth and wealth creation, as well as for improving socio-economic well-being. ICTs are, therefore, increasingly becoming the key drivers for socio-economic development worldwide. It is now acknowledged that a nation's capability to accelerate its socio-economic development process and gain global competitiveness depends very much on the extent to which it can develop, use, and exploit ICT in one form or another.⁴⁷⁵

The policy promotes adopting e-government initiatives to improve public service delivery, such as e-Health and online platforms for government services and digital communication between citizens and government agencies. The NICTP 2003, under a focus area of Public Services, addressed the issue of using ICT to enhance service delivery to the general public. Cognizant of the fact that there were fragmented e-Government initiatives, the Government made a remarkable step of establishing the e-Government Agency (e-GA) in 2010 to coordinate, oversee and promote e-Government initiatives and enforcement of e-Government standards to Public Institutions. Other strides include using integrated HR and Payroll systems covering

⁴⁷⁴ Neema, E.S., 'Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulations' East African Journal of Education and Social Sciences, Vol 4, 2023.

⁴⁷⁵ The emergence of the information age emphasizes the important role that ICT can play in facilitating a nation's socio-economic development (National Information and Communication Policy 2016 – Pg 14).

about 280,000 public servants and adopting an organizational web portal in the Government. Other ICT services, particularly those that allow interaction and/or transaction with MDAs, are rare in Tanzania's public sector.⁴⁷⁶

The policy recognises 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. Human resources are important for a sustainable ICT industry. ICT Human Capital Development, as one of the pillars in the NICTP 2003, aims at expanding and increasing local skilled and competent ICT human resources in the country. Several efforts have been taken to develop the ICT Human capital in the country, including the establishment of ICT colleges in Universities such as the dedicated College of ICT at the University of Dar es Salaam, the dedicated School of Informatics at the University of Dodoma, the introduction of ICT programs in privately owned and operated Universities and an introduction of ICT subject in the primary and secondary school curriculum. As a result, the number of students enrolled and graduates in ICT in both public and private institutions has increased, and more ICT courses are now offered compared to the situation in 2003.

Other efforts include the development of an appropriate scheme of service for ICT cadres in the Government. Despite the achievements above, there are still challenges in the development of ICT human capital which need to be addressed for full exploitation of benefits of the ICT sector, such as non-recognition of ICT professionals

⁴⁷⁶ National Information and Communication Policy 2016 – Pg 10.

and inadequacy of ICT skilled and competent human resources base to accelerate the nation's socio-economic development efforts in the information age. In this context, appropriate policy mechanisms must be implemented to address the challenges above. Tanzania.⁴⁷⁷ In this context, 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.

Enforcement mechanisms are crucial to ensure that employers take safety seriously and make the necessary changes when violations of privacy are found.⁴⁷⁸ Localized ICT solutions can improve the efficiency and effectiveness of public service delivery.

⁴⁷⁷ National Information and Communication Policy 2016 – Pg 19.

⁴⁷⁸ Ibid.

By tailoring electronic systems to meet the specific needs of government agencies, services can become more accessible and responsive to citizens. 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. Evaluating African countries' health policies with regard to e-Health is crucial for understanding their readiness to embrace digital technologies in healthcare. Many African countries have recognized the importance of e-Health and have included it in their national health policies and strategies. These frameworks often outline objectives, strategies, and action plans for implementing e-Health solutions.

5.4 Legal and Regulatory Framework for Personal Data Protection in e-Health

Generally, Tanzania has no specific electronic health data privacy legislation. However, three legal sources regulate privacy protection as a whole. These are the Constitution of the United Republic of Tanzania Constitution 1977, statutes, and case laws as discussed below.

5.4.1 General Domestic Law on Privacy and Personal Data Protection on e-Health

5.4.1.1 The Constitution of the United Republic of Tanzania 1977

Constitutional provisions play a significant role in addressing privacy rights in Tanzania, as they do in many countries. Tanzania's Constitution, like those of many other nations, typically contains clauses or amendments that explicitly protect citizens'

privacy rights. These protections often encompass various aspects of privacy, including personal information, communications, and the right to privacy in one's home. Moreover, legal frameworks and statutes are often developed to align with constitutional mandates, providing further guidance and enforcement mechanisms for safeguarding privacy.⁴⁷⁹ Laws related to data protection, surveillance, and telecommunications often complement constitutional provisions to ensure the protection of individuals' privacy rights.

Privacy encompasses many aspects, including personal data protection, freedom from unwarranted surveillance, and the right to be left alone.⁴⁸⁰ Additionally, developing privacy rights is always influenced by international standards and conventions. Tanzania is also a party to international agreements that address privacy concerns, and these agreements always shape the legal framework within the country. For the purpose of preserving the person's right to privacy with the requirement of the Constitution, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon.⁴⁸¹

Privacy is a constitutional right interpreted in Tanzania and is enshrined in various statutes, although not comprehensively. These include but are not limited to the Medical, Dental and Allied Health Professionals Act, 2017, the Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005, Human DNA

⁴⁷⁹ Article 63(3) of The Constitution of the United Republic of Tanzania 1977 as amended.

⁴⁸⁰ Article 17 of The Constitution of the United Republic of Tanzania 1977 as amended.

⁴⁸¹ Article 16(2) of The Constitution of the United Republic of Tanzania 1977 as amended.

Regulation Act 2009, and HIV and AIDS (Prevention and Control) Act 2008. However, the Constitution of Tanzania 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. For example, Article 16(1) states 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 as 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.⁴⁸² 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.⁴⁸³

The court of law has agreed to respect people's privacy. In *Jackson Ole Nemeteni and 19 Others v the Attorney General*,⁴⁸⁴ the HCT held that "in the absence of a procedure prescribed by law, the administration of a provision of any law which seeks to limit the basic rights of an individual is susceptible to abuse, and cannot therefore be saved under Article 30(2) of the Constitution."⁴⁸⁵

The relationship between doctor and patient is fiduciary. Essentially, it means it is

⁴⁸² Article 16(2) The Constitution of the United Republic of Tanzania.

⁴⁸³ Ibid, Article 16(3).

⁴⁸⁴ Misc. Civil Cause No. 117 of 2004, High Court of Tanzania, Dar es Salaam(Unreported).

⁴⁸⁵ *Jackson Ole Nemeteni and 19 Others v the Attorney General*2.

based on trust between the two. This trust enables patients to disclose personal and sensitive information to the hospital's doctor or service delivery personnel. On the other hand, doctors are not obligated to disclose all information received during the patient's treatment. This is because patients normally share their secrets with hospital personnel, who are sensitive during treatment. If patients' sensitive information is divulged, there is a possibility of not sharing such information in detail on one side. On the other side, it may attract legal action towards 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 important for the right to confidentiality should be protected.

In Tanzania, the right to confidentiality is enshrined under various domestic laws, albeit not specific to e-health service delivery. Such laws generally aim to safeguard individuals' personal information on one side. Conversely, it provides guidelines for organizations' collection, process, and storing of such data. The Medical, Dental and Allied Health Professionals Act 2017,⁴⁸⁶ the Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005, the Human DNA Regulation Act 2009,⁴⁸⁷ and the HIV and AIDS (Prevention and Control) Act 2008⁴⁸⁸ contain provisions that regulate medical confidentiality. These regulations set the standards for healthcare professionals in Tanzania to maintain patient confidentiality and privacy.

