Strathmore University

Law School

AN ANALYSIS OF THE LEGAL FRAMEWORKS SHAPING THE DIGITAL COLLECTION AND STORAGE OF GOVERNMENT HEALTHCARE DATA FOR UNIVERSAL HEALTHCARE.

Submitted in partial fulfilment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School.

BY

YEGO JANETTE JEBET

145721

Prepared under the supervision of

CLAUDE KAMAU

MARCH 2025

WORD COUNT: 13,901

DECLARATION.

I, YEGO JANETTE JEBET, do hereby declare that this research is my original work and that to the best of my knowledge it has not been previously in its entirety or in part, been submitted to any other university for a degree or diploma. Any other works cited or references to are acknowledged accordingly.

Signed…….

Date…… 24th April 2025

This dissertation has been submitted for examination with my approval as University Supervisor

Signed

Claude Kamau

Date: 23rd April 2025

ACKNOWLEDGEMENTS

I would like to thank God for giving me the resilience and strength to face and withstand all difficulties experienced in the writing of this paper. I would also like to thank Claude Kamau for his constant guidance and intellectual input and fruitful discussions throughout this process. Lastly I would like to thank my family for their continuous support throughout this writing journey.

LIST OF LEGAL INSTRUMENTS

Constitution of Kenya

Vision 2030

Kenyan Healthcare Policy 2014-2030

Sessional Paper No. 2 of 2017

Digital Health Bill

Public Health Act

Health Insurance Portability and Accountability Act

General Data Protection Regulations

General Data Protection Regulations

Federal Data Protection Act

Digital Act

Health Data Use Act

Patient Data Protection Act

Infection Protection Act

Act to Strengthen Health Promotion and Prevention

LIST OF CASES

Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others (2016) eKLR.

LIST OF ABBREVIATIONS

WHO- World Health Organisation

SDG- Sustainable Development Goals

UN- United Nations

UHC- Universal Health Coverage

NHS- National Health Service

EU- European Union

EHDS- European Health Data Space

ÖGD- Decentralised Public Health Service

GDPR- General Data Protection Regulation

BDSG- The Federal Data Protection Act

DigiG- The Digital Act

ePA- Electronic Patient Record

GDNG- The Health Data Use Act

PDSG- The Patient Data Protection Act

BMG- Federal Ministry of Health

IfSG- Infection Protection Act

DPA- Data Protection Act

ODPC- Office of the Data Protection Commissioner

AN ANALYSIS OF THE LEGAL FRAMEWORKS SHAPING THE DIGITAL COLLECTION AND STORAGE OF GOVERNMENT HEALTHCARE DATA FOR UNIVERSAL HEALTHCARE

ABSTRACT

With an emphasis on Kenya's Universal Healthcare Coverage (UHC) initiative, this study tackles big data challenges in the healthcare that could potentially affect millions of people. Examining ownership, privacy, consent from patients, existing legal framework, and cybersecurity, the study attempts to strengthen a safe base for the implementation of UHC. Based on institutional theory, it makes the assumption that examining current legislation will provide important information for the control of healthcare data. Effective service delivery, data protection, and adherence to global norms are advocated by this study, which has implications for healthcare institutions, citizens, and international commitments. The literature study emphasises how important it is to have strong legal frameworks, ethical standards and infrastructure while transitioning to digital healthcare administration.

Table of Contents

AN ANALYSIS OF THE LEGAL FRAMEWORKS SHAPING THE DIGITAL COLLECTION AND STORAGE OF GOVERNMENT HEALTHCARE DATA FOR UNIVERSAL HEALTHCARE....1

