UNIVERSITY OF NAIROBI

SCHOOL OF LAW

MASTER OF LAWS - 2020/2021

CYBER-SECURITY IN E-HEALTH:

A CRITICAL ANALYSIS OF THE REGULATORY FRAMEWORK IN KENYA

A thesis submitted in partial fulfillment of the requirements for the award of the degree of Master of Laws (LL.M.) of the University of Nairobi.

MUNYOLO OMUSEBE NELLY GRACE - G62/37416/ 2020

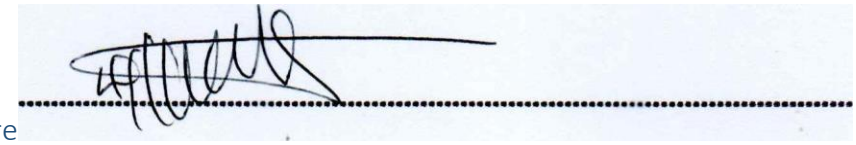
SUPERVISOR: DR. PAUL OGENDI

November, 2021

Table of Contents

DECLARATION:

1. I understand what Plagiarism is and I am aware of the University's policy in this regard.
2. I declare this thesis is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people's work, or my own has been used, this has properly been acknowledged and reference in accordance with the University of Nairobi's requirements.
3. I have not sought or used services of any professional agencies to produce this work.
4. I have not allowed and shall not allow anyone to copy my work with the intention of passing it off as his [her own work.
5. I understand that any false claim in respect of this work shall result in disciplinary action in accordance with the University Plagiarism Policy.



Signature

MUNYOLO OMUSEBE NELLY GRACE

Date: 27th November, 2021

SUPERVISOR

I confirm that the work presented in this dissertation has been researched and written by the student and has been submitted for approval as the University Supervisor.

Name: Dr. PAUL OGENDI

Signature: .....

29 NOVEMBER 2021

Date: .....

DEDICATION

To Moses, Ty, Hans, Eric and Joy without whose random road trips, this thesis would have been completed in half the time.

To Grandma Janet, my first teacher.

And Uncle Sande, my first friend.

ACKNOWLEDGEMENT

I thank God the Almighty for His grace throughout my research work.

My deep and sincere gratitude to my supervisor, Dr. Paul Ogendi. PhD, Lecturer, University of Nairobi for generously providing invaluable guidance throughout this research. His dynamism, clarity, sincerity, motivation and work ethics have deeply inspired me. It was a great privilege and honor to work under his guidance and I am extremely grateful for what he offered me.

I am extremely grateful to my parents Akumu Rubai and Patrick Munyolo for their love, prayers, and sacrifice in educating and preparing me for the future. I am particularly grateful for every time they took in my children so I could complete my project on time.

My dear husband Moses Oduor for the prayers, unwavering confidence in me sometimes against insurmountable health odds, and for being my greatest support.

Our children Ty, Hans, Eric and Joy for the love, humor and road trips.

I am equally grateful to my siblings Maureen, Senser, Naomi, Esther and Reuben for their support and valuable prayers.

Special thanks to my friend Major Lilian Adawo for the countless edits, and constantly pushing me to deliver.

My friends Vienna Amboko, Elizabeth Agina, Ivor Nyamita, Meryline Omondi, Dan Okemwa and Dr. Olive Onyango thank you for the encouragement.

Special thanks to my colleague Ms. Lydia Kenyeru for her genuine sacrifice, taking on extra shifts so I could finish this work on time.

And Delvine for the printing and binding all my drafts.

ABBREVIATIONS

1. **ACPHR:** African Commission on Human and Peoples' Rights
2. **BYOD:** Bring Your Own Device
3. **CEDAW:** Convention on the Elimination of All Forms of Discrimination against Women
4. **CESCR:** Committee on Economic Social and Cultural Rights
5. **CoK:** Constitution of Kenya, 2010
6. **CRC**: Convention on the Rights of Children
7. **DHR:** Digital Health Revolution
8. **EPR:** Electronic Patient's Records
9. **ICESCR:** International Covenant on Economic Social and Cultural Rights
10. **ICT:** Information Communication Technology
11. **IHMIS:** Integrated Hospital Management Information System
12. **ISMS:** Information Security Management Systems
13. **IT:** Information Technology
14. **KE-CIRIT/CC**- National Kenya Computer Incident Response Team- Coordination Center
15. **mHealth:** Mobile Health
16. **NHIF:** National Hospital Insurance Fund
17. **NUPI:** National Unique Patient Identifier
18. **PHI:** Protected Health Information
19. **PPPs:** Public Private Partnerships
20. **UDHR:** Universal Declaration of Human Rights
21. **UN:** United Nations
22. **WHO:** World Health Organization

LIST OF STATUTES

1. Access to Information Act No. 31 Of 2016
2. Computer Misuse and Cybercrimes Act No.5 Of 2018
3. Constitution Of Kenya, 2010
4. Data Protection Act No. 24 Of 2019
5. Health Act No. 21 Of 2017
6. Health Records and Information Managers Act No. 15 Of 2016
7. Kenya Information and Communications Act No. 2 Of 1998
8. Kenya Medical Supplies Authority Act No. 20 Of 2013
9. Pharmacy and Poisons Act No.17 Of 1956
10. Public Health Act No. 38 Of 1921
11. Science, Technology and Innovation Act No. 28 Of 2013

POLICY AND REGULATIONS

1. Kenya National e-Health Policy, 2016-2030
2. Kenya National e-Health Strategy, 2019-2023
3. Kenya Health Policy, 2014-2030
4. Health Information System Policy, 2010-2030
5. Kenya Health Information Systems Interoperability Framework 2020

REGIONAL INSTRUMENTS

1. Africa Health Strategy, 2016-2030
2. African Charter on Human and Peoples' Rights, 1981
3. African Charter on the Rights and Welfare of the Child,1990
4. African Union Convention on Cyber Security and Personal Data Protection, 2014

INTERNATIONAL INSTRUMENTS

1. Budapest Convention on Cybercrime, 2004
2. Convention on the Rights of the Child, 1989 (CRC)
3. International Conference on Population and Development, 1994 (ICPD)
4. International Covenant on Economic, Social and Cultural Rights, 1966 (ICESCR)
5. United Nations Convention against Transnational Organized Crime, 2003 (UNTOC)
6. World Health Organisation Constitution, 1946

REGIONAL LEGAL AND POLICY FRAMEWORK

E-Health Legislation in Rwanda

1. Constitution of Rwanda, 2003
2. National Health Information Exchange. 2010
3. Smart Rwanda Master Plan 2016-2020
4. National Digital Health Strategic Plan 2018-2023
5. The Health Sector Strategic Plan IV 2018-2024
6. National ICT Hub Strategy 2024

E-Health Legislation in Tanzania

1. Constitution of the United Republic of Tanzania (Cap. 2)
2. Tanzania Digital Health Strategy 2019-2024
3. Tanzania Digital Health Investment Road Map 2017-2023

E-Health Legislation in Uganda

1. Constitution of Uganda, 1995
2. Uganda National E-Health Policy, 2016
3. Uganda National e-health Strategy 2017-2021

CYBER-SECURITY IN E-HEALTH:

A CRITICAL ANALYSIS OF THE REGULATORY FRAMEWORK IN KENYA

CHAPTER ONE

INTRODUCTION

1.0 Background to the Study

The promulgation of the Constitution of Kenya (CoK) on 27th August 2010 defined the most pivotal point in Kenya's history. Arguably, this achievement is second only to the attainment of Kenya's independence in 1963. The CoK introduced fundamental changes in the governance of the country including devolution and an expanded Bill of Rights. For the first time in history, Kenya also constitutionalized socio-economic rights such as the right to the highest attainable standard of health.[1] This is important because when the right to health is enshrined in the Constitution, courts can defend the health rights of everyone because it is justiciable.

Notably, the promulgation of the CoK occurred at the cusp of the third and fourth industrial revolutions occasioned by technological advances that fundamentally altered life.[2]Through adoption of technology, the merging of physical, biological and technical worlds created a chance to link global communities lessening social inequity.[3]It also empowered society with services that improved the quality of life such as e-health, which denotes the use of ICT in healthcare.[4]

[1]Art 43, Constitution of Kenya, 2010.
[2] In the 18th century, agricultural societies became more industrialized and urbanized, propelling in the Industrial Revolution. Water and steam power were utilized throughout the First Industrial Revolution. The Second employed electricity to mass-produce. The Third employed IT and electronics to automate production. The Fourth is a digital revolution with technology convergence that blurs the difference between physical, digital and biological worlds.
[3] Thomas Philbecket, "The Fourth Industrial Revolution" 2018 72(1) Journal of International Affairs, p 17-22.
[4] Health Act No. 21 of 2017.

In Kenya, greater internet and mobile penetration facilitated the success of Safaricom's mobile money transfer M-Pesa, therefore setting the stage for many e-health innovations. Safaricom's "Daktari 1525" is an example of an e-health platform offering information on first aid and proper use of medication.[5] A partnership between Kenya's Ministry of Health and Germany-headquartered Merck Group provided a pilot e-health platform linking the Kenyatta National Hospital (KNH) to Machakos Level Five Hospital.[6] Months later, Hello Doctor in conjunction with Safaricom launched an application dubbed 'Sema Doc' enabling patients to consult doctors, get diagnosis and prescriptions without having to visit a health facility.[7] Kenya's health sector is increasingly relying upon ICT for a wide variety of administrative and clinical functions.

The COVID-19 Pandemic has created enormous interruptions in a wide range of industries around the world. In particular, it brought to light the potential for technology in mitigating difficult health situations. The measures put in place to deal with the COVID-19 pandemic necessitated social distancing in a bid to minimize interactions in turn sparked an increased uptake of e-health solutions. The Government of Kenya (GoK) also turned to e-health by setting up a call center for the screening of potential COVID-19 cases.[8]

E-health has created a huge potential to save, extend and enhance lives. Health technology has advanced several advantages such as efficiency, mistake minimization, automation and remote monitoring.[9] It is therefore arguably a mode through which the government can attain efficient, accessible, secure, and consumer-friendly health services. However, despite the benefits, e-health

---

[5] See Safaricom Newsroom, "Doctor on call: The rise of telemedicine" 09/04/2018, <https://news.safaricom.co.ke/doctor-on-call-The-rise-of-telemedicine/> accessed on 25/12/2020.

[6] Ibid.

[7] See Diana Kariuki, Kenyans Given 24 Hour Access to Doctors through Phone App, 12/8/2015 <https://www.kenyans.co.ke/kenyans-given-24-hour-access-doctors-through-phone-app > accessed 27/12/2020.

[8] See Safaricom Newsroom, "Doctor on call; Telemedicine takes its place in a pandemic" <https://news.safaricom.co.ke/doctor-on-call-telemedicine-takes-its-place-in-a-pandemic> accessed on 20/11/2020

[9] Dimiter Dimitro, "Medical internet of things and big data in healthcare" Health Informatics Research, 2016, p 156-163.

poses numerous challenges to patients, health services providers and governments alike. The most significant challenge arising from the current state of cyber security which poses legal and ethical challenges to both providers and users of e-health who are vulnerable to cyber threats.[10]

The computerized systems managing hospital processes collect a trove of private data from patients which are expected to be kept confidential. Being a rich source of valuable data, e-health systems continue to present itself as an attractive target for cybercriminals, posing a significant threat to the successful e-health mainstreaming.[11] There is a steady growth of cyber-attacks specifically targeting e-health systems and in some cases millions of medical records are stolen.[12] While we focus on achieving the best health standard by adopting ICT, large-scale cyber-attacks such as the "WannaCry" ransom ware outbreak continue to affect healthcare facilities[13]which cyber-attacks pose a real threat to the right to health.[14]

This study critically analyses the role of legal and policy frameworks to regulate e-health and address the associated challenge of cyber threats. Traditional cyber security measures are becoming increasingly ineffective in an era where cyber-attackers have developed new and more dangerous online weaponry to steal critical data.[15] Cyber-security experts need to design systems that stay ahead of the criminal elements by working to detect and destroy even the most invisible cyber-threat, which systems must be within a clear and enforceable regulatory framework.[16]

---

[10] Akhil Shenoy and Jacob Appel, "Safeguarding confidentiality in electronic health records" CQ.HE 26. 2017, p 337.
[11] Clemens Kruse, et al, "Cyber security in healthcare: A system review of modern threats and trends" (2017) THC, p 1-10.
[12] Barbara Filkins, et al, "Privacy and security in the era of digital health: what should translational researchers know and do about it?" AJoTR 2016.1560. <http://www.ncbi.nlm.nih.gov/pubmed/ 27186282> accessed 20 October 2020.
[13]Argaw Salem, et al, "The state of research on cyber-attacks against hospitals and available best practice recommendations" BMC medical informatics (2019):1-11<https://doi.org//s12911-018-0724-5> accessed 2 Nov 2020.
[14] Art. 25 Universal Declaration of Human Rights, Art. 12 International Covenant on Economic Social and Cultural Rights, Art. 24 Convention on the Elimination of All Forms of Discrimination against Women.
[15] Douglas Bisson, "Hollywood hospital pays $17,000 to ransom ware attackers" (2018) The State of Security 2016
[16] Steven Cohn, 'Privacy and Confidentiality in the Nationwide Health Information Network' (2006) WDC, p 87-89.

1.1 Statement of the Problem

The existing legal and policy framework on e-health is insufficient and incapable of addressing the challenge of cyber security. Cyber threats effecting the providers and users of e-health remain inadequately addressed in Kenya. The Health Act, 2017 envisaged that the Kenyan Parliament should have legislated this area but this is yet to happen. In particular, the legislation is expected to address the collection, use, storage, sharing and disposal of health data both at the National and County level. This study seeks to address by analyzing whether additional regulation on cyber security is in fact necessary to counter the growing cyber threats on e-health platforms.

1.2 Research Objective

This study looks into the difficulties encountered by e-health users and providers in the face of unsurmountable cyber threats. The study also seeks to evaluate the right to health framework specifically addressing cyber security challenges in e-health. Most specifically, the study aims to establish the required legal interventions in addressing cyber threats faced by providers and users of e-health.

1.3 Research Question

This study seeks to answer three key questions;

- What types of cyber threats are being experienced by providers and users of e-health?
- What is the right to health framework specifically addressing cyber security challenges in e-health?
- What legal interventions are required to address the threats faced by providers and users of e-health using the right to health framework?

1.4 Theoretical Framework

This research is based on legal positivism theory which is concerned with the law as it is, and not as it ought to be. The existence of the law, according to positivism, is one thing; its merits and

demerits are quite another.[17] Legal positivism is critical in understanding that, whatever rules there are in place in a country, depend solely on what social norms its officials consider as authoritative like legislative acts, judgments, and social practices. For this study, legal positivism answers two questions; what is the law? What are the essential functions of the law?

According to Green, rights are entitlements provided for in law under a normative framework.[18] For a right to be validly recognized there must be a law that provides for it.[19] To legitimize rights, positivists require the Government as duty holders to enact and enforce legislation on rights and providing a context in which rights are implemented. This study therefore relies on positivism to critically review the adequacy of the existing legal and policy framework regulating cyber security in e-health so as to analyze the extent to which it has succeeded in securing the providers and users of e-health against cyber threats.

1.5 Literature Review

According to David Banisar and Simon Davies in their book 'Global trends in privacy protection,' cyber-security in e-health is touted as one of the most serious ethical debates of the information age, which problem is agitated by the very fluid nature of the Internet itself.[20]The existence of an inadequately regulatory framework for instance, has failed to effectively oversee implementation focused at securing e-health practice from cyber threats, so much so that, despite gains in overhauling the regulatory framework, a majority of existing laws and regulations remain onerous, out of step with contemporary realities and unsupportive of cyber security needs of e-health.[21]

[17] John Austin, 'The province of Jurisprudence determined' (1982) J Murray, p 33-45.
[18] Leslie Green, Legal Positivism; The Stanford Encyclopedia of Philosophy (2003).
[19] ibid.
[20] David Banisar and Simon Davies, 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments' (1999) J. Marshall J. Computer & Info. L. 18, p 11-18.
[21] Sethi Nayha, and Graeme T. Laurie, 'Delivering proportionate governance in the era of e-health: making linkage and privacy work together' (2013) 13(2-3) Medical law international, p 168-204.