⁴⁸⁶ Section 41 Medical, Dental and Allied Health Professionals Act, 2017.

⁴⁸⁷ Section 64 Human DNA Regulation Act 2009.

⁴⁸⁸ Section 16,17 HIV and AIDS (Prevention and Control) Act 2008.

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 fulfil 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.

In this context, medical confidentiality is safeguarded by the general principle of duty of care on the part of health practitioners, a breach of which may attract a claim based on the tort of negligence in the area of breach of duty of care.⁴⁸⁹ It is important that the regulations of data protection law and the principles of medical confidentiality are very similar in terms of their protective purpose and general design, and the diverging views are, therefore, only relevant in a minimal number of cases.

Some specific laws in Tanzania provide for privacy in health-related issues. These include the HIV and AIDS (Prevention and Control) Act 2008 and the Human DNA Regulation Act 2009. The HIV Act generally provides that medical specialists may not breach medical confidentiality or disclose information about persons' HIV or

⁴⁸⁹ See High Court of Tanzania, *Theodelina Alphaxad a Minor S/T Next Friend Vs the Medical Officer I/C, Nkinga Hospital*, 1992, TLR 235.

AIDS status unless in case of applicable exception.⁴⁹⁰ The Act further provides all health practitioners, workers, employers, recruitment agencies, insurance companies, data recorders, sign language interpreters, legal guardians and other custodians of any medical records, files, data, or test results shall observe confidentiality in the handling of all medical information and documents, particularly the identity and status of persons living with HIV and AIDS.⁴⁹¹

Correspondingly, the Human DNA Regulation Act 2009 regulates the disclosure of personal information relating to human DNA.⁴⁹² The existing legal and regulatory framework imposes very general obligations upon medical practitioners. These include obligations to obtain patients' consent and non-disclosure of medical records. However, these requirements are inadequate in protecting health records in health-related issues and basically on electronic health-generated information.

Generally, confidentiality in health and social care is an essential principle, as discussed above. This is because it helps to build trust between patients and healthcare providers so that they can share information, and this can be extremely important in ensuring they get the care they need and give out proper information. Maintaining confidentiality in medical and social care settings can involve simple, practical measures such as positioning computer screens so that third parties do not accidentally see information and following official guidelines in sensitive and complex situations.

⁴⁹⁰ Section 16 HIV and AIDS (Prevention and Control) Act 2008.

⁴⁹¹ Section 17 Ibid.

⁴⁹² Section 52 to 65 Human DNA Regulation Act 2009.

Those working in health have legal and professional responsibilities to uphold confidentiality and will have to undergo significant training on the subject. In the context of health, confidentiality is an essential principle of providing good care which medical professionals and care practitioners should follow. It means not disclosing information about a patient or client to anyone who should not know or does not strictly need to know unless consent has been given.⁴⁹³

5.4.1.2 Tanzania Personal Data Protection Act 2022 (TPDPA)

The Tanzania Personal Data Protection Act came into force in 1st May in 2023. This is the first harmonized Act protecting personal data in all sectors. The main objective of TPDPA is to provide provisions for “principles of protection of personal data to establish minimum requirements for the collection and processing of personal data; to provide for the establishment of Tanzania Personal Data Protection Commission; to provide for improvement of protection of personal data processed by public and private bodies; and to provide for matters connected therewith.”⁴⁹⁴ The TPDPA has IX Parts: Part I provides the title, scope of application, interpretation, and principles of personal data protection. Part II provides for the establishment of a personal data commission. Part III deals with the registration of data controllers and data processes.

Part IV provides rules for using, disclosing, and retaining personal data. Part V sets rules for trans-border data flow. Part VI deals with the rights of data subjects, while Part VII sets rules for investigating complaints. Part VIII deals with financial

⁴⁹³ Ibid

⁴⁹⁴ Tanzania Personal Data Protection Act 2022.

provisions, and Part IX deals with miscellaneous provisions. The TPDPA applies to Tanzania's mainland as well as Zanzibar.⁴⁹⁵ However, its application is limited to union matters only, and the Act shall not apply to non-union matters. This means that in any non-union matter, this law shall not apply. TPDPA applies to both public and private bodies and individuals in both territories.

Parts I, IV, V and VI are fascinating and relevant to e-Health delivery services. Part 1 provides the principle upon which the data controller or processor ensures that personal data is processed lawfully, fairly and transparently.⁴⁹⁶ Under this principle, fair, lawful, and transparent data processing is 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 their data will be handled. Transparency is key to building trust with data subjects and ensures that they have control over their personal information.

In processing data, stakeholders can be broadly categorized into two main roles: controllers and processors. 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 providing the identity of the controller or processor, laying down the

⁴⁹⁵ Section 2 of PDPA, 2022.

⁴⁹⁶ Section 5 (a) Ibid.

purpose of the collection, ascertaining persons to whom data will be disclosed and specifying whether the supply of information is intentional or mandatory.⁴⁹⁷

In addition, informing about the consequences for the individual if the required information is not provided, specifying whether or not the consent of the individual is required for any processing of the information, and informing the right of access of the individual and the possibility of correction or destruction of personal data to be provided by controller or processor.⁴⁹⁸ 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 collecting such data, of which the collection shall not be unlawful.⁴⁹⁹ 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

⁴⁹⁷ Section 22, Ibid.

⁴⁹⁸ Section 22(2), Ibid.

⁴⁹⁹ Section 23 (2) of the PDPA.

intended.⁵⁰⁰ 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 the case, 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 purposes.⁵⁰¹ The law further requires the data controller or data processor to collect data directly from the data subject.⁵⁰² However, without consent, personal data cannot be processed.⁵⁰³ Similarly, personal data can be processed without consent if they are publicly available, in situations where noncompliance is necessary as the requirement of other written laws or in cases where the data controller has legal obligations to protect the vital interest of the data subject; for administration of justice; or in the public interest.⁵⁰⁴

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.⁵⁰⁵ The longer data is held, the greater the risk of a data breach or unauthorized access. Storing unnecessary data increases the surface

⁵⁰⁰ Section 25(1), Ibid.

⁵⁰¹ Section 25(2), Ibid.

⁵⁰² Section 23(1), Ibid.

⁵⁰³ Section 23(3), Ibid.

⁵⁰⁴ Section 29(1), Ibid.

⁵⁰⁵ Section 28 (1) and (2), Ibid.

area for potential security incidents. It is important to have mechanisms to review and periodically 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 subject.⁵⁰⁶ The provision clarified that no sensitive personal data shall be processed unless the data subject has given their written consent to process such data. Even where the data subject has given consent to process personal data, the law provides the right Data subject to withdraw their consent at anytime of the processing and without explaining why they are withdrawing their consent.⁵⁰⁷

In the context of PDPA, sensitive data include data concerning health.⁵⁰⁸ However, 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 or recall certain data. This can be in circumstances where the processing of such data requires fulfilment in certain written laws or before the court of law for certain trials.⁵⁰⁹

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

⁵⁰⁶ Section 30(1), Ibid.