CHAPTER ONE....9

PART ONE: INTRODUCTION....9

Background....9

Statement of the Problem....6

Research Objectives....6

Hypotheses....7

Research Questions....7

Justification of the Study....7

Theoretical Framework....8

PART TWO: LITERATURE REVIEW....9

PART THREE: RESEARCH DESIGN....13

Research Methodology....13

Limitations....13

Chapter Breakdown....13

Timeline....14

CHAPTER TWO....15

Introduction....15

Regulatory Framework of Healthcare Data Protection in Kenya.....15

Constitution of Kenya, 2010....15

Data Protection Act, 2019....16

Digital Health Act, 2023....17

Health Act, 2017....18

Public Health Act, 1921....19

Regulations and Policies....19

The Guidance Note on the Processing of Health Data, 2023....19

Regulatory Structure of Digital Health in Kenya....21

Cabinet Secretary for Health....21

Digital Health Agency 22
Role of the Cabinet Secretary and Other Key Officials under the Digital Health Act 22
Is the Digital Health Framework missing the mark with data privacy? 23
CHAPTER THREE: 24
Introduction 24
The Definition of Public Health 24
Parameters of Public Health 25
Relevance of Data Privacy in Public Health 27
Cross reference with Kenya's Public Health and Data Privacy Regime 29
Conclusion 30
CHAPTER FOUR 31
Introduction 31
Justification for choosing Germany for this comparative analysis 31
The German Legal Framework in regards to Data Protection, Digital Health and Public Health 33
Data Protection Framework 33
Digital Health Care Framework 34
Public Health Framework 35
Germany's Legal and Regulatory Standpoint of Patient Consent 36
Comparative analysis of Public Health Exceptions for Bypassing Patient Consent in Kenya and Germany 37
Conclusion 41
CHAPTER FIVE 42
Introduction 42
Summary of Findings 42
Recommendations 43
Conclusion 45

CHAPTER ONE

PART ONE: INTRODUCTION

Background

In the midst of our digitally interconnected world where data reigns supreme, the shocking realisation of a massive healthcare data breach in the United States involving over 39 million individuals in early 2023[1] serves as an urgent wake up call. As developments in digital healthcare continues to happen around the world, the importance of legislation to prevent leaking of big data and mismanagement of patient data is in the rise.

The United Nations, aimed at the achievement of the Sustainable Development Goal target 3.8 by the year 2030, through the World Health Organisation focuses on providing technical assistance to member states with the aim of driving their infrastructure to a level of efficiency in order to deliver necessary healthcare services[2]. Such technical support by the WHO is also aimed at facilitating the transition of countries to Universal Healthcare Coverage.

The process of improving digital healthcare has been faced with various challenges in the world with data security in processing big data at the top of these challenges. Big Data refers to a combination of structured, semi-structures and unstructured data that organisations collect, analyse and mine for information and insights[3]. It is information assets with high volume, velocity and variety which requires specific technology and method for its transformation into value[4]. In healthcare, big data includes clinical data which is obtained from electronic medical records, biometric data provided from various types of devices used in monitoring weight, pressure and glucose levels[5], financial data constituting all records of economic operations

[1] <https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far> on 18 December 2023.
[2] <https://www.who.int/news-room/fact-sheets/detail/universal-health-coverage-(uhc)> on 22 February 2024.
[3] <https://www.techtarget.com/searchdatamanagement/definition/big-data> on 14 September 2024.
[4] Batko K, Slezak A, 'The Use of Big Data Analytics in Healthcare,' *PubMed Central,* Page
[5] Batko K *et al,* 'The Use of Big Data Analytics in Healthcare,' page 2.

reflecting the conducted activities, data from scientific research and data provided by patients including prescriptions of preference[6].

Within the past 14 years, between 2005 and 2019, there has been nearly 10 billion records across healthcare industries in various parts of the world that have been made public[7]. To put this into perspective, 43.38% of digital healthcare data collected is lost at some point between the initial collection and processing[8]. According to the Health Insurance Portability and Accountability Act Journal in the United States, between October 2009 and December 31 2023, the Office of Civil Rights has a total of 5,887 healthcare data breaches reported with an alarming 239% increase in hacking related breaches and 278% ransomware attacks[9]. It is not just the number of breaches increasing but also the severity of the breaches. Still within the United States, the number of records breached or accessed by unauthorised personnel has gradually increased from 45.9 million records in 2021 to 51.9 million records in 2022 and an astonishing 133 million records either stolen, exposed or impermissibly disclosed in 2023[10].

Though the largest reported breaches have occurred within the United States, the United Kingdom also faces its fair share of big data regulation challenges[11]. The Information Commissioner's Office released statistics showing that for the last two years to 31 March 2024, there have been 3,557 personal data breaches reported across the healthcare sector with the majority within the National Health Service[12]. In line with the increasing data breaches, the vulnerability of already collected health data is on the rise especially due to increased risks of issues such as state surveillance, increase in malicious targeting, data colonialism and data exploitation as well as involvement by the private sector[13].