Coincidentally, cyber security in e-health has received little attention in Kenya despite the regulatory framework governing e-health being a widely researched on topic with an emerging body of literature. First, there is limited Kenyan literature on whether the existing legal and policy framework on e-health is sufficient and capable of addressing the challenge of cyber security. This limited literature has neither analyzed the threats being experienced by providers and users of e-health, nor proposed necessary legal interventions required to eliminate threats faced by providers and users of e-health as determinant elements to the successful implementation of e-health.

This study attempts to review existing solutions from the international arena on the basis that, the extension of the literature though not Kenyan specific, is important in proposing necessary legal interventions required to address cyber threats faced by providers and users of e-health through additional regulation on cyber security, as well as good cyber security practices aimed at building a cyber-resilient e-health practice.

1.5.1 Cyber Security

According to Stein Schjolberg, Cyber security is defined as a set of procedures for protecting computer-based devices, documents, and services from unauthorized access, modification, and destruction using mechanisms that either completely eliminate cyber threats or mitigate the effects of cyber-attacks.[22] Cyber-attacks against the healthcare sector are steadily growing with millions of medical records stolen through hacking, ransom ware, and insider threats among others.[23] This study therefore seeks to advocate for adequate, sector specific cyber-security legislation, for an effective adoption of e-health.

[22] Stein Schjolberg, ITU Global Cyber security Agenda, High-Level Experts Group, Report of the Chairman<https://www.itu.Int/en/action/cybersecurity/Documents/gca-chairman-report.2008>p 27, accessed on 1/5/2021.
[23] Alwi Williams, Patricia AH, and Andrew Woodward, 'Cyber security vulnerabilities in medical devices: a complex environment and multifaceted problem' (2015) 8, Medical Devices Auckland, NZ, p 305-316.

Ideally, an effective cyber security framework involves a combination of technical, organizational, policy, and legislative elements.[24] Technical aspects involve safeguarding computing systems and networks. Organizational aspeect is concerned with creating institutional capacity to support cyber security like setting up enforcement agencies and Computer Emergency Response Teams (CERTs). Policy aspects involve laws that prohibit actions breaching protection, integrity, and availability of data, along with efforts to promote cross-border collaboration.[25]

Jerome Uchenna in his Journal 'Cyber security Law and Regulation' strongly holds the view that, given the explosive increase of cyber-attacks, successful models are necessary for establishing a protection framework to achieve intended outcomes of intrusion prevention, vulnerability mitigation and threat deterrent while providing a favorable return on investment.[26] Unfortunately, establishing successful cyber threat countermeasures in e-health is not easy owing to a constantly changing threat environment and ease with which hackers upgrade their art. Uchenna therefore proposes that organizations need to adopt a cyber-security policy that is detailed but easy to understand, while observing industry best practices, regulatory compliance, and potential legal liability.[27] Since technology and policies are only as good as the people administering them, health providers have a responsibility to educate everybody in the organization to practice safe computing comprising safe web surfing, safe email use, right use of social media, and responsible cloud use.

1.5.2 Telemedicine

Jennett Penny, et al in their journal article 'The socio-economic impact of tele-health: a systematic review' opine that, telemedicine holds great potential for improving delivery of health services by

[24] Jerome Uchenna, 'The African Union Convention on Cyber security: A Regional Response towards Cyber Stability?' (2018) 12(2) Masaryk University Journal of Law and Technology, p 91-109.
[25] Gercke Marco, 'Understanding Cybercrime: A Guide for Developing Countries' (2009) IT Union, p 84.
[26] Jerome Uchenna, Cyber security Law and Regulation (Wolf Legal Publishers 2012) p 10-22.
[27] Jerome (n 24) p 30-42.

enhancing access, quality and efficiency.[28] However, despite the promise to profoundly transform the delivery of health services, legal and ethical concern pertaining to data dignity and privacy continue to challenge its adoption. According to Martin Njoroge, et al 'Assessing the feasibility of e-health and m-health: a systematic review and analysis of initiatives implemented in Kenya, political and policy reforms must be undertaken in order for cyber-security to be effectively incorporated into m-health. This includes adopting a collaborative, inclusive, pragmatic approach to policymaking in the area of cyber- security.[29] Addressing cyber-security is therefore imperative if telemedicine is to be implemented equitably and to the highest ethical standards.

1.5.3 Health Information Systems (HIS)

According to Elesban Kihuba, et al in their book 'Assessing the ability of health information systems in hospitals to support evidence-informed decisions in Kenya,' everyone in healthcare including governments, patients and health officials use HIS.[30]In Kenya, HIS has generated a huge pool of data, stored in different formats across various systems and locations. Despite cyber-security being a primary concern, the government is yet to legislate its use, making it a desirable target for cyber criminals.

1.5.4 Information for Citizens

Technological advancement has made profound impact on health care by giving more power to patients to actively participate in their own health care decisions. Jane Grimson, et al in the journal article 'The SI challenge in health care' opine that this has converted the healthcare sector into an

[28]Jennett Penny, 'and others',' The socio-economic impact of telehealth: a systematic review' (2003) 6, Journal of telemedicine and telecare, p 311-320.

[29] Martin Njoroge, Dejan Zurovac, Esther Ogara, Jane Chuma, and Doris Kirigia, 'Assessing the feasibility of eHealth and mHealth: a systematic review and analysis of initiatives implemented in Kenya' (2017) BMC Research, p 1-18.

[30]Elesban Kihuba, 'and others,' Assessing the ability of health information systems in hospitals to support evidence-informed decisions in Kenya, (Global health action 7, 2014) 1: 24859.p 124-126

information-intensive knowledge-based enterprise with a significant amount of data making informed consent the most delicate aspect of e-health.[31]

According to Lokesh Nijhawan, et al in their journal titled 'Informed consent: Issues and challenges,' while electronic consents bring numerous forms of interactions, the challenge lies in the scope of this legal duty, specifically whether healthcare professionals still have the same disclosure obligations in an information-overloaded internet world.[32]Kenya has for instance no frameworks for tele-consent and e-signatures, or modalities for moving from paper-based consent to digital consent. Most unfortunately however, patients remain ignorant of risks related to cyber-security concerns of e-consents, which is a value- issue that goes to the very nature of e-health.

1.5.5 E-Learning

By offering flexible services with both online and offline capabilities, e-learning has transformed medical education for the 21st century. E-learning systems in addition to being diversified rely on the internet to collect all necessary information. This is a difficult task especially because the internet has become a hotbed for unlawful operations by cybercriminals. Bandara and Maher in their book 'Cyber security concerns in e-learning education' opine that, by virtue of its open, distributed and interconnected nature, e-learning continuously expose systems to a prevalence of cyber-attacks like viruses, worms, denial of service, espionage, and theft.[33] Kenya for instance lacks laws and policies in e-learning systems specifically focusing on cyber-security that would ensure only authorized actors have access to the right information. To ensure increased investment in health so to achieve UHC by 2030, the Government needs to facilitate the strengthening of

[31] Jane Grimson, William Grimson, and Wilhelm Hasselbring, 'The SI challenge in health care' (2000) 43(6) Communications of the ACM, p 48-55.

[32] Lokesh Nijhawan 'and others,' 'Informed consent: Issues and challenges' (2013) 3(4), Journal of advanced pharmaceutical technology & research 4, p 134.

[33] Loras Bandara and K. Maher, Cyber security concerns in e-learning education (2014): 0728-0734, p 102-112.

partnerships on cyber-security in healthcare which will encourage players to gain from techniques currently prevailing both within and outside the country.[34]

1.5.6 E-Legislation

In the past, the development and design of cyber security laws and policies has not been consultative; but mostly pushed by government without much regard to the unique environment surrounding e-health. Consequently, the legislative framework has failed to acknowledge the special cyber-security needs of e-health users and providers, thereby exposing it to countless cyber-attacks.[35] For example, the regulatory framework fails to address the critical area of responsibility delegation and follow-up on actual implementation of cyber security to identify who secures what, when, and how. This lack of clarity of roles and responsibilities of various stakeholders has left a void that helped to grow cyber-attacks.

Poor coordination at operational level has also led to duplication of services and sub-optimal use of scarce resources.[36] Specifically, there is no institutional structures inside government to monitor the implementation of cyber-security laws on e-health programs. Neither is there a structure for coordinating health stakeholders to enable their participation in developing and implementing cyber security policies, the absence of which makes it impossible to follow implementation progress to identify policy gaps, take remedial action, build feedback mechanisms and assess the impact of cyber security laws on e-health.

Cosmas Zavazava, et al in their journal article titled 'The Role of ICT in Advancing Growth in Least Developed Countries: Trends, Challenges and Opportunities' opine that, besides forming an integral and invisible part of embracing technology, cyber-security legislation needs to be at the

[34] ibid.

[35]França Reinaldo Padilha, Ana Carolina Borges Monteiro, Rangel Arthur, and Yuzo Iano, 'An Overview of Data Privacy in Healthcare in the Current Age' (2021) Data Protection and Privacy in Healthcare p 1-20.

[36] ibid.

core of national technology strategies[37]which calls for a collaborative approach built on fundamental human rights and collective responsibility. There also exists a need for greater standardization and harmonization of cyber security laws within the region, which require greater co-operation between East African nations, so as to negotiate a solution that is appropriate and equitable.[38] In general, for e-health to effectively protect the right to health, an enabling legal and policy framework is required, which calls for among other reforms, additional specific regulation on cyber security.

1.6 Hypothesis

This study progresses from the hypothesis that a comprehensive e-health regulatory framework is required to adequately address the cyber security threats in Kenya's healthcare system.

1.7 Research Methodology

This is a multidisciplinary study comprising law, health, ICT and security. The research methods included a desk review of existing international literature and policy proposals on e-health cyber security, a review of cyber security standards and their implementation in various jurisdictions, as well as observation and recording of phenomena. These component processes were performed between September 2020, and August 2021. On both primary and secondary sources, multiple data collection methodologies have been used. The primary source materials were the CoK, statutes, and judicial precedents which contain a wealth of first hand and in-depth information on cyber-security in e-health, in order to determine whether existing cyber-security laws and legal

[37] Cosmas Zavazava, Lilia Perez-Chavolla, Johannes Bauer, Vanessa Gray, Eric Otenyo, Eric Samarajiva, and Richard Labelle, The Role of ICT in Advancing Growth in Least Developed Countries: Trends, Challenges and Opportunities (2011), p 98-102.

[38]World Health Organization, Everybody's business - Strengthening health systems to improve health outcomes: WHO's framework for action (2007).p 30-33

institutions serve society's e-health needs. Secondary data was gathered from a variety of sources as well as a literature study of papers that were easily accessible in print and on the internet.

International comparative methodology has been used in this study. This included an analysis of documents sourced from the Ministries of Health, complemented with a review of the WHO's e-health strategy development toolkit, as well as other international frameworks. This was necessary for purposes of conducting a cross-jurisdictional analysis of the cyber security regulatory framework in Rwanda, Tanzania and Uganda, and what cyber-attacks threaten the East African Community's e-health agenda. Having been incentivized towards adopting e-health, there are remarkable similarities in the management of e-health platforms across the EAC which makes it necessary to critically explore both enablers and barriers experienced across board. Although original motivators and specific approaches have varied across the selected jurisdictions, all countries have made exceptional gains in cyber securing e-health platforms in the decade and recognize additional opportunities to continue to strengthen the capacity that has been created so far. The researcher used online resources such as the web libraries of key e-health implementers like the Digital REACH Initiative and government websites, as well as literature searches to find reports from various national and regional projects. Published papers on e-health cyber-security were supplemented by a desk examination of unpublished materials to assess the coherence and logical soundness of laws. Observation was used as a visual method on both participants and non-participants. In the former, the researcher sought to interact with the respondents in order to observe and record a phenomenon, whereas in the latter, the researcher sought to observe and record a phenomenon from a distance. This was done to assess insider threats particularly on employees with allowed access to sensitive information who are careless and make unintentional mistakes in the course of their regular device use, as well as employees using weak passwords,

unencrypted computers, and other non-compliance issues that are preventable with proper access review systems. The researcher relied on this approach for a broader and more enriched analysis of whether the users of e-health were conscious of the danger cyber-attacks posed, and what role if any, they played in exposing e-health platforms to cyber-attacks.

1.8 Justification of the Study

The research is important because it analytically examines e-health legislation in Kenya, with a particular focus on cyber security. Specifically, this study is significant in demonstrating a clear view of the cyber security landscape on e-health including; an examination of the legal framework; it's importance in achieving the right to health; an analysis of the threats being experienced by providers and users of e-health; as well as proposal for legal interventions required to eliminate threats faced by providers and users of e-health.

1.9 Scope and Limitations of the Study

Cyber security has many facets that could not be addressed comprehensively in this research. This study therefore primarily focused on critical cyber threats affecting Kenya's e-health platforms. This study's findings have some practical limits. There has never been a previous research analyzing cyber security in e-health in Kenya, the citations and referencing of which, would have constituted the basis of the literature review while providing a theoretical foundations for the research question under investigations. There is also limited access to data provided by the National KE-CIRT/CC on health sector specific cyber threats due to the sensitivity and confidentiality surrounding health records. Though important, the sensitive data including the names of endangered hospitals and data which could place patients, the public, or vulnerable groups at risk has been anonymised or redacted prior to sharing.

1.10 Chapter Breakdown

The research consists of six chapters as explained below.

Chapter One: Introduction

The chapter lays out the general structure of the study.

Chapter Two: An overview of the cyber threats cases experienced by providers and users of e-health platforms in Kenya.

The chapter analyses the cyber threats frequently experienced by e-health providers and users.

Chapter Three: The international framework for addressing cyber threats in e-health.

The chapter assesses the legislative framework for cyber security in e-health under international and regional laws, as well as the gaps that exist.

Chapter Four: E-health legislation in selected jurisdictions and how they address cyber security threats.

This chapter explores the legislative framework in selected jurisdictions to establish whether the current regulation is adequate, and whether additional specific regulation is required to address the cyber security threats effecting providers and users of e-health systems.

Chapter five: The National framework governing cyber security in e-health

This chapter analyses the legislative framework in Kenya to establish whether the current framework is adequate, and whether additional specific regulation is required to address the cyber security threats effecting providers and users of e-health systems.

Chapter six: Conclusion and Recommendations

The study having demonstrated consequences of not having specific legal protections in place for cyber security in e-health, this chapter proposes necessary legal interventions required to address

the cyber threats faced by providers and users of e-health using the right to health framework; as well as good practices aimed at building a cyber-resilient e-health practice.

2.0 CHAPTER TWO

AN OVERVIEW OF THE CYBER THREATS CASES EXPERIENCED BY PROVIDERS AND USERS OF E-HEALTH PLATFORMS IN KENYA.

2.1 Introduction

The adoption of e-health offers a wealth of medical convenience. Unfortunately, as a wealthy source of valuable data that is poorly protected, it is also most susceptible to dangerous cyber-threats.[39]While the volume of medical information dictates the use of technology, a failure of e-health systems to include security as a priority is making e-health systems compromise easier.[40] As working remotely continues to be a new reality, cyber threat actors are exploiting e-health vulnerabilities to carry out attacks, mostly attributed to lack of information security personnel and poor information management frameworks.