⁵⁰⁷ Section 30(2), Ibid.

⁵⁰⁸ Section 3, Ibid.

⁵⁰⁹ Section 30(3), Ibid.

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 any association that exists for political, ethical, religious or employment union purposes during its appropriate activities. The processing is carried out for scientific research according to the specific guidelines. It relates only to individuals 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.⁵¹⁰

The second principle states that personal data shall be obtained only for explicit, specified, and lawful purposes and shall not be further processed in any manner incompatible with that purpose.⁵¹¹ The Purpose Limitation Principle 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. 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

⁵¹⁰ Section 30(5) of Tanzania Personal Data Act 2022.

⁵¹¹ Section 5(b) Ibid.

processing of the data should be consistent with the original intent and within the bounds of the law. This principle prohibits collecting information about people consistently and arbitrarily without a thorough, clear and genuine purpose. Data controllers can only process personal information against the purpose they registered for.⁵¹² This is whether ‘you use and disclose the data in a way that those who supplied the information would expect to be used and disclosed, for example, the transmission of personal information to the controller’s agents who carry data operation on behalf of such controller and not recalling it for their purpose.

If an organization wishes to use the data for a new or different purpose not originally communicated to the data subjects, it would need to seek additional consent from the individuals or find another lawful basis for the new processing. This principle helps protect individuals' privacy and ensures that their data is not misused or used in ways they did not expect or agree to.

The third principle is that personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.⁵¹³ This principle ensures that organizations collect and process only the minimum amount of personal data required to achieve their legitimate objectives. By adhering to this principle, organizations can limit privacy risks and ensure that individual's data is handled responsibly and respects their privacy rights. This principle is also reflected in section 24 of the TPDPA, which states that personal data should be accurate, relevant, and not misleading. This

⁵¹² Section 14 (1), (2) Ibid.

⁵¹³ Section 5(c) Tanzania Personal Data Protection Act, 2022

principle means that the data controller should only collect and keep enough information that enables them to achieve the purpose for which information is collected and not an additional purpose. The controller is barred from collecting and maintaining information if it can be used in the future.

Moreover, controllers are prohibited from asking very personal questions if the information obtained in this way is not demeaned, for which they embrace personal data. The data collected should be sufficient to fulfil the specific purpose for which it is being processed. In other words, the data should be enough to achieve the intended goal and no more than that. Such data should have a clear and direct connection to the purpose of processing. Irrelevant or unnecessary information should not be collected or retained. Data collection should not be excessive concerning the intended purpose. Organizations should avoid gathering more personal data than is necessary for the specified purpose of processing.

The fourth principle states that personal data shall be accurate and, where necessary, kept up to date.⁵¹⁴ Accurately and keeping personal data up-to-date are crucial principles in data protection and privacy regulations. This statement aligns with the data protection principles in various laws, including the GDPR in the EU. This principle appears that a data controller must rectify, block, erase or destroy the data as appropriate after being informed of the inaccuracy of personal data by a data subject. Personal data should be accurate and free from errors. Organizations should take

⁵¹⁴ Section 5(d), Ibid.

reasonable steps to ensure the data they collect, and store is correct and up-to-date. Inaccurate data can lead to incorrect decisions, adversely affecting individuals and organizations.

This obligation extends to the third party involved in the transaction of such information. Suppose the data controller fails to rectify, block, erase or destroy inaccurate personal data. In that case, a data subject may apply to the Commissioner to have such data corrected, blocked, erased or destroyed. The Act further provides that this requirement of keeping data accurate and up-to-date has an additional importance in that it may result in the liability of a data controller to an individual for damages if the former fails to observe the duty of care provision in the Act applying.

By adhering to data accuracy and updating, organizations can build trust with their customers or users, comply with data protection laws, and ensure that the personal data they process remains relevant and reliable. The fifth principle states that personal data processed for any purpose shall not be kept longer than is necessary for the purpose or those purposes.⁵¹⁵ This principle is otherwise known as the retention of personal data. The principle is one of the fundamental data protection principles often found in data protection and privacy laws worldwide. It is commonly known as the "Principle of Data Minimization" or the "Principle of Storage Limitation."

The essence of this principle is that personal data should not be retained for a longer

⁵¹⁵ Section 5(e) Tanzania Personal Data Act 2022.

period than necessary to fulfil the specific purposes for which it was collected. In other words, organizations should only keep personal data for as long as it is needed to achieve the purposes for which it was originally collected or for legitimate and lawful additional purposes. This requirement places a responsibility on data controllers to be clear about when the data will be kept and why the information is being retained. If there is no good reason for retaining personal information, then that information should be consistently erased.

Besides, suppose the data controller would like to retain information about customers to help provide better service to them in future. In that case, they must obtain the customer's consent for retention.⁵¹⁶ To comply with the principle of data minimization, organizations need to establish data retention policies that outline specific timeframes for retaining different types of personal data. These policies must consider the purpose of data processing, legal requirements, and other relevant factors. Once the retention period expires or the purpose is fulfilled, the data should be securely deleted or anonymized further to protect individuals' privacy and personal data protection.

The sixth principle is that personal data shall be processed per the rights of the data subjects as applied under this Act.⁵¹⁷ This principle is a key component of data protection and privacy regulations, such as Federal Data Protection Act 2017. Germany has integrated the GDPR into its national law through the Federal Data

⁵¹⁶ Section 28 (1) and (2), Ibid.

⁵¹⁷ Section 5(f) Tanzania Personal Data Protection Act 2022.

Protection Act.⁵¹⁸ This act complements and specifies the GDPR's provisions, ensuring alignment with German legal principles to include rights of the data subjects. The principle emphasizes that individuals have certain rights regarding their data, and organizations or entities that collect and process this data must respect and uphold these rights. This principle has to be read in conjunction with Part VI of the TPDPA, which deals with the rights of data subjects. The right of access to personal data under section 33(1) of the Act is the most important to the exercise right to be informed as to who is processing his or her data, to whom such data is referred and for what purpose to be precise of other rights includes rectification, blockage, erasure or destruction of such data deemed not intended by the data subject.

Moreover, it obligates the data controller to explain to the data subject the logic used in any programmed decision-making process where the decision significantly affects the individual and is solely based on the automatic process.⁵¹⁹ However, data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects them. Adhering to this principle means that organizations must implement appropriate measures to ensure data subjects' rights are respected throughout the data processing lifecycle. This includes providing clear and transparent privacy notices, establishing mechanisms to handle data subject requests efficiently, and maintaining data security to protect against unauthorized access or data breaches.

⁵¹⁸ Section 47 (4) and (5) of the Federal Data Protection Act 2017.