Despite attempts to secure Kenya's cyber space by assuring the safety of electronic transactions and online services such as e-Government and health, cyber security attacks continue to jeopardize e-health's confidentiality, credibility, and availability for both providers and users.[41] Proliferation of e-health platforms has also birthed new forms of cyber-threats, with computer systems, the internet, and databases providing an incentive to promote conventional crimes such as fraud; as well as a vehicle for new forms of crimes that arise in tandem with the emergence of various e-health technologies.[42] This chapter therefore seeks to critically analyze the emerging cyber threats

[39]Yingnan Sun, Frank P-W. Lo, and Benny Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey." IEEE Access 7 (2019): 18.
[40]Hossam Ahmed, Abeer Alsadoon, Prasad, Costadopoulos, Lau Siong Hoe, and Amri Elchoemi. "Next generation cyber security solution for an e-health organization." In 2017 5th International Conference on Information and Communication Technology (ICoIC7), pp. 1-5. IEEE, 2017.
[41] National KE-CIRT/CC Cyber Security Report for the Period January to March 2021.
[42] Martin Guy, Paul Martin, Chris Hankin, Ara Darzi, and James Kinross. "Cyber security and healthcare: How safe are we?" Bmj 358 (2017). 23-24

cases posing a significant danger to Kenya's e-health landscape while demonstrating why cyber security in e-health is a major concern in progressively achieving the right to health.

2.2 The Threat Landscape

Cyber threats are defined as adversaries displaying strategic actions and ability to manipulate cyberspace with the aim of causing harm to people, information, operations, and property.[43]The Communication Authority of Kenya (CAK) in its latest sector statistics report revealed an uptick in cyber threats mostly attributed to the work-from-home shift and increased uptake of e-commerce due to the COVID-19 pandemic. The report further noted that the most common threats were detected from hacktivists, criminal organizations seeking financial gain, and state-sponsored security, and intelligence services pursuing individual national security objectives.[44] In general, cyber threats are broadly categorized into two; cyber warfare, and cyber-crime.

2.2.1 Cyber Warfare

Cyber warfare is malevolent activity which poses a threat to the security, defense mechanisms or vital installations of a state resulting from vulnerabilities in critical infrastructures including hardware and software flaws.[45] Virtually, every element of cyber warfare has a transnational dimension that affects device users. Cyber warfares in the e-healthcare landscape take the form of trying to shut down a facility's computer networks or revealing personal patient files to the public with the general effect being a compromised patient care, and diminished trust in the health systems.[46] Every member of society faces a serious repercussions of cyber warfare, such as the loss of important and vital data and an inaccessibility to legitimate services. For example, in 2017,

[43]Zeadally Sherali, Jesús Téllez Isaac, and Zubair Baig. "Security attacks and solutions in electronic health (e-health) systems." Journal of medical systems 40, (2016) p 12.
[44] During the period January to March 2021, The National KE –CIRT/C, Cyber Security Report (n 41) detected 28,247,819 cyber threat attempts compared to the 56,206,097 detected in the previous period of October to December 2020.
[45]Angela Clem, Sagar Galwankar, and George Buck. "Health implications of cyber-terrorism." Prehospital and disaster medicine (2003) 18(3) p 272-275.
[46] ibid.

the WannaCry ransomware crypto worm launched the global attack against computer systems windows Operating Systems, encrypting data and making demands for ransom payments, with total damages ranging into billions of dollars from an estimated 300,000 users in about 300 countries. Despite provided advisories and the availability of security patches, hospitals experienced system-wide shut downs, postponements in treating patients, and malfunction in devices connected such as MRI machines and blood storage coolers.[47] Despite the fact that the cyber-attack was not directly targeted at healthcare, the harm it caused was unparalleled.

The CAK confirmed that at least nineteen businesses in Kenya had been impacted by the WannaCry virus attack without disclosing the sectors targeted. The Authority instead, through National Kenya Computer Incident Response Team (National KE-CIRT) coordinated the virus's eradication, given that almost 80 per cent of Kenya's servers, including those used in public healthcare facilities, run on the Windows operating system, with another 16 per cent on the Linux variant.[48] Fortunately, beyond the WannaCry, no major cyber-attack has been effective against Kenya's healthcare system. There is however concern that cyber threats are growing in number and yet a sizable portion of Kenya's healthcare system is ill-equipped to handle them.

2.2.2 Cybercrime

Cybercrime is a broad term that applies to illegal activity involving use of a computer or network as source, weapon, goal, or location of the crime.[49] Cybercrime has proven to be an extremely lucrative niche in many respects, as it enables offenders to easily operate transnationally and earn enormous profits without taking excessive risks. These offenses fall into two categories: those

[47]Jesse Ehrenfeld. "Wannacry, cyber security and health information technology: A time to act." Journal of medical systems (2017): p 104.
[48] See <https://www.the-star.co.ke/news/2017-05-22-panic-as-wannacry-virus-hits-19-kenyan-firms/>22 May 2017 accessed on 1/12/2020.
[49]Hossam Ahmed (n 40) p 30-42.

directed at computer networks or devices, and those enabled by computer networks or devices but with a primary goal that is not a computer network or device.

2.2.2.1 Crimes Targeting Computer Networks or Devices

This is the most basic form of computer-related offense primarily targeting confidentiality, credibility, and availability of computer data and systems, including unauthorized access, malware and denial of service attacks.[50] This category effects data both at rest and in motion, as well as networks like firewalls, servers, routers, switches, and mobile devices. In 2015 for instance, Anthem Blue Cross experienced a healthcare breach as a result of which 78.8 million patient records were stolen, with the cyber-attackers claiming sensitive data of their patients.[51]

2.2.2.1.1 Access without Authorization (Hacking/Computer Trespass)

This includes offenses of hazardous threats and assaults against device and data. Unauthorized intrusion, including hacking, cracking and computer trespassing are principally illegal as they prevents users of systems and data from legitimate services. Hacking is a leading cause of cyber threats to e-health, with hackers using inadequate protection to target e-health sites, denying access to health services and causing deliberate damage.[52] Ultimately, such compromises lead to financial losses, loss of credibility and reduced patient safety, especially for patients with stigmatizing diagnoses like sexual or mental health conditions.[53] Hacking infects medical devices by establishing vulnerable links in hospital safety defenses, and equipment like MRI machines which had not previously been identified as a risk factor. Hackers also leverage on system and network

[50] Serianu. Africa Cyber Security Report Kenya, 2019/2020. Local Perspective on Data Protection and Privacy Laws. Insights from African SMEs.
[51] Kristie Chung. "Applying systems thinking to healthcare data cyber security." Diss. Massachusetts Institute of Technology, 2015. P 80
[52] Hossam Ahmed (n 40) p 52-60.
[53] Ibid.

vulnerabilities to unveil even more aggressive hacking attacks to manipulate critical healthcare systems, thereby compromising public safety.[54]

With the rollout of COVID-19 vaccines, there is a notable move by hackers to compromise healthcare and pharmaceuticals applications of organizations involved in the COVID-19 vaccine development and distribution. This is being carried out for purposes of spreading disinformation campaigns designed to undermine trust in the vaccines.[55]

2.2.2.1.2 Malware Attacks

Malware are malicious codes or programs that give cyber threat actors explicit control over a system.[56] Malware utilizes known communication devises to spread through emails, texts, and infected files downloaded from the internet. In Kenya for instance, Emotet, one of the most expensive and devastating malware variants ever seen employs a variety of persistent and evasion techniques to remain undetected while circulating via phishing and spam emails containing malicious links or attachments.[57]

Ransomware is an advanced sub-type of malware that enables cyber threat actors to seize control of a computer system and prevent users from accessing services unless a ransom is paid.[58] This is a growing concern in e-health with the monetary value of the average ransom significantly increasing. The development of ransomware variants allows cyber threat actors to sponsor the development of tools to execute attacks, with the ransomware developers earning a commission on successful ransom payments. This has led to the development of sophisticated ransomware variants that use anti-forensic techniques to cover their footprint making them difficult to detect.[59]

---

[54] ibid.
[55] National KE-CIRT/CC, Cyber Security Report (n 41).
[56] Mamoona Humayun, et al. 'Internet of things and ransomware: evolution, mitigation and prevention' (2020) Egyptian Informatics Journal, p 140-144.
[57] National KE-CIRT/CC, Cyber Security Report (n 41).
[58] Mamoona (n 55).
[59] National KE-CIRT/CC, Cyber Security Report (n 41).

Viruses are self-replicating programs infecting machines and then spreading to other computers connected to a network.[60]

Worms constantly create usable copies of themselves, until they consume all available memory on a computer.[61] Trojan horse, which is most often downloaded unintentionally, refers to a class of technology threats that appear to perform a useful function but actually perform unknown malicious functions that grant unauthorized access to the host machine.[62]Spyware, on the other hand is secretly installed on a user's computer so as to intercept or partially control the user's computer interactions without the user's knowledge or agreement. This is accomplished by altering computer settings, resulting in sluggish communication speeds and/or the loss of internet or other program features.[63]

For example, in 2016, the Lukaskrankenhaus Neuss, a public hospital in Germany, received multiple error messages as a result of a ransomware attack that used a social-engineering technique. In order to examine and disinfect all compromised systems, servers and computer systems were brought offline. While high-risk procedures were rescheduled, personnel continued to work utilizing pen, paper, and fax machines.[64] Even in the absence of an actual data breach, it took the hospital several months before their normal operations normalized.[65]Generally, illegal access in e-health is difficult to manage because of the sophisticated nature of skills employed by the hackers with an uncanny ability to destroy, erase, deteriorate, modify, transmit, or alter computer data without leaving digital footprints.

---

[60] ibid.
[61] ibid.
[62] ibid.
[63]AbuKhousa, Eman, Nader Mohamed, and Jameela Al-Jaroodi. "E-health cloud: opportunities and challenges." Future internet 4, no. 3 (2012): 621-645.
[64]Steffen S. “Hackers hold German hospital data hostage.” DW. 2016. http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030. Accessed 2/2/2021.
[65]Zorz Z.”Crypto-ransomware hits German hospitals.” Help Net Security 2016. https://www.helpnetsecurity.com.crypto-ransomware-hits-german-hospitals Accessed on 2/6/21

2.2.2.1.3 Attempts at Denial of Service

A Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack is a malicious attempt to prevent legitimate users from accessing a computer resource by interfering with the normal traffic of a targeted server, service, or network.[66]DoS attacks are often defined as coordinated attempts to prevent an internet service from functioning efficiently or at all, either permanent or temporary, with perpetrators of DoS attacks typically targeting services located on high-profile web servers such as hospitals.[67] Flooding the target hospital machines with external communications requests, so that it cannot react to legal traffic, or replies so slowly that it effectively fails to answer is one common method of a DoS attack on e-health platforms.

In 2014 for example, Anonymous, a known hacktivist group launched a DDoS attack on Boston Children's Hospital. This was after the hospital requested one of its patients, a 14-year-old girl, be admitted as a state award and custody be taken away from her parents, Doctors having concluded that the child's illness was a psychological condition, and that her parents were pressuring her to undergo unnecessary therapies for a disorder she did not have. Members of the Anonymous group, saw it as an affront to the girl's rights, [68]and responded by launching DDoS assaults against the hospital's network, cutting off Internet access to others on the network, including all of its hospitals. For almost a week, patients and staff were unable to access their online accounts to check appointments, test results, and other case information.[69]

[66]Sherali Zeadally, Jesús Téllez Isaac, and Zubair Baig. "Security attacks and solutions in electronic health (e-health) systems." Journal of medical systems 40, no. 12 (2016): 1-12.
[67] ibid.
[68]Hongach Jr, William J. Mitigating Security Flaws in the TCP/IP Protocol Suite. Diss. Utica College, 2018.p 34-35
[69] ibid

2.2.2.2 Crimes Enabled by Computer Networks or Devices but With a Primary Goal That Is Not a Computer Network or Device

This is a broadened version of computer-related crimes in which computers and telecommunications networks are used to target legal interests that are usually shielded by criminal law from attacks using conventional methods.

2.2.2.2.1 Cyber Stalking and Cyber Bullying

One danger arising out of e-health practice is cyber-trauma, which refers to a variety of trauma-referrals associated with the use of, and interaction in cyberspace like extreme violence, graphic material, sexual content, and cyber-victimization and bullying.[70] Cyber-stalking on the other hand is the use of the internet or other electronic means by an individual to harass, bully, or stalk an individual, [71]with cyber bullies relying on private information extracted from breached e-health platforms to profile victims. Social media, texting, online forums, and now even computer games have broadened the definition of cyberbullying to encompass both overt and subtle harassment in the digital environment,[72] the anonymity affording abusers on the internet creating a new venue for bullying to take place. As a result, cyberbullying should be a regular component of any child's mental health examination as a healthy approach.[73]

2.2.2.2.2 Health Fraud, Forgery and Identity Related Crime

The adoption of e-health has opened up new opportunities to steal, duplicate, and dishonestly misuse personal information, pointing to a series of complex violations of identity data sparked by cybercrime's evolution. Fraud is described as any deceptive misrepresentation of facts intended to

[70]Suman L. N. 'Cyber Trauma: An Overview' (2018) 45(1), Indian Journal of Clinical Psychology, p 7-17.
[71] ibid.
[72]Kathleen Bartholomew, and Karen Curtis. "High-tech, high-touch: Why wait?" Nursing management 35.9 (2004): 48-54.
[73] Ainoa Mateu, Ana Pascual-Sánchez, Maria Martinez-Herves, Nicole Hickey, Dasha Nicholls, and Tami Kramer. "Cyberbullying and post-traumatic stress symptoms in UK adolescents." Archives of disease in childhood 105, no. 10 (2020): 951-956.https://adc.bmj.com/lookup/doi/10.1136/archdischild-2019-318716. accessed on 1/6/2021

persuade anyone to do or refrain from doing anything that results in financial loss.[74] In e-health, fraud revolves around obtaining a profit by modifying, damaging, suppressing, or stealing data, typically to disguise unauthorized transactions for illicit purposes.

Phishing is a type of e-health fraud in which a person impersonates a trustworthy person in an electronic message in order to steal confidential information.[75] Cyber criminals use phishing to spread attacks by convincing users to enter personal information on a fake website that looks and feels almost similar to the real one. Computer-related forgery entails the unauthorized creation or alteration of data so that it acquires a different evidentiary meaning in legitimate transactions that depend on the data's authenticity.[76] Identity related crime covers all forms of illicit conduct including identity fraud and identity theft. As an e-health-related offense, identity theft refers to deception in which someone pretends to be somebody else in order to acquire benefits. Identity theft is the use of a fake identity to commit fraud.[77] Identity fraud is used to aid activities such as hacking and identity cloning, which are used to target payment systems, including medical insurance.

2.2.2.2.3 Illegal Sale of Controlled Substances, Including Pharmaceutical Preparations

Drug dealers are rapidly taking advantage of technology to sell and distribute illicit drugs via encrypted e-mail and other health technology, posing a danger to e-health platforms. The selling of illicitly produced natural and synthetic products like heroin or amphetamines, as well as prescription preparations containing narcotic drugs and psychotropic substances, is taking place

[74] Marlene Heffner and Dixie Farley, 'Health Fraud: A growing problem' (1986) 151(7) p 374-379.
[75] ibid.
[76] ibid.
[77] Allison Stuart, Amie Schuck, and Kim Lersch, 'Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics' (2005) 33(1) Criminal Justice, p 19-39.

on the internet.[78] Traditional drug formulas that were once closely guarded secrets have now been made accessible to everyone with a computer.[79]

Unfortunately, due to a lack of cooperation between judicial, prosecution, police, customs, and other entities with little experience investigating drug-related internet-based crime, illicit trade in internationally regulated licit drugs ordered through the internet continues to increase.