⁵¹⁹ Section 33 (c), *Ibid.*

The seventh principle states that appropriate measures must be taken to ensure appropriate security for personal data. Organizational measures shall be taken against unauthorized or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.⁵²⁰ This principle is an essential aspect of data protection. It is found in various privacy laws and regulations worldwide, such as the GDPR in the EU. This principle is broadly covered in section 27 of the TPDA as part of a data controller's obligations. However, sufficient details of security measures are provided in the section. The Federal Data Protection Act incorporates this principle providing that such personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.⁵²¹

Organizations must implement appropriate security measures to protect personal data from unauthorized or unlawful processing. This means setting up safeguards to prevent unauthorized access, use, disclosure, or alteration of personal data. These include regular data backups, disaster recovery plans, and appropriate storage practices, assessing the costs of security measures against other factors, evaluating the state of technological development, training staff, using contractual obligations to put processors under compliance with the application of appropriate security measures providing appropriate access control, and physical security. The responsibility for ensuring data security is not limited to technical measures alone but also includes

⁵²⁰ Section 5(g), *Ibid.*

⁵²¹ Section 47(6) of the Federal Data Protection Act 2017.

organizational measures. This could involve establishing clear policies, procedures, and guidelines for handling personal data securely and responsibly within the organization.

The eighth principle is on cross-border transfer of personal data, which states that personal data shall not be transferred to another country unless that country ensures an adequate level of protection of the rights of data subjects concerning the processing of personal data.⁵²² This principle is a fundamental concept in personal data protection and privacy regulations, and it is often found in laws and regulations that govern the transfer of personal data from one country to another. The adequacy principle states that personal data should not be transferred to a country outside the EEA or any other jurisdiction with similar data protection laws unless that country provides adequate protection for the rights and privacy of data subjects concerning processing their data. This principle is also discussed under section 31 of the TPDA.

The latter section deals with the international transfer of personal data to states with adequate personal data protection. The idea behind this principle is to ensure that when personal data is transferred to a foreign country, it will receive a level of protection equivalent to the level of protection provided in the country where the data was originally collected. This helps to safeguard individuals' rights and privacy and prevents their data from being misused or exploited in jurisdictions with weaker data protection standards.

⁵²² Section 5(h) Tanzania Personal Data Protection Act 2022.

It is important to note that, to date, Tanzania does not have a specific e-Health data protection institution. Some relevant institutions and frameworks could protect health-related data and ensure privacy in the e-healthcare delivery services within the Country. The Personal Data Protection Commission is the main institution that enforces data protection in the country. The Commission is established under section 6(1). This Commission is chaired by the Director General of the Commission, whom the President appoints.⁵²³ The Commission falls under the President's Office.

There is the establishment of the Board of Personal Data Protection Commission as provided under Section 8 of TPDPA is vital for protecting personal data by providing regulatory oversight, enforcing laws, promoting a culture of data privacy, offering redress mechanisms, fostering international collaboration, and supporting innovation. Effective data protection measures can actually foster innovation by promoting trust and confidence in digital services. One of the primary functions of this Board is to stand as a watchdog, oversee the performance of the Commission, and make sure the Commission adheres to the laws and regulations of the country as provided under the Act.⁵²⁴

The functions of the Commission are well articulated under Section 7 of TPDPA to include monitoring compliance with data processing, registering data controllers within the Country, receiving and dealing with complaints that are on the violation of

⁵²³ Section 11(1) of Tanzania Personal Data Protection Act, 2022.

⁵²⁴ Section 9(1), Ibid.

personal data and breach of privacy in the due cause of processing personal data, bringing awareness to the general public on the importance of privacy and personal data protection, looking for ways of cooperation's among the data protection authorities and looking for appropriate measures to ensure that matters on the processing of personal data meet the adequate standards so as not to infringe the individual's privacy.

The oath places the Commissioner and other Board members in the Commission under a duty of confidentiality. They are not required to disclose any information obtained in exercising power or performing a duty under the Act. This function is further merged in section 14 of the Act on the creating and maintaining a register of all data controllers and data processors, exercising control on all data processing goings-on, either at its discretion or at the request of a data subject, and verifying whether the processing of data is in accordance of the TPDPA or regulations made under it. Whether or not the Tanzania Data Protection Commission is independent is difficult to assess. Yet, in theory, the general view is that the Commission is independent. However, assessing how the Commission and the Board of Personal Data Protection functions have been implemented in practice is important.

The Tanzania Communication Regulatory Authority (TCRA) was established under the Tanzania Communications Regulatory Authority Act No. 12 of 2003, which merged the Tanzania Communications Commission and the Tanzania Broadcasting Commission. TCRA became operational on 1 November 2003 and has effectively taken over the functions of the two defunct commissions. TCRA regulates and

oversees the communications sector, including aspects of eHealth, such as telecommunications and data networks. While its primary focus might not be e-Health data protection, it may have some regulatory oversight in the broader data protection and privacy context. The authority works to protect the interests of consumers by ensuring that service providers adhere to quality standards and provide reliable services.

The Ministry is responsible for formulating and implementing such policies regarding health-related matters. The ministry has developed different strategies to affect the introduction of e-Health in Tanzania, such as The Tanzania National Digital Health Strategy of 2019–2024, which resulted from a consultative and collaborative approach which engaged stakeholders at different levels in the health sectors.

National Digital Health Steering Committee (NDHSC). The NDHSC is an important organ for ensuring the successful implementation of the Digital Health Strategy, which has the following main roles: provide leadership and strategic guidance to all digital health initiatives in the health sector to ensure that they are well aligned with the National Digital Health Strategy and the Health, Policy and Health Sector Strategic Plan priorities, oversee the implementation of the Digital Health Strategy, guide the engagement of stakeholders in the implementation of the Digital Health Strategy, provide a system-level perspective and technical guidance on digital health initiatives, mobilize resources for strategic investment in digital health initiatives across the health sector, review and approve digital health initiatives, oversee compliance with digital health standards and guidelines, establish and oversee standards and guidelines to

govern issues of ownership, compliance, privacy, confidentiality, and security in the digital health.

5.5 Conclusion

Privacy as a concept in Tanzania has evolved over time, influenced by cultural, legal, and technological factors. Historically, Tanzanian society placed significant emphasis on communal living and collective values, where privacy may have been less of a concern compared to individualistic societies. However, with modernization, globalization, and advancements in technology, the notion of privacy has gained more recognition and importance. Tanzania's legal system has played a crucial role in shaping the concept of privacy. The country's constitution guarantees the right to privacy under Article 16. The proliferation of technology, particularly mobile phones and the internet, has brought privacy concerns to the forefront. Tanzanians, like people worldwide, are increasingly aware of the need to protect their personal information online. Issues such as data breaches, identity theft, and online surveillance have heightened concerns about privacy rights.

In the healthcare sector, there has been a growing recognition of the importance of medical privacy in e-Health. Laws and regulations govern the handling of sensitive medical information to ensure patient confidentiality and privacy rights are upheld. Patient confidentiality not only brings up trust between healthcare providers and patients but also safeguards sensitive personal information. Laws and regulations such as the Tanzania Personal Data Protection 2022, and similar regulations in relation to personal data protection globally, set standards for the protection of medical

information. These laws dictate how healthcare providers can collect, use, and disclose patients' health information, mandating strict protocols for its security and privacy. With the advent of digital health records, ensuring the privacy and security of medical information has become even more critical, encouraging advancements in encryption, access controls, and other technologies to safeguard patient data.