2.2.2.2.4 Intellectual Property Crimes

Copyrights, trademarks, patents, industrial design rights, and trade secrets are common forms of intellectual property in e-health, the majority of which rights provide authors of original works with an economic opportunity to produce and exchange innovations through a kind of temporary monopoly. Intellectual property rights violations, on the other hand, are among the most frequently committed offenses on e-health sites, posing a danger to both copyright holders and others who work professionally with computers.[80]

Without the permission of the copyright holder, protected e-health work such as literary, photographic, visual, and computer programs are reproduced and disseminated on the internet.[81] The ease and scale with which unauthorized copies are made, reproduced and disseminated among electronic networks makes it necessary to enhance international cooperation against intellectual property crimes so as to secure e-health.

---

[78] Tim Mackey, and Bryan Liang, Pharmaceutical digital marketing and governance: illicit actors and challenges to global patient safety and public health (2013) 9(1), p 1 - 22.
[79] ibid.
[80] Liu Qiong, and others, 'Digital rights management for content distribution', proceedings of the Australasian information security workshop conference on ACSW frontiers, (2003) p 21.
[81] ibid.

2.2.2.2.5 Insider Threats

Employees that target the organization's cyberspace properties are known as insider threats.[82] These are divided into three categories: malicious actors that steal data or inflict damage on intent, actors who are unintentionally exploited by third parties, and those who are careless and make unintentional mistakes. High-level access users, such as hospital system managers, often search for system loopholes by which they can obtain unauthorized access or ride on the rights of other users without their permission to target organizational structures for a variety of reasons, including dissatisfaction, retaliation, and extortion.[83]

Regular device users with allowed access to sensitive information may also occasion insider threats. Employees of all cadres often accumulate access levels than they need for their roles, generating higher security risks that are preventable with proper access review systems. Employee error still exists, in which workers make health-care organizations vulnerable to attack by using weak passwords, unencrypted computers, and other non-compliance issues.[84]

In April 2020, for example, Christopher Dobbins, a former employee of a medical device packaging company, was charged with hacking into his former employer's package shipping system and deleting shipping information, causing the delivery of personal protective equipment to be disrupted in the midst of a global pandemic. Dobbins had administrator access to the company's computer systems including shipment information while worked there. Dobbins was fired from his job at the corporation in early March 2020, and he lost access to the company's computer systems.

[82] Mercy Okikiola and others, 'A new framework for detecting insider attacks in cloud-based E-Health care system' (2020) International Conference in Mathematics, Computer Engineering and Computer Science IEEE, p 120-128.
[83] ibid.
[84] ibid.

He logged into the company's computer systems three days after receiving his final paycheck, using a phony user account he had created while employed there. Dobbins allegedly created a second false user account after logging in using the fake user account and used that account to change roughly 115,581 records and remove approximately 2,371 entries. Dobbins then disabled both phony user identities and signed out of the system as a result of his activities. The company's shipping operations were affected by the alterations and deletions to its records, slowing traffic in the delivery of critical PPEs to healthcare professionals.[85]

With a growing amount of confidential health data being remotely stored on the cloud, e-health systems are constantly under threat. The use of cloud applications to support remote information system infrastructure with the continued shift to remote working has resulted in a considerable increase in malware being delivered via cloud applications.[86]

2.3 Conclusion

It is apparent that cyber threats on e-health are evolving at a much faster rate than cyber defenses, many of which attacks involve highly sophisticated technical and social engineering tactics aimed at gaining access to sensitive information, and stealing intellectual property from healthcare organizations. As e-health becomes more widely used, cyber security risks will develop and multiply, becoming much more harmful than they are now amidst a systematic return to post covid-19 normalcy. Unfortunately, there is limited access to data provided by the National KE-CIRT/CC on health sector specific cyber threats due to the sensitivity and confidentiality surrounding health records including the names of endangered hospitals which could place patients, the public, or vulnerable groups at risk.

---

[85] See <https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic> accessed 08 September, 2021.

[86] National KE-CIRT/CC Cyber Security Report (n 41).

To mitigate against these cyber threats, it is important that Kenya prioritizes cyber awareness and cyber education as part of the key strategies towards enhancing national cyber readiness.[87]The right to health framework tackling cyber threats in e-health must be placed at the heart of patient safety as part of a comprehensive approach.

[87] Serianu (n 50).

3.0 CHAPTER THREE

THE INTERNATIONAL FRAMEWORK FOR ADDRESSING CYBER THREATS IN E-HEALTH

3.1 Introduction

The previous chapter having analyzed the cyber threats experienced by providers and users of e-health systems in Kenya, this chapter offers a critical examination of the legal and policy framework addressing cyber threats in e-health under the international and regional framework. This is based on the conviction that cyber security is a critical component of sound e-health practice, and that law is a critical tool for e-health adoption. In evaluating legislation as a crucial component of e-health practice, the chapter will primarily focus on whether policymakers have attained an equilibrium between the personal interest in data privacy and the public interest in data collection, use, and preservation.

3.2 International Law Governing Cyber Security in E-Health

International treaties have created an important role for the United Nations system, including specialized organizations like the World Health Organization, whose role is to promote treaty enforcement at the national level through binding and non-binding legislation and international codes of practice. Consequently, international instruments ratified by Kenya recognize the fundamental right to health which embodies e-health, and which, by virtue of Article 2 of the CoK, forms part of Kenyan law, as discussed below:-

3.2.1 World Health Organisation Constitution, 1946[88]

The World Health Organization (WHO) is a United Nations specialized body in charge of global public health. WHO achieves its goals of reaching the highest possible level of health for all people through its Constitution and lobbying for universal care, documenting public health hazards, planning responses to healthcare crises, and promoting public health. It provides technical support to states, develops global health guidelines and standards, and administers the World Health Survey, which gathers data on health care issues. Human rights, particularly the equal distribution of medical information and new e-health solutions that balance protection and usability, are also a priority for the WHO.[89]

As a consequence of acknowledging health as a human right, nations are legally obligated to provide timely, satisfactory, and fair health care, as well as the underlying health factors like privacy and data protection. In 2005, the World Health Assembly witnessed the birth of e-health by passing a resolution that laid the groundwork and established a frame for e-health adoption, as well as paving the way for e-health to be institutionalized on a global scale.[90] Having considered the previous report on e-health, the assembly noted the potential advances ICT had on health-care delivery.[91] The Fifty-eighth World Health Assembly endorsed e-health as the cost-effective and secure use of ICT in support of health and health-related fields like surveillance, education, and research. The assembly encouraged nations to consider formulating and executing a long-term comprehensive strategy for e-health services in different areas of the health sector, such as administration, having institutional and legal framework as well as facilities that inspire public-

[88] The Constitution was adopted in 1946 and came into effect in 1948. Amendments adopted by Resolutions WHA26.37, WHA29.38, WHA39.6 and WHA51.23 entered into force in 1977, 1984, 1994 and 2005 respectively.
[89] Art. 2, WHO Constitution 1946.
[90]WHA 58.28.e-health in the Fifty-eighth World Health Assembly <http://apps.who.int/gb/ebwha/pdf files/WHA58-/English/>) 2005, p 108–110, accessed 04 December 2020.
[91]Healy, J. C, 'The WHO E-Health Resolution; (2007) 46(01), Methods of information in medicine, p 02-04.

private partnerships. The Assembly also requested that Member States evaluate e-health operations and share knowledge of cost-effective designs while upholding quality, safeness, and ethical principles in strict adherence to the values of information confidentiality.[92] Following the adoption of this resolution, WHO regional governing bodies adopted regional resolutions on e-health, with a Regional Committee for Africa adopting resolution AFR/RC60/R3[93] and AFR/RC/63/9[94].

The World Health Organization's Sixty-Sixth World Health Assembly adopted a new resolution in 2013 on e-health standardization and interoperability[95]which was founded on the understanding that the secure, effective, and timely electronic collection, storage, and transmission of health data would be in strict adherence to the highest standards. This was critical in order to increase trust in e-health solutions by providing secure online management of sensitive health data.[96] As a result, the resolution requested that Individual Countries investigate options for partnering with relevant parties, such as national governments and academia to develop a detailed plan for the implementation of health data standards. This includes, when needed, the development of laws and legislative procedures related to a national e-health plan in order to assure public and private sector.[97] In 2018, the proposal on Digital Health was unanimously adopted by the Seventy-First

[92]See WHA58.28.e-health in the Fifty-eighth World Health Assembly, <http://apps.who.int/gb/ebwha/pdf files/WHA58-/English/)> 2005, p 108–110, accessed 04 December 2020.

[93]See E-health solutions in the African Region: current context and perspectives. WHO Regional Committee for Africa Sixtieth session, Malabo, Equatorial Guinea, August 30 – September 3, 2010. Brazzaville: Regional Office for Africa; 2010, See <http://apps.who.int/iris/ handle/10665/19931>, accessed 07 July 2021.

[94]See Utilizing e-health solutions to improve national health systems in the African Region, WHO Regional Committee for Africa, Sixty-third session, Brazzaville, Republic of Congo, September 2– 6, 2013. Brazzaville: WHO Regional Office for Africa; 2013<http://www.afrowho.int/index.php?option=com.docman&task. Doc. download & gid=5728> accessed 07 July 2021.

[95] See <http://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_R24-en.pdf> accessed 07 July 2021.

[96] Najeeb Al-Shorbaji, 'The World Health Assembly resolutions on eHealth: eHealth in support of universal health coverage' (2013) 52(6), Methods of information in medicine, p 463-466.

[97] ibid.

World Health Assembly[98] whose overarching intent was to galvanize action from the highest levels of government on implementing digital health for strengthening national health systems and to help achieve major public health objectives. The Assembly urged nations to develop laws that are compliant with international commitments on issues of data access, sharing, consent, security, confidentiality, and interoperability; and to communicate these to WHO on a voluntary basis.[99]

The decision also requested the Director-General to focus on ensuring that WHO capitalizes on it's strong points by building digital health based on existing guidelines and successful examples from global, regional, and national initiatives, such as the identification and promotion of quality standards like evidence-based digital health.[100]

These resolutions established e-health as a legitimate field of work for WHO with implementation leading to the attainment of e-health practice as part of health system strengthening. The adoption of the ten guidelines on how countries should use digital health technologies to enhance patient care, for example, encouraged nations to evaluate their use of technology for health. It also tasked WHO with developing institutional guidelines in e-health, such as promoting evidence-based e-health interventions through the identification and dissemination of best practices.[101] In order to achieve this, e-health must be embedded into health targets to benefit people in an ethical, healthy, secure, efficient, equitable, and sustainable manner while adhering to the values of openness. The WHO equally released the Global strategy on digital health 2020–2025, with the aspiration of improving health for just about everyone by intensifying the acceptance of person-centric digital

[98]World Health Organization. WHO guideline: recommendations on digital interventions for health system strengthening. World Health Organization, (2019).p 80-84

[99]ibid.

[100]ibid.

[101] Item 12.4, Resolution on digital health. Seventy-first World Health Assembly, Geneva, May 26, 2018: WHO <A71/VR/7; http://apps.who.int/gb/ebwha/ pdf. files/WHA71/A71R7-en.pdf.> accessed 01 March 2021.

health solutions that are appropriate, available, cost effective, expandable, and reliable.[102] Unfortunately, WHO's work is geared more towards promotion of e-health systems and not cyber security which is an integral part of e-health adoption.

3.2.2 United Nations Systems

The United Nations System acknowledges health as a core human right necessary for the exercise of other human rights, the recognition of which can be pursued through a variety of complementary approaches such as the adoption of specific legal frameworks, the formulation of healthcare policy, or the execution of WHO-developed health programs such as the adoption of e-health practice.[103] The right to health also includes components such as openness, accessibility, scalability, interoperability, privacy, security, and confidentiality critical to a cyber-secure e-health practice which are legally enforceable as will be discussed below;

3.2.2.1 International Covenant on Economic, Social and Cultural Rights. ICESCR (1966)[104]

The ICESCR which Kenya ratified in 1972, established a legislative foundation for health as an inclusive right that includes timely, high-quality, and adequate health. The right to best possible bodily and mental health entails improving all elements of environmental and industrial hygiene, as well as creating conditions that ensure everyone has access to medical care in the case of illness.[105] The treaty underscores that the right to health must be construed as a right to a range of facilities, products, services, and situations in order to reach the optimum possible level of health quality. States Parties are obligated to provide prompt and decent healthcare while still tackling underlying medical determinants including access to secure technology. The Committee identifies

[102]Arriel Benis, Oscar Tamburis, Catherine Chronaki, and Anne Moen, 'One Digital Health: A unified framework for future health ecosystems' (2021)2, Journal of Medical Internet Research 23, e22189.

[103]Marcia Rioux, The right to health - Human rights approaches to health, staying alive: Critical perspectives on health, illness, and health care (2006), p 85-114.

[104] The ICESCR adopted by the UNGA in 1966 via Resolution 2200A (XXI) and entered into force in 1976.

[105] Art. 12, ICESCR.

key and linked components that States Parties must apply in order to fulfill their duties under article 12 in General Comment 14. These elements encompass ease of access, acceptability, and quality.[106] A sufficient supply of operational public health and healthcare facilities, goods, and services is required for availability. Health-care facilities, goods, and services should be available to everyone without regard for their ability to pay. Physical accessibility is also included in accessibility, as all health services must be physically accessible to all segments of the population. The responsibility of States parties to guarantee that all health facilities, goods, and services are ethical and culturally appropriate is referred to as acceptability. On the other hand, quality demands states to ensure that all services are scientifically and medically suitable, as well as of a high standard of quality.[107] Nations are expected to take adequate legal, institutional and awareness - raising actions to guarantee the availability, ease of access, acceptance, and reliability of e-health practice.

3.2.2.2 Convention on the Rights of the Child. 1989[108]

The CRC which Kenya ratified in 1990, is the only child-focused treaty that is significant as a normative declaration of children's health rights. The Convention requires nations to take sufficient steps to minimize infant and child mortality, as well as to provide the necessary health services.[109] Such initiatives include proposals like the introduction of mobile and primary health care clinics, availability and affordability of generic medicines, training of gynecologists and midwives in health facilities, the application of malnutrition protocols in health facilities, the adoption of an integrated childhood illness program, and implementation of a national

[106] General Comment No.2014, adopted on August 11, 2000 at the Twenty-second Session of the Committee on Economic, Social, and Cultural Rights (Contained in Document E/C.12/2000/4).
[107] ibid.
[108]The UNGA approved the CRC in 1989, and took effect in 1990.
[109] Art. 24, CRC.

immunization programmes, all which have tenets of e-health.[110] Nations therefore should encourage public-private alliances and initiatives that can boost accessibility and affordability of e-health to ensure that benefits reach all children who may need them. This necessitates that health professionals advise caregivers on how to safely obtain and manage these simple and easily accessible innovations.[111]

3.2.2.3 International Conference on Population and Development.1994[112]

The ICPD adopted a revolutionary strategy to advance human well-being by putting individual rights at the heart of the global development agenda, leading to a new concept of population policies that prioritized reproductive health.[113]In developing health as a pillar of population and growth, the ICPD stresses the importance of investing in women and girls, both as a goal in and of itself, and as a means of enhancing everyone's quality of life. It highlights the significance of sexual and reproductive health, including family planning, as a precondition for women's empowerment, along with having an impact on population dynamics and environmental protection. In general, it recognized the importance of sexual and reproductive health rights to growth and wellbeing, with universal access relying entirely on the bolstering of health systems. This necessitates broadening their scope and comprehensiveness. Given its confidential nature, secure e-health technologies need to be embraced to ensure the availability, accessibility, acceptability and quality comprehensive family planning services encompassing sexuality education, including

[110]Committee on the Rights of the Child; See also Art. 24 General comment No. 15 (2013) on the right of the child to the enjoyment of the highest attainable standard of health.

[111] ibid.

[112]The ICPD was held under the auspices of the UN and coordinated by a secretariat comprised of the Population Division of the then-UN Department for Economic and Social Information and Policy Analysis (now the Department of Economic and Social Affairs) and UNFPA.

[113] 'Reproductive health' was described in paragraph 7.2 of the Programme of Action as "…a state of complete physical, emotional, and social well-being in all matters relating to the reproductive system," which "implies that people are able to have a fulfilling and healthy sex life, and that they have the capacity to reproduce and the freedom to determine if, when, and how much they do so."

counselling for both married and unmarried. Countries should therefore implement technology such as social media to help make sure that teenagers do not lack access to sexual and reproductive health services that are available. Relatively brief contraceptives, such as condoms, hormonal procedures, and contraceptives, as well as provision of safe abortion and post-abortion care facilities, should be made easily and easily accessible to teenagers, regardless of whether abortion itself is legal.[114] In general, e-health techniques must provide unrestricted advertising space for health education, protect patients' privacy and security, and promote access to information while not producing communication programs and material that are harmful to general health or legitimizing health-related stigma.

3.2.2.4 UN Convention against Transnational Organized Crime. 2003[115]

The UNTOC is a forward-thinking step in the fight against transnational organized crime, such as cybercrime committed on e-health platforms. Criminal organizations have embraced today's globalized economy and the technological advancements that coincides it, resulting in the current state of security breaches in e-health like hacking, ransomware, and insider threats. Since the cyberspace in which e-health operates has no physical borders, perpetrators can change their locations in the digital world from one country to another in seconds regardless of their physical location. The UNTOC emphasizes the importance of fostering international collaboration in order to combat crimes by offering new resources to combat cyber-crime as a global threat. The Convention allows e-health platform providers and customers everywhere to achieve protection and integrity of themselves and their medical data. To that end, the UNTOC implements a number of measures against transnational organized crime, such as the creation of domestic criminal

[114]General comment No. 4 (2003) on adolescent health and development in the context of the Convention on the Rights of the Child, Official Records of the General Assembly, Fifty-ninth Session, Supplement No. 41 (A/59/41), Annex X, para 6.
[115]The Palermo Convention (UNTOC) was ratified by GAR 55/25 in 2000 and went into effect in 2003.

offenses, the implementation of extradition structures, mutual legal assistance and law enforcement collaboration, and the advancement of development and professional assistance to help authorities build or upgrade the necessary competence.[116] Unfortunately, efforts to combat transnational cyber criminals are very fragmented, and weapons in protecting the cyber environment remain obsolete due to the lack of the appropriate structure to react adequately to growing cybercrimes on e-health platforms.

3.2.2.5 The Budapest Convention on Cybercrime 2004[117]

The Budapest Convention on Cybercrime is the only legally binding international treaty aimed at directing countries to set up cybercrime prevention measures. It offers comprehensive national strategies against cybercrime by harmonizing national legislation, developing investigative methods, and growing international cooperation. It takes a legal approach that seeks to limit cyberattacks by enacting cyber-crime legislation that provides for criminal procedural and the prerogatives required for the investigation and prosecution of such offenses, or evidence in relation to which is in digital form.[118]

It describes many e-health-related offenses like unauthorized entry, illegal surveillance, data intrusion, machine interference, software misuse, hacking, and copyright offenses. It also sets procedural law issues such as speedy data retention, disclosure, machine data search and capture, and content data interception.[119] Although achieving a common legal structure that would facilitate the enforcement of borderless e-health cybercrimes might not be entirely feasible, transposing the Convention into domestic law is the first step towards combating cybercrimes associated with e-

[116] ibid, Arts. 5, 16-21 and 28.
[117] Convention was adopted on November 8, 2001, at its 109th Session, and went into effect on July 1, 2004.
[118] Section 1, Budapest Convention on Cybercrime.
[119] Sections 2 and 3, Budapest Convention on Cybercrime.

health practice. Unfortunately, in many countries, given the existing regulatory void and lack of ability, e-health remains a possible gray zone from which cyber criminals operate with impunity.

3.2.2.6 Special Rapporteur on the Right to Health[120]

This is an independent expert appointed to track abuses, promote transparency while advancing human rights through country missions, government correspondence, public statements, and council reports.[121] In advancing e-health, the Special Rapporteur reports on e-health laws, policies, good practices and obstacles; makes recommendations to states.[122] In the arena of international law, the Special Rapporteur remains perhaps the most critical aspect in assessing the effects of core human rights treaties on e-health. Generally speaking, there exists a strong international regulatory framework in support of e-health practice. However, there is widespread uncertainty as to whether the current global system adequately addresses the cyber threats associated with e-health practice.

3.3 Regional Laws Governing Cyber Security in E-Health.

Africa as a Continent has passed several instruments in a bid to address the cyber security challenges associated with e-health practice as discussed below;

3.3.1 African Charter on Human and Peoples' Rights 1981[123]

Ratified by Kenya in 1992, the ACHPR unequivocally provides that everyone has a right to the best possible physical and mental health. The ACHPR further obligates nations to progressively see to the delivery of quality medical services.[124] An important aspect of the ACHPR is the

[120]Special Rapporteur's mandate on physical and mental health was established in 2002 by Res.2002/31. The mandate was endorsed and extended by the HRC with Res.6/29 of 2007 and most recently renewed by Res. 42/16 of 2019.

[121] Paul Hunt and Sheldon Leader, 'Developing and applying the right to the highest attainable standard of health: the role of the UN Special Rapporteur in Global Health and human Rights 2002–2008, (2010) Routledge,p 68-71.

[122] ibid.

[123] ACHPR also known as the Banjul Charter, was adopted unanimously in 1981 and came into effect in 1986.

[124] Art. 16, ACPHR.

reporting system whose primary objectives is to establish a framework for constructive dialogue between States parties. This is important in addressing shortcomings in implementing health-related rights, including those associated with the adoption of e-health technologies across Africa.

3.3.2 African Charter on the Rights and Welfare of the Child 1990[125]

Kenya ratified the ACRWC in 2001 comprehensively outlining basic values for African children. While acknowledging the child's special and privileged role in society, the ACRWC guarantees access to the best possible physical and mental health. It also obliges states to reduce infant and child mortality rates, ensure children receive the necessary medical support, with an emphasis on primary health care.[126]In broadly interpreting the right to health, the ACRWC facilitates safe lives through the adoption of proven and readily available technologies. Countries are therefore expected to introduce secure e-health into policies and services, which is critical given that e-health community-based initiatives can significantly reduce health hazards if made broadly accessible.

3.3.3 African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention) 2014[127]

Kenya is yet to ratify this convention, which seeks to harmonize African laws governing e-commerce, information security, cyber security management, and cybercrime control. The Convention requires countries to implement legal, policy, and regulatory initiatives to ensure cyber security governance.[128] The Convention recognizes cybercrime as presenting a significant threat to the protection of computer networks, consequently highlighting the need to define broad guidelines for the strategic approach to repress it. It requires states to provide a strong legislative

[125]ACRWC was passed in 1990 and went into effect in 1999.
[126] Art. 14, ACRWC.
[127]Adopted by AU Heads of State and Government at the AU Assembly's 23rd Ordinary Session in 2014.
[128] Art. 20, Malabo Convention.

structure to protect confidentiality and security as core data processing principles, the defense of critical infrastructure, and the establishment of regulatory authorities.[129]

The Convention is critical in examining how its adoption can promote cyber stability of the health sector in the African region in analyzing the nature and scope of cyber security governance obligations. There are presently obstacles impacting the use of the Convention as a foundation for enhancing regional cyber predictability in Africa. Some of the main reason why the Convention has not been fully implemented as a framework for promoting regional cyber stability are the slow pace of Member State ratification and the absence of meaningful regional coordination. Given the transnational nature of cyber threats associated with e-health, this study argues for the creation of a regional monitoring mechanism within the AU framework to improve regional harmonization of cyber security governance mechanisms, as well as embracing the application of the Law as a framework for promoting regional cyber stability, particularly in e-health.

3.3.4 Africa Health Strategy 2016-2030[130]

This was motivated by the need to strengthen commitments recorded in global and continental instruments concerning the right to health. This it does by establishing a strategic forum for health sector reforms, including the implementation of e-health. In upholding health as a human right, the Strategy obligates African States to create better performing health sectors that will address challenges caused by the disease burdens.[131]

[129] Art. 21 and ch 3, Malabo Convention.

[130] AHS 2016–2030 was established in 2015 at the 1st African Union Specialized Technical Committee on Health, Population and Drug Control (STC-HPDC), which revised the first AHS 2007-2015 to incorporate health science and innovation. It is based on a number of continental and global health policy commitments and instruments, such as Agenda 2063, 'The Africa We Want' the 2030 Agenda for Sustainable Development, the Sexual and Reproductive Rights Continental Policy Framework and its revised Maputo Plan of Action 2016-2030, among others.

[131] Part 3, African Health Strategy, (2016 – 2030).

This will be achieved by exploiting existing opportunities including adoption of e-health technologies, an initiative that requires multi-sectorial collaboration.

3.4 Conclusion

In general, the International legal framework strives to ensure that the ethical values of autonomy, beneficence, and justice are put into action.[132] This is significant because it establishes a structure inside which any failure to carry out the duties emanating from those precepts can be addressed, thereby establishing the legal environment in which e-health can be practiced free from cyber threats. The International framework is also crucial in establishing reasonable expectations and limits on rights and responsibilities[133]which has enabled stakeholders to highlight possible indicators that need to be focused on, thereby ensuring equity in e-health practice.

The World Health Organisation framework for instance advocates for training in e-health skills in medical schools, having adequate skilled and well distributed workforce in the public health sector,[134] all which are expected to align the cyber security needs of the providers and users of e-health. Unfortunately, the expectations have remained a pipe dream in as far as protecting providers and users of e-health from cyber threats, which situation is replicated across East Africa as will be established in the next Chapter. The continued lack of a structured cyber security regime in e-health has led to an increase in cyber-attacks, which in turn minimizes consumer confidence while increasing operational and reputational costs for e-healthcare providers.

[132] Jennifer L Bayuk, et al. "Cyber security policy guidebook." John Wiley & Sons, 2012.
[133] ibid.
[134]Najeeb Al-Shorbaji, 'The World Health Assembly resolutions on eHealth: eHealth in support of universal health coverage' (2013) 52(6), Methods of information in medicine, p 463-466.

4.0 CHAPTER FOUR

E-HEALTH LEGISLATION IN SELECTED JURISDICTIONS AND HOW THEY ADRESS CYBER SECURITY THREATS

4.1 Introduction

The e-health ecosystem in three East African countries is assessed in this chapter by conducting a cross-jurisdictional analysis of laws and policies governing e-health and how they address cyber security threats. Generally, the chapter seeks to answer one key question; whether the current e-health regulation is adequate, and whether additional regulation on cyber security is in fact, necessary. This is useful in revealing the consequences of not having specific cyber security legal protections in place for e-health growth across East Africa.

The East African Community's (EAC) e-health agenda has gained a lot of traction over the last decade. For example, the 2nd EAC Regional e-health and Telemedicine Workshop, Ministerial Conference, and International Trade Exhibit (EASTECO 2018) in Kigali, Rwanda entrusted member states with aligning the integration of regional policies and laws on patient safety, data sharing, data security, and confidentiality.[135]The EAC also established the Digital Regional East African Community Health (Digital REACH) Initiative aiming to leverage the power of e-health in the region through implementation of weighted, organized, life changing, and creative strategies via a sharable framework.[136] The EAC continues to perform periodic e-health readiness assessments which include aspects of system interoperability, benefits of e-health investments thus far, as well as trends in cyber-attacks and ways to address them. This aids in the culturing of local

[135]Measure Evaluation, 'East African Community Digital Health and Interoperability Assessment' (2019) Chapel Hill, NC, USA, University of North Carolina, p 138-149.

[136] See East African Health Research Commission, Digital REACH Initiative Roadmap (2017) < https://www.k4health.org/sites/default/files/digital-reach-initiative-roadmap.pdf.> accessed 11 May 2021.

e-health options and allows for the submission of status reports to relevant sub-regional councils every two years.

4.2 E-Health Laws in Rwanda and How They Address Cyber Security Threats

Rwanda was among the first nations in the region to embrace digital health, which is attributed to strong political will to improve healthcare through the use of digital technology. Aside from being one of few developing countries in the world with universal health coverage (Mutuelle de Santé) [137]Rwanda established electronic health records for HIV patients in 2005, a program that was later expanded to include all clinical records.[138] Building on technology to advance long-term health goals, Rwanda, in collaboration with Babylon Health, a UK-headquartered remote consultations provider established the world's first digital universal primary health care services, allowing patients to access consultations via mobile phones.[139] This significantly shortened appointment delays by allowing the patient to use text messages to electronically schedule laboratory tests and collect reviews online. Zipline, headquartered in Silicon Valley, also established a collaboration with the government to use drones to distribute blood, vaccines, frozen plasma, and other critical medical items to hospitals in remote areas.[140]This reduced the time taken to deliver emergency products from days or hours, to minutes. More recently, the Covid-19 pandemic has seen Rwanda use its own digital health capabilities in response to the Corona Virus, with the country's emergency response applying several digital health technologies to aid in pandemic management. This involved real-time digital mapping of disease transmission and telemedicine to reduce the

[137] This is a community-based medical insurance scheme that has been in place since 1999 as part of Rwanda's national health policy to provide universal health care.

[138] Cheryl Amoroso, 'Using Electronic Medical Records for HIV care in Rural Rwanda' (2010) Med Info, p 88-120.

[139]Owoyemi Ayomide, Adenekan Osiyemi, Joshua Owoyemi, and Andy Boyd, 'AIM for Healthcare in Africa' (2020) Artificial Intelligence in Medicine, p 1-10.

[140] Evan Ackerman, and Michael Koziol. "The blood is here: Zipline's medical delivery drones are changing the game in Rwanda." IEEE Spectrum 56, no. 5 (2019), p 24-31.

need for infected patients to physically attend doctors.[141] This has been made possible by laws that lay out the goals, strategies, and policies for e-health, including the following;

4.2.1 The Constitution of Rwanda. 2003

According to Article 21, everybody has the right to basic health. Article 45 on the other hand, requires the state to organize the citizens for activities to improve health and to assist them in carrying out such practices. These two provisions give the Constitutional basis for the right to health under which e-health practice falls.

4.2.2 National Health Information Exchange. 2010

Rwanda developed the Health Information Exchange (RHIE) project, whose main goal was to make client information more easily available to healthcare providers so as to enable them efficiently and effectively provide healthcare services. The foundational structure for RHIE sought to define, develop and implement a health enterprise architecture with the aim of supporting e-health programs, including identifying appropriate cyber security standards, functional requirements and interoperability profiles across multiple healthcare platforms.[142]

4.2.3 Smart Rwanda Master Plan (SRMP) 2016-2020

The Smart Africa Manifesto unveiled during the 2013 Transform Africa Summit served as inspiration for the SRMP. In aligning national vision and strategies, the plan recognized health as a pillar of development.[143]In terms of improving health services, the strategy prioritized research leveraging global technology trends to accelerate digital transformation.[144]Specifically, SRMP introduced project cyber security by design to ensure Rwanda's cyber space is safe and robust. As

[141]Clarisse Musanabaganwa, Muhamed Semakula, Jean Baptiste Mazarati, Jose Nyamusore, Aline Uwimana, et al. "Use of technologies in Covid-19 containment in Rwanda." Rwanda Public Health Bulletin 2, no. 2 (2020), p 7-12.
[142] Crichton, R., et al. “An interoperability architecture for the health information exchange in Rwanda” 2012.
[143] Solange Mukamurenzi, Åke Grönlund, and M. Sirajul Islam. "Challenges in implementing citizen-centric e-government services in Rwanda." Electronic Government, an International Journal 15, no. 3 (2019), p 283-302.
[144]ibid.

the global world became more linked, and new cyber-attacks became more widespread, all systems designed for government were to be designed with the highest security requirements, rather than applying security fixes to vulnerabilities discovered after the systems were in operation.[145]

4.2.4 National Digital Health Strategic Plan 2018-2023

This is the guiding document that presents a high-level plan to develop and implement e-health's long-term vision in Rwanda. The plan underlines previous visions like the Smart Rwanda Master Plan, with an overreaching goal of improving health service delivery and accessibility through e-health. The plan is based on the knowledge that, electronic information is often vulnerable to unauthorized use, if effective security measures are not implemented.[146] To ensure the success of e-health, processes must be in place to track and record access and notify authorities if there are any security breaches.