CHAPTER SIX

SUMMARY OF RESEARCH FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 Summary of Research Finding

The major objective of this thesis was to analyze the legal framework for protecting patients' personal information in the e-healthcare delivery system in Tanzania. It further suggested a legal framework approach for patient health data protection in e-Health delivery system. The thesis explored the challenges Tanzania faces in implementing privacy protections and personal data, particularly electronic health-generated data, despite having the Personal Data Protection Act 2022.

It was found that the legislation provides essential lessons for safeguarding data privacy. However, there are obstacles posed by the country's socio-economic and cultural context that surrounds the concept of privacy and personal data protection. The researcher further observed that while the Personal Data Protection Act of 2022 offers valuable insights into how data privacy can be maintained, the practical application of these principles is hindered by the specific social, economic, and cultural conditions in Tanzania. These challenges include issues related to technological infrastructure, public awareness of data privacy, legal enforcement mechanisms, and potential conflicts with cultural norms and practices.

The secondary data reveal that the socio-economic factors perpetuate the problem under examination due to poverty, illiteracy, and high corruption rates among public

institutions in Tanzania. These factors contribute to people protecting their privacy and welfare, particularly health-related information. Social relations in Tanzania favour sharing information and sincerity in ways inconsistent with claims to control one's health information under privacy legislation. Moreover, social obligations may influence a person's consent to the extent that the idea of consent as freely given may not be easy to ensure in some aspects of the e-Health sub-sector.

The research further reveals that health policies in Tanzania do not reflect e-Health practice that often rotates around the observation of existing healthcare policies, as observed in this Chapter. Health regulations have not kept up with the rapid advancements in digital health technologies and practices. The pace of technological change in the e-Health field has often overtaken the development and implementation of policies and regulations. As new tools and platforms emerge, policymakers struggle to keep up with creating relevant rules and guidelines. Many e-Health technologies involve collecting, storing, and sharing sensitive patient data. However, developing effective policies that balance innovation and protecting patient rights can be complex. Thus, policies must address these concerns open-mindedly to ensure patient privacy and data security.

One challenge in implementing e-Health is the lack of harmonisation and consistent, standardized legal frameworks governing e-Health practices in Tanzania. E-Health technologies are evolving rapidly, often outpacing the ability of regulatory bodies to establish comprehensive and up-to-date legal frameworks. This can result in fragmented regulations that struggle to address new challenges emerging technologies

pose. It involves multiple stakeholders, including healthcare providers, technology companies, patients, insurers, and governments. Balancing the interests of these diverse groups in legal frameworks can be challenging.

Chapter three discussed international benchmarking on e-Health. Unlike some other sectors, no binding international treaty regulates e-Health sector. The absence of a standardized international framework can lead to inconsistencies in the implementation of e-Health. Without international instruments on e-Health, each country is at liberty to develop its own set of laws and regulations. This can result in a fragmented legal landscape, with varying requirements, standards, and guidelines that may not align across borders. The practice of every country's independent regulation on e-Health diminishes patients' trust in the e-Health system. The absence of consistent regulations on e-Health can make it complex for healthcare providers to deliver services in multiple jurisdictions, hindering the expansion of cross-border healthcare delivery services.

Based on the research conducted, no case law relates to e-Health in Tanzania. The court of law develops no jurisprudence because it is a new and unregulated area that needs an immediate clear legal framework intervention. The challenge of establishing legal precedents in the field of e-Health arises from the unique nature of e-Health situations. E-Health technologies are progressing quickly, often beating the development of legal frameworks to regulate them. This makes it difficult for courts and legal authorities to keep up with the complexities of new technologies and their potential legal implications. However, the regulation regarding e-Health is of the

essence and cannot be undermined by any means to protect personal data in the health sector.

Traditional legal precedents might not directly apply to these emerging issues, leaving legal practitioners and judges without clear guidance on the related matters. It is clear that legal precedents are built upon previous court decisions, and the absence of such decisions in the e-Health context makes it difficult for lawyers and judges to establish consistent interpretations of the law when surrounded with such a situation. In Tanzania, no particular case has been decided on in the context of e-healthcare delivery services. Without legal frameworks, individuals may face difficulties litigating e-health-related cases. Another reason would be that e-healthcare services are not widely adopted or understood in Tanzania. If the use of digital technologies in healthcare is still emerging, there may not be enough disputes or legal issues to result in case law. However, that does not mean that the problem does not exist.

Chapter four revealed that limited internet connectivity, unreliable electricity grids, shortage of computer systems and other e-Health infrastructure are among significant challenges to establishing and maintaining e-Health systems in Tanzania. Reliable and high-speed internet connectivity is an essential requirement for successful e-Health systems. It is crucial for exchanging medical data, telemedicine consultations, accessing EHRs, and other online healthcare services. Some remote and rural areas in Tanzania have limited internet connectivity that compromises the essential functions of e-Health sector in protecting personal data.

To implement and maintain practices of e-Health systems, all stakeholders of e-Health

must have access to basic technologies such as computers and smartphones. A shortage of these devices can delay the benefits of e-Health initiatives. The findings indicated that most individuals in rural areas in Tanzania do not have access to e-Health facilities. Without these devices, access to e-Health services will be difficult.

The researcher further intended to compare the legal framework of protecting patients' health records in Tanzania and Germany. The findings on the legal framework show that Germany likely has stringent regulations regarding data privacy, security, and interoperability of e-Health systems. Tanzania is still developing or refining its regulatory framework to address similar concerns while ensuring accessibility and affordability of e-Health services. Cultural attitudes towards healthcare and technology can significantly influence the adoption of e-Health solutions. In Germany, there is greater trust in digital healthcare platforms and a higher acceptance of remote consultations among the population. In Tanzania, factors such as language diversity, literacy rates, and traditional healthcare practices, in most cases, shape the adoption and usage patterns of e-Health services.

Chapter Five presented a significant difference in infrastructure, technological adoption, regulatory frameworks, and cultural attitudes towards healthcare and technology. Germany typically boasts advanced infrastructure and widespread access to high-speed internet, which facilitates the implementation of e-Health solutions. In contrast, Tanzania is facing challenges related to internet connectivity, particularly in rural areas, which can hinder the adoption of e-Health technologies.

Data protection is a global phenomena. This study is all about transfer of data from one health facility to another within the country and one health facility to another outside the country. Cross border transfer of data is there fore global. The findings in chapters four and five indicated that Germany is far ahead of technological innovation, with a strong emphasis on research and development in healthcare technology. Health data from Tanzania are being transferred to so many health facilities across the World and Germany is one of the place where patients information from Tanzania are being exchanged. Thus there is a demand that there must be proper protection of personal data both from the point of origin to the destination of such data.

6.2 Conclusion

Many countries adopt e-Health applications to support healthcare delivery services in the country. These applications influence digital technologies to improve and support various aspects of healthcare delivery services and patient records management. Modern health care depends on the availability of health-related information and communication systems that form the technical foundation of e-Health. E-Health aims to increase the quality and efficiency of care, reduce costs for clinical services, reduce administrative costs of the healthcare system, and enable new healthcare delivery models. Evidence shows that e-Health can support the quality and efficiency of patient care in a great achievement. However, the successful adoption of e-Health applications also comes with challenges, including concerns about data security and patients' privacy of sensitive information, variations in digital literacy among patients and healthcare professionals, regulatory compliance, and ensuring equitable access to these technologies across different jurisdictions.