4.2.5 The Health Sector Strategic Plan IV 2018-2024

The strategy documents the framework of the health system and incorporates e-health into many program areas laying the groundwork for ICT implementation in the health sector. The policy identifies strategies and innovations which will assist the health sector in meeting its objectives, such as data security.

4.2.6 National ICT Hub Strategy 2024

The strategy is supplemented by other ICT initiatives and policies to advance e-health[147] in profoundly aligning the selection of ICT policies and services with the national vision and priorities such as healthcare. The ICT Hub identifies e-health as one of the flagship projects expected to run for the whole duration of the strategic plan. This includes encouraging cyber

[145]ibid.
[146]Christopher Seebregts, Anban Pillay, Ryan Crichton, and Deshendran Moodley, "14 Enterprise Architectures for Digital Health." Global Health Informatics: Principles of EHealth and MHealth to Improve Quality of Care 2017, p 173.
[147] Vision, Mission, & Strategic Goals, National ICT Hub Strategy 2024.

security adoption while maintaining commitment to recommendations and best practices shared with stakeholders on a regular basis. This is to be coordinated by the e-health department which spearheads planning and implementation of e-health initiatives, to ensure a highly effective, reliable, secure, and innovative e-health practice.[148]

Despite the presence of general laws, policies and regulations governing e-health, cyber security threats effecting both providers and users of e-health systems have remained largely unaddressed. This makes it necessary for Rwanda to establish a legal and policy framework to coordinate the implementation of an e-health cyber security regime as a matter of priority.

4.3 E-Health Legislation in Tanzania and How They Address Cyber Security Threats

Tanzania launched its first e-health policy in 2013 with the goal of enabling a healthy, inclusive, effective, and sustainable health system for all people.[149]The introduction of the first e-health strategy as anticipated, resulted in changes in disease monitoring, information management, as well as decision making at various levels. To that end, the United Republic of Tanzania established a governance framework comprised of a steering committee and a technical working group.[150]Recognizing the enormous potential of e-health to transform the delivery of quality healthcare, Tanzania implemented several applications to improve access, effectiveness, and quality of healthcare. Afya-Tek funded by the Swiss-based charity Foundation Botnar, is an example of e-health technology enhancing community decision making and quality of care.[151]To integrate the fragmented practice, Tanzania has adopted the following framework to regulate e-health practice;

[148]ibid.
[149] Mbiki Msumi, "An Overview of Tanzanian e-health Regulations" (2018) 42(6), DuD, p 373-375.
[150]ibid.
[151] Bakar Hamad, "Current Position and Challenges of E-health in Tanzania: A review of literature's 7.9.2019.

4.3.1 Tanzania Digital Health Strategy 2019-2024

Founded on the e-health strategy 2013-2018, this plan establishes a governance structure for the e-health system by giving a road map that will help Tanzania achieve universal health coverage. Through a digitally enabled health care system, the plan seeks to accelerate transformation through innovative, data-driven, client-centric and efficient digital health solutions.[152]The plan hopes to achieve secure data-driven initiatives where the correct information will be available to the users in a timely fashion. The strategy also adopts interoperability which promotes seamless and secure information exchange in a bid to ensure data security, privacy and confidentiality. The plan also establishes the National Digital Health Steering Committee, The National Digital Health Committee, Regional Health Management Team, Institutional Digital Health Committees and Health Facility Digital Health Committees which are mandated to oversee cyber security issues in e-health implementation.[153]

4.3.2 Tanzania Digital Health Investment Road Map (2017-2023)

This plan outlines 17 investment recommendations to enhance health system efficiency by improved data usage. The recommendations are intended to improve service quality, strengthen health system efficiency, maximize resource management, and connect and integrate data systems.[154] As Tanzania strives to achieve middle-income status and achieve health-related Sustainable Millennium Development Goals such as eliminating maternal, under-five, and tuberculosis mortality, increasing antenatal and births with a skilled birth attendant, family

[152] Measure Evaluation, "East African Community Digital Health and Interoperability Assessments" (2020) The United Republic of Tanzania, Chapel Hill, NC, USA: University of North Carolina.
[153]ibid.
[154]ibid.

planning, and antiretroviral-therapy coverage, the plan details the government's commitment to expand e-health platforms across Tanzania in a safe and equitable way.[155]

Despite the preceding framework, Tanzania unfortunately neither has an e-health cyber security framework nor stringent data security laws to safeguard patient information. As a result, patients' confidential data is used and stored without adequate legal protections.

4.4 E-Health Legislation in Uganda and How They Address Cyber Security Threats

Uganda, like the other jurisdictions under consideration has welcomed the use of e-health platforms to enhance primary healthcare delivery. The growth of e-health continues to generate opportunities for new technologies, the implementation of which has yielded good outcomes.[156]Uganda continues to invest in e-health which investment is enabling patients benefit from e-health.[157]The District Health Information System was adopted by Uganda as a National Standard method for gathering and reporting health data.[158] In 2011, Uganda launched mTRAC an e-health solution for tracking essential medicines, and improving health service delivery.[159] Health workers still use the tool to submit their weekly reports via SMS codes, while tracking stock levels of essential malaria drugs.

In an attempt to establish a clear legislative plan for e-health, Uganda has adopted several laws mostly aimed at delivering a safe, high-quality and affordable healthcare. This has also helped replace paper-intensive services with computerized systems, which has greatly done away with

[155] Geoff Watts, "The Tanzanian Digital Health Agenda" (2020) 2(2), the Lancet Digital Health, p 60-63.
[156] Vincent Kiberu, et al. "Development of an evidence-based e-health readiness assessment framework for Uganda." Health Information Management Journal, 2019 p 183.
[157] ibid
[158]Vincent Kiberu, "Barriers and opportunities to implementation of sustainable e-Health programmes in Uganda" (2017) 9(1) African journal of primary health care & family medicine, p 1-18.
[159] ibid

service fragmentation and duplication. Currently, the legislative and policy framework regulating cyber security in e-health consists of the following;

4.4.1 The Constitution of Uganda, 1995

Article 20 requires the Government to take all steps to make sure that basic medical services are available to the citizenry. Though not specifically related to e-health, it establishes the legal structure under which health can be practiced and governed.

4.4.2 Uganda National E-Health Policy, 2016

The plan carries the long-term plan for the health sector in Uganda by ensuring effective use of ICT to boost health outcomes by creating an enabling environment where sustainable e-health initiatives can thrive. It sets out areas of implementation including leadership and governance, e-health architecture, as well as the legal framework. The plan set out several principles that form the foundation for the document, like establishing a client focused e-health agenda, user-friendly technologies, multi-sectorial approach, human rights and quality information in e-health.[160]

4.4.3 Uganda National E-Health Strategy 2017-2021

It provides a foundation for the continued growth of e-health in Uganda by leveraging what is already in place to provide the value of a healthy, high-quality, inclusive, reliable, and sustainable health care system.[161]The plan provides a supportive framework for the creation, implementation, and use of long-term, ethically sound, and standardized e-health programs including e-health information security.[162] However, despite the presence of general health-related laws and policies,

[160]Wilson Okaka, and Irene Judith Nagasha, Promoting Effective National E-health Communication Campaigns to Attain the SDG 3 Progress in Uganda (Kyambogo University, Faculty of Education, Kampala 2018) p 7.
[161]Dinusha Vatsalan, et al. 'Mobile technologies for enhancing eHealth solutions in developing countries, Second International Conference on eHealth, Telemedicine, and Social Medicine' (2010), IEEE, p 45
[162]ibid.

cyber security in e-health has been largely ignored. Uganda needs to review its existing legal and policy framework to ensure cyber security threats on e-health are adequately addressed.

4.5 Conclusion

The EAC has a solid foundation of e-health laws and policies the majority of which lay out a road map for e-health practice. Unfortunately, little effort has been made to create a coherent collection of best practices and ethical standards which could be beneficial in the region's regulation of e-health cyber security. E-health in East Africa has largely grown without the benefit of any clear structures legislating its cyber security needs. The existing framework imposing general obligations to adhere to the requirements of privacy and confidentiality is not sufficient to protect e-health from the ever growing cyber threats.[163] As a result, policies that protect the privacy and security of health data while also addressing the needs of the stakeholders that use health data are urgently needed.[164]It is therefore advised that the region assesses the gaps in its legal and policy frameworks and begin to take necessary action to remedy them. Only after adequately addressing these obstacles and finding sustainable country-centered solutions for the effective roll-out of strong e-health projects will the much-needed scale be achieved to fulfill the demand for affordable, accessible and a cyber secure e-health practice.

[163] Darcy Niamh, et al, "eHealth strategy development: a case study in Tanzania" (2014) 2(2) JHI Africa, p 80
[164] World Health Organization, 'National eHealth strategy toolkit' (2012) International Telecommunication Union.

5.0 CHAPTER FIVE

National Laws Governing Cyber Security in E-Health

5.1 Introduction

This chapter provides an assessment of Kenya's e-health ecosystem by analyzing the regulatory framework governing e-health and how it addresses cyber security threats. The chapter seeks to establish whether the current e-health regulation is adequate, and whether additional regulation on cyber security is necessary. Technological advancement in Kenya has seen a surge in the adoption of e-health platforms allowing Kenyans to access better and faster health services. While a well-planned and controlled e-health ecosystem can improve healthcare delivery, it requires an effective strategy to match health priorities in a way that effectively implements e-health cyber security needs of both users and providers.

5.2 Laws Governing Cyber Security in E-Health

Parliament has passed several health, data and privacy laws that broadly speak to the cyber security environment in e-health practice including the following;

5.2.1 Constitution of Kenya, 2010[165]

The CoK is the supreme law granting a broad range of socio-economic rights. It contains a detailed Bill of Rights[166]that is binding on all organs and citizens, expressly requiring all state organs to uphold the rights enshrined.[167]The CoK specifically acknowledges the right to the best health possible.[168] It provides a framework for ensuring a rights-based approach to health-care delivery, including e-health. The CoK also mandates each state organ to take legislative, policy and other

[165] The CoK was promulgated on 27 August 2010 to replace the 1963 independence constitution.
[166] Chapter 4, CoK (n 1).
[167] ibid, Arts. 20 and 21.
[168] ibid, Art. 43 (1).

steps, including setting standards to achieve progressive realization of the rights protected in Article 43. It equally creates a national government and 47 county governments, each with unique health functions.[169]While recognizing general international law rules as part of nation law, the CoK accepts ratified international treaties- including e-health and cyber security related treaties- as part of Kenya's laws.[170]

5.2.2 Health Act No. 21 of2017[171]

This is the primary piece of health-related legislation. According to the Act, e-health is the use of electronic communication and information technology in the health sector including telemedicine, which is the provision of health services and the sharing of medical knowledge through telecommunications, including consultative, diagnostic, and treatment. While regulating health innovations, the Act recognizes e-health as a type of health service. Within three years of the Act's implementation, the Cabinet Secretary must enact regulations for the management of health information banks, including interoperability, data interchange and security, collection and use of personal health information, management of disclosure of personal information, and privacy protection, among other things.[172]

The Act requires the MOH to establish and maintain a comprehensive integrated HIS system which shall include one for national government health functions and another for county health functions, as well their consolidation and harmonization. It requires the Cabinet Secretary to develop legislation for m-health, and procurement of health products and technologies. Prior to providing any prescribed health care, health institutions are required to obtain written consent from

[169] Schedule 4, CoK (n 1).
[170] ibid, Art. 2(5 and 6).
[171]Approved in 2010 and began in 2017 as an act consolidating the health system, to coordinate the interrelationship between the national and the county governments, health products and health technologies among others.
[172] Sections 103 and 104, Health Act (n 4).

the patient.[173]Medical information is deemed confidential and is not to be disclosed except in response to a court order, for clinical studies, or to avoid a danger to public health. Both county and national governments are responsible for ensuring that there are appropriate public health facilities to provide adequate services, while the MOH retains responsibility for the creation and regulation of e-health facilities.[174]

Regrettably, at the national and county levels, Kenya has taken no legislative steps to regulate the collection, use, storage, distribution, and disposal of data. The absence of a regulatory framework outlining protocols for cyber-security in e-health has resulted in the users and providers of e-health coming under frequent cyber threats that continue to threaten the safety of medical data, consequently threatening the enjoyment of the right to health.

5.2.3 Public Health Act, No. 38 of 1921[175]

The Public Health Act creates a Medical Department tasked with preventing and guarding against the introduction of infectious disease into Kenya, promoting public health, and the prevention, limitation, or suppression of infectious, communicable, or preventable disease within Kenya; advising and directing local authorities on public health matters.[176]In managing the COVID –19 pandemic for instance, the Public Health Act has been critical in adoption of e-health technologies that have been a critical aspect in curbing the spread of the disease.

5.2.4 Health Records and Information Managers Act, No. 15 of 2016[177]

[173] Health Act (n 4), Sections 8 and 105.

[174] ibid.

[175] Commenced on 6 September 1921, as a Parliamentary Act providing for the protection and maintenance of health.

[176] Sections 10, 17 and 44, Public Health Act.

[177] Assented to in May 2016 and commencing in June 2016 as an Act of Parliament to provide for education, registration, and licensing of health records and information managers; to govern their practice; to create, empower, and operate the Health Records and Information Managers Board; and to accomplish other related purposes.

The Act defines a manager as an officer tasked with managing health records and information for health services, including data analytics, research, and the use of e-health applications. It establishes the Health Records and Information Managers Board, which is responsible for establishing and improving standards for the health records and information managers' profession in all areas. The Act also contains rules governing professional misconduct, such as disclosing information acquired during a professional engagement to anyone other than a client without consent.[178]

5.2.5 Pharmacy and Poisons Act, No.17 of 1956[179]

Health products, health technology, medical devices, and medicinal substances are specified in the Pharmacy and Poisons Act. It establishes the Pharmacy and Poisons Board, required to create guidelines for regulating the manufacture, import, export, distribution, sale, and use of medical products, as well as to prescribe relevant standards for new medical products regulating health products and technologies, ensuring all medicinal products meet prescribed standards on quality, safety, efficacy, and conduct research on products and technology.[180]Additionally, it creates the National Quality Control Laboratory responsible for chemical, biological, biochemical, physiological, and pharmacological research, and pharmaceutical evaluations that adhere to e-health principles.[181]

5.2.6 Kenya Medical Supplies Authority Act, No. 20 of 2013[182]

According to the Kenya Medical Supplies Authority Act, medical supplies include pharmaceuticals, non-pharmaceuticals, vaccines and therapeutic antisera, medical equipment and

[178]Sections 3 and 35, Health Records and Information Managers Act.

[179] Assented on 11 May 1956 and commenced on 01 May 1957 as an Act of Parliament to strengthen the regulation of the pharmacy profession and the trade of drugs and poisons.

[180] Section 3, Pharmacy and Poisons Act.

[181] Sections 25, 31, 35 and 44.