To effectively implement e-Health technologies, e-Health strategies need to consider the development of norms, regulations and laws. The study analyzes the relationship between e-Health applications and privacy concerns across Germany and Tanzania. It builds on the prior research and analysis that uses several methods to provide a cross-country analysis of the two dimensions. The use of ICT and the availability compared with e-Health access and usage of e-Health technologies among health professionals. The researcher observed that e-Health technologies have unique characteristics in their application from both countries, with a common feature of supporting patients' health, providing treatment and monitoring progress. The researcher's main concern is how to improve the user ability of e-Health technologies in Tanzania. Advancements in e-Health technologies and privacy implications depend on circumstantial factors such as healthcare organizations, national health policies, and healthcare financing positions.

The safety of electronic health applications in Tanzania, as in any other country, depends on various factors, such as the security measures in place, the reliability and accuracy of the data, and the level of training and expertise of the users. Electronic health applications can improve healthcare delivery in Tanzania by enabling better data management and more efficient communication among healthcare providers. However, there may also be risks associated with using electronic health technologies, such as data breaches, privacy concerns, and technical errors.

In conclusion, the e-Health systems in Germany and developing countries differ significantly due to variations in culture and norms, infrastructure, resources, policies, and healthcare access. Germany is known for its advanced digital health infrastructure

and widespread adoption of e-Health technologies. On the other hand, developing countries and Tanzania face challenges related to limited resources, infrastructure constraints, and inadequate regulatory framework. The efforts to bridge these gaps involve improving technology infrastructure, digital literacy, and regulatory framework to ensure that e-health technology implementation is implemented. Despite the challenges, e-Health applications hold great potential to revolutionize healthcare delivery services by making them more patient-centered, efficient, and accessible. Collaboration between healthcare providers, technology developers, policymakers, and patients is essential for advancing e-Health applications.

6.3 Recommendations

In reliance to the above research findings discussed above, the researcher recommends the following:

6.3.1 Recommendations on the Law Reforms

The researcher recommends the following to the legislature for legal reforms to the e-Health Personal Data Protection

That, Tanzanian Data privacy legislations 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.

That, Tanzanian legislature should react to the phenomenon of self-exposure on social media with the Data Protection legal framework amendment and limit research in social networks for private communication.

That, in order to fill the gaps in the legal framework on health information privacy protection, the researcher recommends that the Tanzania legal framework on e-Health should adopt international standards on e-Health related data privacy and personal data protection all these should be embraced.

That, the Tanzania domestic laws should adopt the model pointed to the current personal data protection framework available in Germany. The German data protection regime provides a comprehensive approach to protecting all classes of personal information, and in particular, it imposes detailed obligations on those who collect sensitive personal information.

That, Germany has a strong data protection regime in place, primarily governed by the GDPR at the EU level and the BDSG, the German Federal Data Protection Act—the need for a strong and independent Personal Data Protection Commission, therefore it becomes a proper case study to the Tanzanian legal position on e-Health.

That, there is a need for a strong and independent personal data protection commission in Tanzania which shall be crucial for Tanzania's today's digital age, where collecting, processing, and sharing personal data have become integral to various aspects of society and the economy.

That, the Tanzania domestic laws should ensure that personal data is collected and processed transparent, fair, and lawful and that individuals can control how their data is used. Many countries, such as the EU's GDPR, have adopted data protection

regulations to align with international standards. A robust personal data protection commission helps ensure that a country's regulations.

That, a new Tanzanian e-Health Act could be instrumental in addressing these concerns by establishing clear guidelines and regulations for the collection, storage, and sharing of electronic health data.

That, a new e-Health Act can enhance patient trust in healthcare by setting forth legal requirements for sensitive personal data protection. For this case, a dedicated e-Health Act can clarify legal obligations, rights, and responsibilities for healthcare providers, technology vendors, and patients.

That, the Tanzanian TCRA Act 2019 must be amended to recognize specifically the e-Health Personal Data Protection so as to criminalize any unauthorised access to such patients data which is restricted to public disclosure.

That, the Tanzanian Evidence Act RE 2019 must be amended so as to include a specific provision of law that provides on how evidences obtained from the e-Health discrepancies are admissible before the courts of law.

That, the Tanzania Cyber Crimes Act RE 2019 must be amended to establish and define cyber crimes related to e-Health and patient data protection and hence provide the sanctions or punishments for such crimes thereafter. This shall be a great move for the protection of the private data of the patients.

That, the Legal frameworks for data protection, telemedicine, and electronic health records in Tanzania should be established or updated to accommodate the digital healthcare landscape.

That, e-Health Policies in Tanzania must address the balancing data of access for healthcare providers while safeguarding patient privacy.

6.3.2 Recommendations on Institutional Reforms

The researcher recommends the following on Institutional reform to the e-Health Personal Data Protection

That, the Tanzania Communcion Regulatory Authority should enact special regulations that shall control the data sharing information between Health Institutions in regards to the patients Data.

That, the the Tanzania Communcion Regulatory Authority should come up with an Administrative action of integrating all health institutions in regards to the protection of the patients personal data.

That, the Tanzania Communcion Regulatory Authority should enact special procedures which shall be applied in the adjudication of personal data protection breaches by the health institution or data processors.

That, the Tanzania Communcion Regulatory Authority should contain the status of a

quasi judicial body with powers to entertain all disputes emanating from the e-Health sector.

That, the National Health Data Protection Steering Committee should be granted powers by law to possess auditing powers to all public and private health institutions in regards to data security and protection.

6.3.3 Recommendations on Policy Reforms

The researcher recommends the following on policy reform to the e-Health Personal Data Protection

There is a need for e-Health policy that is appreciated to enable and facilitate patient mobility, licensing agreements, data sharing. Regulation of personal data privacy in public and private sectors must be strong and comprehensive to safeguard people's right to privacy.

That, the new Tanzanian e-Health Policy must provide a policy framework on how the security of the data belonging to the patients shall be protected in regards to the unauthorised access or illegal use of such data to the detriment of the patient.

That, the new Tanzanian e-Health Policy must provide a policy framework so as to ensure that the data collected by the Health Institutions or data processors regarding to patients privacy are limited to lawful and fair collection of the data. The policy must provide procedures on how to collect data from the patients.

That, the new Tanzanian e-Health Policy must provide the distinction between the public disclosure of the Health Services of the health institutions and the public disclosure of patients data to the general public.

That the new e-Health Policy must provide the procedures for remedy once the personal data of a patient has been breached by a health institution or data processor.

6.3.4 Recommendations to Future Legal Researchers

The researcher recommends the following to future legal researchers regarding e-Health Personal Data Protection. That, the future legal researchers should ensure that they fill the gaps that the current thesis has failed to fill in regards to the e-Health Personal Data Protection in Tanzania.

6.3.5 Other Recommendations

The researcher recommends the following trivial aspects that may be of great reform to the e-Health Personal Data Protection

That, Electronic health has the potential to significantly improve healthcare delivery in Tanzania by making it more efficient, accessible, and cost-effective. Here are some recommendations for implementing e-Health care delivery services and the concern of privacy in personal data protection in Tanzania: implementing e-Health in Tanzania requires the development of necessary infrastructure, including reliable internet connectivity and the hardware and software needed.

That, the successful implementation of e-Health in Tanzania, or any other region for

that matter, requires the development of the necessary infrastructure, including reliable internet connectivity and the required hardware and software.

That, 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.

That, 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. This includes electronic health record (EHR) systems, telemedicine platforms, health information exchange (HIE) systems, and various health monitoring, diagnostics, and treatment planning applications. These software solutions must be user-friendly, secure, and compliant with global privacy regulations.

That, 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.

That, 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.

That, educating patients and communities about the benefits and proper use of e-Health 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.

That, the security measures are necessary to protect patient information from unauthorized access, attack or breaches. This includes encryption, secure authentication methods, regular software updates, and adherence to relevant data protection regulations.

That, protecting health data is of utmost importance to ensure patient privacy and maintain the trust of individuals using electronic healthcare services. Maintaining detailed audit trails helps track who accessed the data, when, and for what purpose. This not only aids in identifying unauthorized access but also assists in compliance with data protection regulations.

That, the private sector partners play a crucial role in successfully implementing e-Health technologies. Private sector companies often have specialized expertise, technological capabilities, and financial resources that can significantly contribute to

developing, deploying, and maintaining e-Health technologies. This can range from software development and data analytics to hardware manufacturing and infrastructure management. Their involvement can lead to the creation of new and advanced e-Health solutions that can improve patient care, streamline processes, enhance diagnostics, and enable remote monitoring and telemedicine services. Private sector partners often have extensive networks and customer bases. Their ability to market and distribute e-Health technologies can help ensure widespread adoption and use among healthcare providers, professionals, and patients.

That, there is a need to raise public awareness about their sensitive personal information's right to privacy and applicability. Due to the collective African cultures, the issue of privacy is still very new to many people, let alone data privacy. Many Tanzanians do not pay much attention to how their information is being used. Currently, we observe several complaints on social media information. Awareness will always be a key to the success of privacy and data protection.

That, the judiciary plays a vital role in ensuring one's rights are protected, which should also be the approach to privacy and personal data protection. The judiciary should be fully involved to protect this sensitive right. Magistrates and Judges should be offered several trainings on data privacy's core values and principles. Involving the judiciary and offering them training on data privacy is a valuable approach to safeguarding privacy rights in an increasingly digital world. Such initiatives can contribute to a legal environment where individuals' privacy is respected, balanced with other legitimate interests, and upheld by knowledgeable and impartial judges.

BIBLIOGRAPHY

Books and Chapters

- Acquisti, A., et al, eds. 'Digital Privacy: Theory, Technologies and Practices', (New York; Auerbach Publications, 2008.
- A. Adler-Milstein and A.K. Jha, "Sharing Clinical Data Electronically: A Critical Challenge for Fixing the Health Care System", JAMA, 307(16), pp. 1695-1696, 2012.
- Bennett, Colin J & Charles D Raab. The Governance of Privacy: Policy Instruments in Global Perspective, Cambridge: MIT Press, 2006.
- Bernal, Paul. Internet Privacy Rights: Rights to Protect Autonomy (London: Cambridge University Press, 2014.
- Bhan, Anant, Mina Majd & Adebayo Adejumo. "Informed Consent in International Research: Perspectives from India, Iran and Nigeria" (2006) 3 Medical Ethics 36.
- Brkan, M and Psychogiopoulou, E., Courts, Privacy and Data Protection in the Digital Environment, Edward Elgar, UK/USA, 2017, pp. 32-62.
- Bygrave, Lee. "The Place of Privacy in Data Protection Law" (2001) 24 UNSWLJ 277 at 280.
- Bygrave, L.A., 'Data Protection Pursuant to the Right in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol.6, No.3, pp.247-284
- Canadian Institute of Health Research. Secondary Use of Personal Information in Health Research: Case Studies (Ontario: Public Works and Government Services Canada, 2002).

- Chen, Min et al. *Big Data: Related Technologies, Challenges and Future Prospects* (Cham: Springer, 2014).
- Chui, W.H and McConville, M (eds)., *Research Methods for Law*, Edinburgh University Press, 2010, p.4
- De Hert, P and Gutwirth, S., ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action’, in Gutwirth, S et al (eds)., *Reinventing Data Protection?* Springer, 2009, pp.3-44;
- Digital Health Strategy July 2019 – June 2024. The United Republic of Tanzania, Ministry of Health, Community Development, Gender, Elderly and Children.
- Eysenbach, G., and Köhler, C., ‘Health-related searches on the Internet’ (2004) 291 (24) *J Am Med Assoc* at 2946.
- Ezeome, ER & PA Marshall. “Informed Consent Practices in Nigeria” (2009) 9 *Developing World Bioethics* 138.
- Fontaine, P., Ross, S.E., Zink, T., Schilling, L.M., *Systematic Review of Health Information Exchange in Primary Care Practices*. The Journal of the American Board of Family Medicine, 2010, p. 31.
- George, C et al., *eHealth: Legal, Ethical and Governance Challenges*, Springer, Heidelberg/New York/Dordrecht/London, 2013, vii.
- Gutwirth, Serge. *Privacy and the Information Age* (Oxford: Rowman & Littlefield Publishers, 2002).
- Greenleaf, Graham. “The influence of European Data Privacy Standards outside Europe: Implications for globalization of Convention 108” (2012) 2 *International Data Privacy Law* 68.
- Harman, Laurinda B, Cathy A Flite & Kesa Bond. “Electronic Health Records:

- Privacy, Confidentiality, and Security” (2012) 14 American Medical Association Journal of Ethics 712.
- Hohmann, J., and Benzschawel, S., ‘Data protection ine-Healthplatforms,’ in Legal and Forensic Medicine, 2013 p. 1633
- Ho, Kendall. “Health in the Digital World: Transformational Trends” in Stefane M Kabene, ed, Healthcare and the Effect of Technology: Developments, Challenges and Advancements (Hershey: IGI Global, 2010).
- Jones, Chris. “The utilitarian argument for medical confidentiality: a pilot study of patients’ views” (2003) 29 Journal of Medical Ethics.
- Kaplan, W.A., ‘Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?’ Globalization and Health, 2006, Vol.2, No.9 2006, pp.1-14.
- Keshta, I & Odeh, A., ‘Security and Privacy of Electronic Health Records: Concerns and Challenges,’ 2020.
- Khalifehsoltani, S.N and Gerami, M.R., ‘E-Health challenges, opportunities and experiences of developing countries’, International Conference on e-Education, e-Business, e-Management and e-Learning, 2010.
- Makulilo, A.B., ‘Privacy and Data Protection in Africa: A State of the Art’, International Data Privacy Law, 2012, Vol.2, No.3, pp. 163-178.
- Makulilo, A.B (Editor)., African Data Privacy Laws, Springer, Switzerland, 2016.
- Makulilo, A.B., ‘You must take medical test: Do Employers intrude into Prospective Employees’ Privacy?’, Datenschutz und Datensicherheit-DuD, 8/2010, pp.571-575.
- Mbiki M. M., “An Overview of eHealth Regulations in Tanzania” DuD • Datenschutz

und Datensicherheit: 2018, Vol 6.