[182]Assented on 14/1/2013 and took effect on 25/1/2013 to provide for the creation of the KEMSA.

devices, medical appliances, health technologies, laboratory supplies and reagents, dental materials, and hospital consumables.[183] The Act establishes the Kenya Medical Supplies Authority, which is tasked with prescribing essential health packages, collecting information, and reporting to the national and county governments on the state and cost-effectiveness of procurement, as well as assisting county governments in establishing and maintaining appropriate supply chain systems for drugs and medical supplies. In carrying out its functions, the Authority is required to implement measures to ensure maximum efficiencies, as well as to conduct analyses of medical supplies to ensure their effectiveness, use, storage, or disposal in order to ensure compliance with the standards set.[184]

5.2.7 Kenya Information and Communications Act, No. 2 of 1998[185]

Most terms associated with e-health practice such as device, computer system, data, e-government, electronic record, electronic signatures, information and communication technology, password, and acts of vandalism, are defined in the Kenya Information and Communications Act. Cyber security is defined in the Act as a collection of resources, policies, security concepts, security safeguards, guidelines, risk management techniques, actions, training, best practices, assurance, and innovations used to protect the cyber environment. The Act sets up the Communications Authority of Kenya, which is tasked with providing telecommunication services, protecting the rights of all users in terms of costs, efficiency, and variety of such services, and ensuring privacy.[186] The Commission promotes public trust in the integrity and reliability of digital records, promotes the use of digital signatures to lend integrity and authenticity to electronic communications, and creates sound frameworks to reduce the risks of forged electronic records and fraud in electronic

[183] Section 2, Kenya Medical Supplies Authority Act.
[184] ibid, Sections 6 and 19.
[185] Section 23, Kenya Information and Communications Act.
[186] ibid.

transactions, among other things. The Act prohibits unauthorized entry to, and interception of, computer service with the intent of obtaining any computer service, as well as the damaging, degradation, failure, interruption, or obstruction of the functioning of a computer system, or a denial of access to, or impairment of any program or data stored in, the computer system, including the unauthorized interception of computer service.[187]

5.2.8 Access to Information Act. No. 31 of2016[188]

Article 35 of the CoK governs the right to information through the Access to Information Act. It defines personal information with records of health and medical history considered such. However, this right is not absolute. Violation of privacy and the potential to threaten the health or life of another may limit the right. The Act establishes criminal responsibility for knowingly disclosing information in contravention of the law.[189]

5.2.9 Data Protection Act, No 24. of 2019[190]

The Data Protection Act is used to control data processes while ensuring the full protection of data subjects' rights. It aims to define legislative and technological processes and tools to protect informational rights such as data secrecy, constitutional privacy rights, and the right to free access to and correction of personal information stored in public and private databases. It establishes quality standards for information technology goods and services through registration and certification, as well as the establishment of the Office of the Data Commissioner.[191]

Personal data breach is described as a security breach that results in the unintentional or unlawful destruction, loss, modification, unauthorized disclosure, or access to personal data transmitted,

[187] ibid, Section 83 C, W and Z.

[188]Assented on 31/8/2016 and began on 21/9/2016 as a Parliament Act to give effect to Article 35 of the CoK; to impose on the Administrative Justice Commission supervisory and compliance duties and powers for related purposes.

[189]Section 28, Access to Information Act.

[190]Assented to on 8/11/2019 and began on 25/11/2019 as an Act of Parliament

[191] Section 5, Data Protection Act.

stored, or otherwise processed. Personal health data can only be accessed by or under the supervision of a healthcare provider or an individual subject to the legal duty of professional confidentiality. Personal information may be transferred to another country only if the data controller has given evidence of safeguards to the Data Commissioner.[192]

5.2.10 Science, Technology and Innovation Act, No 28 of 2013[193]

The Science, Technology, and Innovation Act creates the National Commission for Science, Technology, and Innovation, which is tasked with establishing priorities for scientific, technological, and innovation activities in relation to government policies and the country's international obligations, including safe e-health practices.[194]

5.2.11 Computer Misuse and Cybercrimes Act, No. 5 Of 2018[195]

The Computer Misuse and Cybercrimes Act aims to protect the confidentiality, integrity, and availability of computer systems, programs, and data; to prevent unauthorized use of computer systems; to improve cybercrime prevention, detection, investigation, prosecution, and punishment; to protect the rights to privacy, freedom of expression, and access to information guaranteed by the CoK; and to facilitate international cooperation.

The Act creates the National Computer and Cybercrime Co-ordination Committee, which is in charge of receiving and acting on computer and cybercrime reports, coordinating the collection and analysis of cyber threats, and responding to cyber incidents that threaten Kenyan cyberspace whether such threats or incidents arise in outside Kenya; and create codes of cyber-security

[192] Sections 44 and 48, Data Protection Act.

[193] Assented in 2013 and commenced in 2014 as a Parliamentary Act to promote the promotion, coordination, and regulation of the country's advancement in science, technology.

[194] Sections 6 and 29, Science, Technology and Innovation Act.

[195] Assented and commenced in 2018 as an Act of Parliament providing for computer-related offenses; encourage the prompt and successful identification, prohibition, prevention, response, investigation, and prosecution of computer and cybercrime; to facilitate international cooperation in dealing with computer and cybercrime.

practice and performance requirements for implementation by owners of sensitive national information infrastructure; and build a curriculum for training on computer and cybercrime prevention, identification, and mitigation.[196]It also describes other risk-based protection considerations that are relevant and essential to protect public health and safety, while proposing methods of protecting critical infrastructure against cyber threats to owners of critical infrastructure. The Act governs information-sharing arrangements to ensure cyber security, the detection and prosecution of cyber-related crimes, and the protection of an individual's life or property.[197]The Act also defines crimes such as unauthorized entry, intrusion, interception, and unauthorized disclosure of a password or access code, computer fraud, phishing, and fraudulent use of electronic data.[198]

5.3 Policy and Regulations Governing Cyber Security in E-Health

In adopting the national e-government strategy and Vision 2030, the National ICT policy identified e-health as a national priority, and a solution towards achieving Universal Health Coverage. On that backdrop, the Government has enacted several policies and regulations governing cyber security in e-health practice, which despite existing in the legal framework, are seldom well understood nor enforced.

5.3.1 Kenya National E-Health Policy 2016-2030

The Policy developed by MOH fulfills the mandate to provide the best possible healthcare, as documented in the CoK and Vision 2030 development blueprint, by implementing a user-friendly e-health platform. The primary goal of the policy is to plan, design, and implement ICT infrastructure and software for the management and delivery of essential healthcare. The Policy is

[196] Section 3, Computer Misuse and Cybercrimes Act.
[197] ibid, Sections 6 and 12.
[198] ibid, Part III, IV and V.

significant for the National and County Governments because it aims to guide them in planning and budgeting for healthcare services at all levels of care.

5.3.2 Kenya National E-Health Strategy 2019-2023

The e-health Strategy is based on the realization of Vision 2030, whose overarching goal is to provide equitable, affordable, and high-quality healthcare. The strategy develops efficient, accessible, equitable, secure, and consumer-friendly healthcare services enabled by ICT in order to improve clinical practice quality, safety, and efficiency by increasing access to consumer health information, clinical evidence, and clinical decision support tools, while also enabling the health sector to operate more effectively as an interconnected system.

5.3.3 Kenya Health Policy 2014–2030

The Kenya Health Policy, 2014–2030, outlines strategies for significantly improving Kenya's health status in accordance with the CoK, Vision 2030, and global health commitments. It demonstrates the health sector's dedication to ensuring that the country achieves the highest possible levels of health while remaining sensitive to the needs of its citizens. The Policy specifies health building blocks, the most important of which are health products and technologies, as well as evidence-based quantifiable data collection and storage, which improves e-health system use.

5.3.4 Health Information System Policy 2010-2030

The HIS Policy is motivated by a need to create and maintain a simple, consistent, scientifically sound, easily understandable, and compatible information system for tracking the degree to which health sector objectives are being met, while taking into account national values such as universal coverage, equity, quality, and social justice, as well as the recognition of the right to privacy.

5.3.5 Kenya Health Information Systems Interoperability Framework

The Kenya HIS Interoperability Framework aims to help the Ministry of Health and county health departments improve health information systems across the spectral range of data collection, information generation, analysis, and utilization, which framework is intended to support effective decision-making among health information producers and consumers.

5.4 The Role of a Regulatory Framework in Addressing Cyber Security in E-Health

In Kenya, there are three systems for governing e-health: comprehensive laws, sector-specific laws, and informal rules. The specific right to health, as well as the relationships that give rise to a legal presumption that privacy will be respected, are outlined in e-health comprehensive laws, which are frequently based on human rights.[199] E-health sectoral laws are relevant in as far as they respond to specific obligations of health in a social interaction such as telemedicine and e-learning. Soft law, such as practice guidelines, social customs, professional organization codes of conduct, and other guidelines for good practice, are examples of informal rules.[200]The framework is important in managing public health by safeguarding Kenyans from diseases by restricting disease carriers' right to social interaction in circumstances such as the COVID-19 Pandemic through health and safety legislation such as travel restrictions to selected locations which ultimately improves access to the right to health.

5.5 Conclusion

According to the preceding analysis, e-health practice is derived from a general legal framework based on human rights principles, the CoK, health laws, and the general medical ethical framework on respect for privacy in the doctor-patient relationship. Is a cyber security regulatory framework at the heart of the e-health practice in Kenya? The answer appears to be yes. However, it is a

[199] Eric Muhati, 'Factors affecting cyber-security in Kenya–A Case of Small Medium Enterprises'(2018) Diss. Strathmore University.20-22

[200] ibid.

qualified yes. Until now, the use of legislation and policy has been limited to basic regulation. There is no appropriate framework to secure health data, both on transit and at rest. Cyber threats being experienced by providers and users of e-health have also not been adequately addressed through the framework. This indicates that a framework is being developed retroactively to the adoption of e-health as a result of which, their potential to serve as a catalyst and enabler for e-health adoption is being underutilized.

Generally, the cyber security regulatory framework is not yet prepared for the full and effective implementation of e-health solutions. Currently, the legal and policy framework's heart is beating slowly and failing to deliver the force of law to the far reaches of e-health, preventing health care systems from fully taking the advantage of a shareable, easily accessible, and secure system. As will be established in the next Chapter, in order for the Government to establish effective legal and policy framework to facilitate change, cyber security legislation should be made an integral part of patient safety.

6.0 CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

This chapter presents a summary, conclusion, and set of recommendations based on the findings presented in the previous chapters.

6.1 Summary

This study shows that while Kenya made a bold move in adopting e-health, it was necessary to determine what cyber threats if any, are being experienced by the users and provides of e-health. Importantly, the study sought to interrogate the existing regulatory framework in selected EAC countries and how it addresses cyber threats in comparison to Kenya's, as well as propose necessary interventions to eliminate cyber threats faced by providers and users of e-health. The Covid-19 pandemic forced many healthcare facilities to transform their business models into adopting technology. As a result, cyber-attacks multiplied as criminals enhanced their foray into vulnerable and exposed networks. For example, during the period January to March 2021, the National KE-CIRT/CC registered 28,247,819 cyber threat incidents, with cyber threat actors metamorphosing the form of attacks to bypass existing threat detection systems.[201]

Generally, the study establishes that, cyber threats on e-health systems are evolving at a much faster rate than cyber defenses. The cyber threats also involve highly sophisticated technical and social engineering tactics aimed at gaining access to sensitive information, and stealing intellectual property from healthcare providers and users. On paper, the national cyber security framework is well thought out and perfectly documented. In practice, however, much more needs to be done to guarantee the safety of e-health service users and providers.

6.2 Conclusion

[201] National KE-CIRT/CC Cyber Security Report for the Period January to March 2021.

Kenya has a vibrant e-health cyber threat landscape marked by highly skilled and organized cyber-crime networks seeking to exploit vulnerabilities for illegitimate purposes. From the findings of the study, the cyber threat landscape is broadening by day, with threats growing in scale and sophistication, which requires prioritizing cyber security in both funding and implementation.

In an effort to secure the health sector against the growing attacks, CAK has improved processes and system capabilities with the goal of increasing cyber threat detection, prevention, and response capacity aimed at ensuring the optimization and sustainability of Kenya's previous cyber security successes. Unfortunately, overlapping laws governing the health sector have failed to bridge the cyber security gap, consequently failing in their role as a catalyst and facilitator in driving the e-health agenda.

6.3 Recommendations

Based on the study's findings, recommendations are based on risk management methods and best practices which can be used to safeguard e-health. Though not exhaustive, these recommendations serve as a baseline for improving computer security. In view of cyber threats in e-health, taking into account the lessons and milestones gleaned from a comparative analysis of selected case studies' approaches to e-health legislation, the study makes the following recommendations.

6.3.1 Short Term Recommendations

6.3.1.1 Create a Risk Management and Vulnerability Framework

Healthcare providers need to implement administrative and technical policies such as quick response teams and breach notification rules. This will ensure consistency in scanning for cyber threats, with breaches immediately being brought to the attention of security managers for prompt action. This also requires updating policies to remain compliant with industry standards including adopting a full spectrum of cyber security practices before, during and after an attack. With

prevention being the most powerful tool at deterring attacks, it is recommended that, all mobile devices be protected, with computers being stored securely. Health-care facilities should conduct due diligence on potential service providers and choose vendors based on compliance and risk assessment. They equally need to conduct internal risk assessments, vulnerability scanning, and penetration tests which together, will ensure data safety, both at rest and on transit.

6.3.1.2 Skilled Frontline Cyber Security Workforce

The human factor is a major aspect of cyber security. In building a cyber secure and resilient e-health practice, there is need to invest in a skilled frontline workforce. As a vital part of improving cyber security, this entails continuous capacity building. This also involves adoption of access control mechanisms to ensure employees only come in contact with the health information they need. A skilled frontline workforce is also necessary in conducting an inventory of the location of patient's data on an ongoing basis, developing policy for proper disposal procedures, and conduct regular trainings with staff to discuss the dangers in sharing passwords or leaving password information exposed. Organizations should also appoint chief information security officers who will oversee the implementation of health-care institutions' cyber-security programs and the enforcement of cyber-security policies.

6.3.1.3 Maintaining Good Computer Habits

Internet evolves fast. Installing anti-virus software alone is insufficient. Cyber security comes with maintaining good computer habits like creating a preventive cyber hygiene routine, regularly changing strong passwords, vulnerability and patch management which are essential in ensuring healthcare devices are protected to the greatest extent possible, including ensuring a firewall is installed on everything linked to the internet. This also necessitates the continuous advancement

of security technologies and privacy techniques that aid in the detection and prevention of threats such as spam, malware, and viruses from accessing e-health platforms.

6.3.1.4 Prioritize Cyber Security as a Company Imperative

While Kenya hopes the health sector will rise to the occasion and establish industry specific cyber security guidelines, it is recommended that in the meantime, cyber security be integrated into overall health management. This necessitates a departure from traditional risk-control strategies and toward a threat intelligence-driven cyber security program. There is need to raise industry standard to keep everyone safe including employing transaction monitoring tools, keeping software up to date, and locking down lost devices to ensures platforms are protected from the ever advancing cyber threats. This also entails fostering a security culture that includes continuous cyber security education and training, emphasizing that cyber security is a collective responsibility.

6.3.2 Long Term Recommendations

6.3.2.1 Capacity Building

It is recommended that the health sector focuses on cyber intelligence training and capacity building on management of health data. It is also necessary for the Government to partner with e-health providers in providing outreach and safety training and educational materials to ensure employees receive regular cyber security education to identify threats. E-health providers should introduce cyber security awareness programs to include insight on best security practices especially for senior managers and the board. Customers, clients, vendors, associates, outsourced service providers, and other third parties with access to the institution's IT infrastructure should all receive cyber security knowledge and information.

6.3.2.2 Research and Innovations

The Government needs to invest in research and innovations given how sophisticated cyber-attacks are becoming. This includes carrying out a risk assessment to present a survey of the risks and situational awareness on e-health platforms. There is also need to introduce a vulnerability reward programme including payment of independent researchers to identify system flaws and rewarding all the cutting-edge contributors who keep e-health platforms secure. As established cloud providers including Microsoft and Google devote considerable resources towards security, there is need to invest in reliable cloud infrastructure that is cost effective and secure. This will involve adoption of encryption, machine learning as well as artificial intelligence to evaluate spam trends and block questionable or harmful email, phishing, or malware from reaching e-health platforms.