Michael, J., *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology*, Dartmouth, 1994.

Mcgrath, J.E., ‘Methodology Matters: Doing Research in the Behavioural and Social Sciences’, in R. M. Baecker et al., (eds), *Readings in Human-Computer Interaction: Toward the Year 2000*, Morgan Kaufmann Publishers, 1995, p. 154.

Miles, Steven H. *The Hippocratic Oath and the Ethics of Medicine* (Oxford: Oxford University Press, 2005).

Newman, Abraham L. *Protectors of Privacy: Regulating Personal Data in the Global Economy* (London: Cornell University Press, 2008).

Savin, Andrej. *EU Internet Law* (Massachusetts: Edward Elgar Publishing, 2013).

Solove, Daniel J. *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

Verhenneman, G. and Dumortier, J., ‘Legal Regulation of Health Records: A Comparative Analysis of Europe and the US’ in George, C et al., *eHealth: Legal, Ethical and Governance Challenges*, Springer, Heidelberg/New York/Dordrecht/London, 2013, pp.25-56, at p.25.

Wacks, Raymond. *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989).

Wilson, J “Essentials of Business Research: A Guide to Doing Your Research Project” SAGE Publications, 2020.

JOURNALS, ARTICLES AND PUBLISHABLE PAPERS

Friederici, N., Hullin, C., & Yamamichi, M., 'Chapter 3: mHealth' in Kelly, T., (ed.)

Information and Communications for Development 2012 - Maximizing Mobile

(2012). Available at <http://siteresources.worldbank.org/externalinformation>

andcommunicationandtechnologies/Resources/IC4D-2012-Chapter-3.pdf

(accessed on 21 October 2020 at 20:03).

George, J., & Bhila, T., 'Security, Confidentiality and Privacy in Health of Healthcare

Data.' International Journal of Trend in Scientific Research and Development,

Vol 3(4), 2019, Pp 373-377

Hamad, W.B., 'Current Position and Challenges of E-Health in Tanzania: A Review

of Literature.' Global Scientific Journal, Vol 7(9), 2019, Pp 364-376.

O'Donoghue, J., & Herbert, J., "Data Management within mHealth Environments:

Patient Sensors, Mobile Devices, and Databases.". Journal of Data and

Information Quality. 4: 5. October 2012. Available at <https://doi:10.1145/2378016.2378021>.

Retrieved on 15 October 2020 at 13:53.

Lazarus, D., A Tough Lesson on Medical Privacy, Pakistani Transcriber Threatens

UCSF Over Back Pay, S.F. Chron. (San Francisco), October 22, 2003,

available at http://articles.sfgate.com/2003-10-22/news/17513957_1_medical-transcription-ucsf-medical-center-medicalprivacy (visited on October

18, 2020 at 20:51).

18, 2020 at 20:51).

Love, D.L., "IT Security Strategy: Is Your Health Care Organization Doing Everything

It Can to Protect Patient Information?" Journal of Health Care Compliance,

2011, p.66.

Makulilo, A.B., 'Sources of literature on data protection in Africa: a review and

analysis', 2017, Unpublished paper.

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.

Mbiki M. M., "An Overview of eHealth Regulations in Tanzania" DuD • Datenschutz und Datensicherheit: 2018, Vol 6.

Neema, E,S., 'Handling of Electronic Health Records in Tanzania: Awareness and Use of Available Regulations' East African Journal of Education and Social Sciences, Vol 4, 2023.

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

Savage, M., NHS thousands of medical records – Exclusive: Information watchdog orders overhaul after 140 security breaches in just four months, The Independent (London), May 25, 2009, available at <http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medicalrecords-1690398.html> (visited on October 19, 2020 at 17:42).

Yilma, K.M., and Birhanu, A., 'Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices,'26 (1) Journal of Ethiopian Law,2013 p. 7.

Ulyashyna, L., 'Does case law developed by the European Court of human Rights pursuant to ECHR Article 8 add anything substantial to the rules and principles found in ordinary data protection principle?', A Tutorial Paper presented at the Norwegian Centre for Computers and Law(NRCCL), Spring, 2006

PUBLISHABLE THESIS

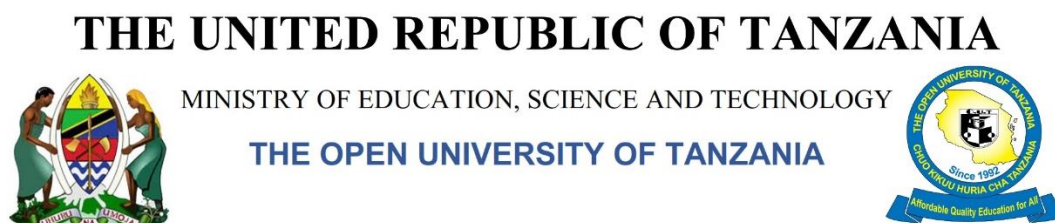
Diogenes, D., “Assessment of Independence of Regulatory Structures Governing Data Protection and Privacy in East Africa: A Case Study of Kenya and Tanzania”, thesis, The Open University of Tanzania, 2023

Kiunsi, H., “Transfer Pricing in East Africa: Tanzania and Kenya in Comparative Perspective”., ["eprint_fieldopt_thesis_type_phd" not defined] thesis, The Open University of Tanzania, 2017.

Townsend, B.A.,” Privacy and data protection in eHealth in Africa: an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking?” Doctoral Thesis, University of Cape Town, 2017, pp. 199-200.

APPENDICES

Appendix 1: Research Clearance Letter



Ref. No OUT/ PG201900315

28th May, 2023

Director,
Kinondoni Municipal
P.O Box 31902
Dar-es-salaam.

Dear Director,

RE: RESEARCH CLEARANCE FOR Ms.MBIKI MKUDE MSUMI, REG NO: PG201900315

2. The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1st March 1993 by public notice No.55 in the official Gazette. The Act was however replaced by the Open University of Tanzania Charter of 2005, which became operational on 1st January 2007. In line with the Charter, the Open University of Tanzania mission is to generate and apply knowledge through research.

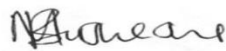
3. To facilitate and to simplify research process therefore, the act empowers the Vice Chancellor of the Open University of Tanzania to issue research clearance, on behalf of the Government of Tanzania and Tanzania Commission for Science and Technology, to both its staff and students who are doing research in Tanzania. With this brief background, the purpose of this letter is to introduce to you **Ms. Mbiki Mkude Msumi, Reg. No: PG201900315**) pursuing **PhD**. We hereby grant this clearance to conduct a research titled **Protection of Personal data in E-Health Tanzania and German in a**

Comparative perspective ”.She will collect her data at your Municipal from 2nd May to 28th may 2023.

4. In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O.Box 23409, Dar es Salaam. Tel: 022-2-2668820.We lastly thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours sincerely,

THE OPEN UNIVERSITY OF TANZANIA



Prof. Magreth S. Bushesha

For: VICE CHANCELLOR

PUBLICATIONS