6.3.2.3 Improved Infrastructure and Resources

The Government needs to increase funding of the health sector and improve health infrastructure to cushion the operational costs that come with securing e-health platforms. Adequate funding requires sufficient budgets for technology operations and an investment in people's cyber security skills. Besides detecting and preventing threats, the security infrastructure adopted should build protection into everything. This includes encryption technologies and reliable cloud infrastructure. There is also a need for the segregation of voice and data traffic to and from e-health platforms so that the two can be properly monitored, irregular trends that suggest cyber-attacks be identified and remedial steps taken in a timely manner.

6.3.2.4 Establish a National E-Health Cyber Security Framework

With cyber-attacks evolving faster than cyber defenses, improving the legal and policy framework like adoption of comprehensive laws is necessary. This necessitates a clear regulatory structure that establishes obligations and priorities for the development of a comprehensive cyber secure e-

health practice. There is also need to adopt a comprehensive e-health strategy whose mission is to improve the country's cyber security posture. This will give providers and users more trust in online and mobile transactions, creating a safe cyber environment.

6.3.2.5 Audit of E-Health Systems

There is need to routinely audit the available e-health platforms to include transparency reports of the specific threats and the security initiatives employed. It is also important to share progress with users and encourage them to adopt stronger security standards so as to elevate security across the industry. This creates a need for audit guidelines specific to healthcare organizations, requiring all security incidents to be typically considered a breach, unless the affected agencies can show that there is a slim chance that the privacy of health information will be jeopardized.

6.3.2.6 Harmonizing the National Cyber Security Regimes

Kenya has a Ministry of Information Communication and Technology, a Communications Authority, a National Computer Security Incident Response Team - Coordination Centre (KE-CIRT/CC), a National Computer and Cybercrimes Coordination Committee, and a Cybercrime unit under the National Police Service's Directorate of Criminal Investigations. Unfortunately, all these units have an overlapping mandate, which complicates the incident reporting protocol due to conflict and duplication of efforts.

As the number and complexity of cyber threats targeting critical infrastructure increases, the potential disruption and impact of these threats will become an issue of national concern. Because cyber security is a shared responsibility among multiple stakeholders, a single institution should be in charge of implementing cyber security policies. Cyber security awareness and capacity building, early warning and technical advisories, and incident response should all be assigned to a single department. Additionally, it is essential to promote knowledge sharing and collaboration

amongst relevant stakeholders in order to create an atmosphere conducive to achieving a safe e-health practice. This includes having a liaison department in the MoH to receive reports of cyber threats on e-health infrastructure.

6.3.2.7 Promote International Cooperation and Legal Harmonization

As cyber security threats persist, international cooperation is essential in the collective creation of a more protected internet. It is therefore recommended that Kenya promotes international cooperation and collaboration with the aim of strengthening cyber security through openly sharing experiences and policy making with organizations and countries around the world. It also calls for collaboration with academia and the private sector to promote security while creating game-changing solutions to protect consumers of e-health platforms. The National KE-CIRT/CC leveraging on partnerships with various other National Computer Incident Report Teams (CIRTs), the global 24/7 G7 Cybercrime Network, and the International Telecommunication Union (ITU) needs to push for legal harmonization of the legal and policy framework addressing cyber security in e-health while adhering to the principle of double criminal liability.

6.3.2.8 Expand Cybercrime Offences to Cover E-Health Platforms

There is a need to enact a sector specific legislation to substantively address e-health-related offenses that threaten the security, integrity, availability, and sustainability of e-health. Measures that ensure the removal of safe havens, coordinate cooperation in the detection and prosecution of e-health related crimes and training law enforcement officers to combat crimes should also be included. This will help bolster evidence across jurisdictions while also allowing for the preservation and rapid access to electronic evidence pertaining to e-health investigations. As a result, such regimes will lead to the timely investigation and prosecution of crimes such as the illegal distribution of internationally controlled illicit substances through the internet.

6.3.2.9 Use of Digital Forensics to Support Healthcare Cyber Defense

Many incident response approaches in e-health focus on the containment of the incident for purposes of minimizing harm, launching a swift response and recovery; as opposed to preservation and/or collection of data for purposes of investigations and prosecution. As a result, vital evidence is often lost, which would otherwise have aided investigations and possible successful prosecution of the cyber criminals behind the attack. That makes it necessary to invest in digital forensics to support a healthcare organization's defense after a cyber-incident.

With the continued increase in the volume of digital evidence, it is recommended that the government does invest in up to date digital forensic tools to aid in the prosecution of e-health crimes. Digital examiners must be conscious of the volatility and fragility of evidence, and must therefore ensure that the access, collection, packaging, transfer, and storage of digital evidence follows protocols that keep digital evidence's credibility and admissibility in court. In addition, there is need to invest in capacity building of digital forensics examiners to match the rapid changes in the quantity and complexity of cyber-attacks against e-health platforms. There is also need to regularly retrain digital forensics examiners on emerging trends in cyber threat distribution and execution, in order to address these rising trends, as well as capacity building of the prosecutorial and judicial agencies to equip them with the necessary competencies to deal with the nature and extent of ever-evolving e-health cybercrimes.

6.3.2.10 Cyber-Insurance

Cyber insurance specifically designed to cover e-health related risks is evolving as a cornerstone of risk management programs. Though relatively expensive, it is recommended that healthcare organizations move to insure themselves against data security and privacy claims. This will help organizations handling legally protected information recover from their insurers on cyber claims.

6.4 Recommendation for Future Research

Beyond the analysis provided, this study further recommends more research on the human rights issues arising from cyber security management. The growing importance of cyber security requires that the government actively engages in monitoring and surveillance by state agencies. A study should therefore be carried out to identify the extent to which, improving cyber security encroaches on the privacy and freedom in the cyber space. Even as the National KE-CIRT/CC continues to spearhead the protection of the Kenyan cyber space against various emerging and persistent cyber threats through 24/7 monitoring, analysis and response, a similar study should be undertaken to investigate the appropriateness of, and progress of the recommendations made in this study once implemented.

BIBLIOBRAPHY

Books

1. Austin J, The province of Jurisprudence determined. J Murray, 1982
2. Bayuk J, et al, Cyber security policy guidebook. John Wiley & Sons. 2012.
3. Green L, Legal Positivism: The Stanford Encyclopedia of Philosophy.2003.
4. Marco G, Understanding Cybercrime: A Guide for Developing Countries. I.T Union. 2009
5. Padilha F, et al, An Overview of Data Privacy in Healthcare in the Current Age. Data Protection and Privacy in Healthcare.2021
6. Rioux M, The right to health - Human rights approaches to health, staying alive: Critical perspectives on health, illness, and health care. 2006
7. Uchenna J, Cyber security Law and Regulation. Wolf Legal Publishers 2012

Journal Articles.

1. Ackerman E, et al, The blood is here: Zipline's medical delivery drones are changing the game in Rwanda. IEEE Spectrum. 2019
2. Al-Shorbaji N, The World Health Assembly resolutions on eHealth: eHealth in support of universal health coverage. Methods of information in medicine. 2013.
3. Amoroso C, Using Electronic Medical Records for HIV care in Rural Rwanda. Med Info. 2010
4. Ayomide O, et al, AIM for Healthcare in Africa. Artificial Intelligence in Medicine. 2020
5. Bandara L, et al, Cyber security concerns in e-learning education. 2014
6. Banisar D, et al, Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. J. Marshall J. Computer & Info. L. 1999
7. Bartholomew K, et al, High-tech, high-touch: Why wait? Nursing management. 2004

8. Benis A, et al, One Digital Health: A unified framework for future health ecosystems. Journal of Medical Internet Research 23. 2021
9. Clem A, et al, Health implications of cyber-terrorism. Pre hospital and disaster medicine. 2003
10. Cohn S, Privacy and Confidentiality in the Nationwide Health Information Network. DC. 2006
11. Crichton R, et al, An interoperability architecture for the health information exchange in Rwanda. 2012
12. Dimitro D, Medical internet of things and big data in healthcare. Health Informatics Research, 2016
13. Ehrenfeld J, Wannacry, cyber security and health information technology: A time to act. Journal of medical systems.2017
14. Eman A, et al, E-health cloud: opportunities and challenges. Future internet 4. 2012
15. Filkins B, et al, Privacy and security in the era of digital health: what should translational researchers know and do about it?" AJo TR. 2016
16. Grimson J, et al, The SI challenge in health care. Communications of the ACM.2000
17. Hamad B, Current Position and Challenges of E-health in Tanzania: A review of literature. GSJ. 2019
18. Healy J, The WHO E-Health Resolution. Methods of information in medicine. 2007
19. Heffner M, et al, Health Fraud: A growing problem. ACM. 1986
20. Humayun M, et al, Internet of things and ransomware: evolution, mitigation and prevention. Egyptian Informatics Journal. 2020
21. Hunt P, et al, Developing and applying the right to the highest attainable standard of health: the role of the UN Special Rapporteur in Global Health and human Rights. Routledge. 2010
22. Kiberu V, Barriers and opportunities to implementation of sustainable e-Health programmes in Uganda. African journal of primary health care & family medicine. 2017
23. Kiberu V, et al, Development of an evidence-based e-health readiness assessment framework for Uganda. Health Information Management Journal. 2019

24. Kihuba E, et al, Assessing the ability of health information systems in hospitals to support evidence-informed decisions in Kenya. Global health action. 2014
25. Kruse C, et al, Cyber security in healthcare: A system review of modern threats and trends. THC 2017
26. Mackey T, et al, Pharmaceutical digital marketing and governance: illicit actors and challenges to global patient safety and public health. 2013
27. Mariani D, et al, Cyber security challenges and compliance issues within the US healthcare sector. International Journal of Business and Social Research. 2015
28. Mateu A, et al, Cyberbullying and post-traumatic stress symptoms in UK adolescents. Archives of disease in childhood. 2020
29. Msumi M, An Overview of Tanzanian e-health Regulations. DuD. 2018
30. Mukamurenzi S, et al, Challenges in implementing citizen-centric e-government services in Rwanda. Electronic Government, an International Journal 15. 2019
31. Musanabaganwa C, et al, Use of technologies in Covid-19 containment in Rwanda. Rwanda Public Health Bulletin 2. 2020
32. Nayha S, and Graeme T, Delivering proportionate governance in the era of e-health: making linkage and privacy work together. Medical law international. 2013
33. Niamh D, et al, eHealth strategy development: a case study in Tanzania. JHI Africa. 2014
34. Nijhawan L, et al, Informed consent: Issues and challenges. Journal of advanced pharmaceutical technology & research. 2003
35. Njoroge M, et al, Assessing the feasibility of eHealth and mHealth: a systematic review and analysis of initiatives implemented in Kenya. BMC Research.2017
36. Okikiola M, et al, A new framework for detecting insider attacks in cloud-based E-Health care system. International Conference in Mathematics, Computer Engineering and Computer Science IEEE.2020

37. Penny J, et al, The socio-economic impact of tele-health: a systematic review. Journal of telemedicine and telecare. 2003
38. Philbecket T, The Fourth Industrial Revolution, 2018 72(1) Journal of International Affairs.
39. Salem A, et al, The state of research on cyber-attacks against hospitals and available best practice recommendations. BMC medical informatics. 2019
40. Seebregts C, et al, 14 Enterprise Architectures for Digital Health. Global Health Informatics: Principles of EHealth and MHealth to Improve Quality of Care. 2017
41. Shenoy A, et al, Safeguarding confidentiality in electronic health records. CQ.HE 26. 2017
42. Sherali Z, et al. Security attacks and solutions in electronic health (e-health) systems. Journal of medical systems. 2016
43. Stuart A, et al, Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Criminal Justice P. 2005
44. Suman N, Cyber Trauma: An Overview, Indian Journal of Clinical Psychology. 2018
45. Uchenna J, The African Union Convention on Cyber security: A Regional Response towards Cyber Stability? Masaryk University Journal of Law and Technology.2018
46. Vatsalan D, et al, Mobile technologies for enhancing eHealth solutions in developing countries, Second International Conference on eHealth, Telemedicine, and Social Medicine. IEEE. 2010
47. Watts G, The Tanzanian Digital Health Agenda. The Lancet Digital Health.2020.
48. Williams A, et al, Cyber security vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices Auckland, NZ, 2015
49. Zavazava C, et al, The Role of ICT in Advancing Growth in Least Developed Countries: Trends, Challenges and Opportunities. 2011

50. Zeadally S, et al, Security attacks and solutions in electronic health (e-health) systems. Journal of medical systems. 2016

Graduate thesis

1. Chung K, Applying systems thinking to healthcare data cyber security. Massachusetts Institute of Technology. 2015
2. Hongach J, et al, Mitigating Security Flaws in the TCP/IP Protocol Suite. Diss. Utica College. 2018.
3. Muhati E, Factors affecting cyber-security in Kenya-A Case of Small Medium Enterprises. Diss. Strathmore University. 2018
4. Okaka W, et al, Promoting Effective National E-health Communication Campaigns to Attain the SDG 3 Progress in Uganda (Kyambogo University, Faculty of Education, Kampala.) 2018

Websites

1. http://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_R24-en.pdf>
2. http://www.afrowho.int/index.php?option=com_docman&task= doc. download&gid=5728>
3. https://news.safaricom.co.ke/doctor-on-call-telemedicine-takes-its-place-in-a-pandemic
4. https://news.safaricom.co.ke/doctor-on-call-The-rise-of-telemedicine/
5. https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic
6. https://www.justice.gov/usao-wdpa/pr/south-hills-pharmacist-pleads-health-care-fraud-conspiracy-fraudulently-obtaining
7. https://www.k4health.org/sites/default/files/digital-reach-initiative-roadmap.pdf.
8. https://www.kenyans.co.ke/kenyans-given-24-hour-access-doctors-through-phone-app
9. https://www.the-star.co.ke/news/2017-05-22-panic-as-wannacry-virus-hits-19-kenyan-firms/

WHO Policies and Reports

1. World Health Organization, Everybody's business – Strengthening health systems to improve health outcomes: WHO's framework for action. 2007
2. World Health Organization. National eHealth strategy toolkit. International Telecommunication Union. 2012
3. WHO Regional Committee for Africa, Utilizing e-health solutions to improve national health systems in the African Region, Sixty-third session, Brazzaville, Republic of Congo, September 2–6, 2013. Brazzaville: WHO Regional Office for Africa. 2013.
4. WHO Regional Committee for Africa Sixtieth session, E-health solutions in the African Region: current context and perspectives. Malabo, Equatorial Guinea, August 30 – September 3, 2010. Brazzaville: Regional Office for Africa; 2010.

Regional Cyber Security Reports

1) Measure Evaluation, East African Community Digital Health and Interoperability Assessment Chapel Hill, NC, USA, University of North Carolina. 2019
2) Serianu, Africa Cyber Security Report Kenya, Local Perspective on Data Protection and Privacy Laws. Insights from African SMEs. 2019/2020.
3) National KE-CIRT/CC, Cyber Security Reports. 2021
4) Qiong L, et al, Digital rights management for content distribution. Proceedings of the Australasian information security workshop conference on ACSW frontiers. 2003
5) Schjolberg S, ITU Global Cyber security Agenda, High-Level Experts Group, Report of the Chairman.2008

Online Sources

1. Bisson D, Hollywood hospital pays $17,000 to ransom ware attackers. The State of Security 2018
2. Steffen S, Hackers hold German hospital data hostage. DW. 2016.
3. Zorz Z, Crypto-ransomware hits German hospitals. Help Net Security 2016