In 2016, Denmark experienced a massive breach which lead to the changes on the processing of patient data leading to removal and changes in dosage for 267 patients[14]. The Danish Data Protection Authority held that the controller of the Shared Medical Record had breached Article 32(1) of the General Data Protection Regulation as his duty includes the identification of data

[6] Batko K *et al,* 'The Use of Big Data Analytics in Healthcare,' page 2.
[7] Hussein A, Zarour M, Alenezi A, Krishna A, Agrawal A, Kumar R, Ahmed R, 'HealthCare Data Breaches: Insights and Implications', 8 *Healthcare Journal* 2, 2020, page 2.
[8] Hussein A *et al,* 'Healthcare Data Breaches: Insights and Implications', page 2.
[9] <Healthcare Data Breach Statistics (hipaajournal.com)> on 13 September 2024
[10] <Healthcare Data Breach Statistics (hipaajournal.com)> on 13 September 2024.
[11] <Thousands of patients hit by NHS data breaches | The Independent> on 14 September 2024.
[12] <Thousands of patients hit by NHS data breaches | The Independent> on 14 September 2024.
[13] Davis S, 'The Trojan Horse: Digital Health, Human Rights, and Global Health Governance', 22 *Health and Human Rights Journal* 2, 2020, page 43.
[14] *Danish Health Data Authority,*

processing risks to the data subjects and to implement appropriate security measures to protect against those identified risks[15]. Similarly, in Singapore, an American working with a Singaporean doctor leaked the confidential information of 14,200 patients living with HIV[16].

In adherence to the SDGs, as part of their obligations as a member state of the UN, Kenya has made steps to reform its healthcare systems to incorporate digital infrastructure as a method of transitioning to UHC. The process of digital integration in healthcare is supported by various legislation in Kenya such as the Kenyan Constitution[17], Kenya's Vision 2030 plan[18] as well as the Kenya Health Policy of 2014 to 2030[19] and Sessional Paper No. 2 of 2017[20] read together with the Health Act of 2017. The realisation of UHC through digitalisation of the healthcare sector and the collection and keeping of medical data therefore requires the implementation of strong and effective systems to ensure the protection of the medical data to further ease the transition to Universal Healthcare Coverage[21].

In Kenya the Digital Health Act[22] is aimed at such effectiveness and protection as well as guiding the collection and use of medical data. As it strives to achieve patient privacy and to safeguard the data collected, the Act also provides for instances where a patient's consent to process their data would be bypassed[23]. According to the Act, a healthcare provider shall ensure that they obtain consent to process sensitive personal data unless where the health service being provided is for public health in accordance with the Public Health Act and in compliance with any other statutory requirements[24].

[15] Article 32(1), *General Data Protection Regulations (Denmark).*
[16] <Data of 14,200 people with HIV leaked online by US fraudster who was deported from Singapore | The Straits Times> on 13 September 2024.
[17] Article 43 (1) of the Constitution of Kenya provides for every person's right to the highest attainable standards of health, which include the right to healthcare services inclusive of reproductive healthcare; Article 43(2) states that no person shall be denied emergency healthcare treatment while Article 43(3) states that the State is obligated to provide social security to persons who are unable to support themselves and their dependents.
[18] Vision 2031 is aimed at improving overall livelihood of Kenyans with the efficient providence of integrated and highly affordable healthcare systems.
[19] The goal of the policy is to attain the highest possible standard of health through supporting equitable, affordable and high quality health services by the Ministry of Health and the health sector as a whole.
[20] The Sessional paper and the Act are aimed at advancing UHC through ensuring inclusive access, financial risk protection and fostering sustainability within the country.
[21] Wilson D, Sheikh A, Görgens M, Ward M, 'Technology and Universal Healthcare Coverage: Examining the Role of Digital Healthcare,' 11 *Journal of Global Health,* 2021, page 3.
[22] The Digital Health Act lays out the protection of medical data banks within Kenya.
[23] Section 31, *Digital Health Act*.
[24] Section 31, *Digital Health Act.*

Public Health is generally defined as the science of protecting and improving the health of people and their communities[25]. It is achieved by researching disease and injury prevention, and detecting, preventing and responding to infectious diseases[26]. The Public Health Act does not give a definition of public health neither does it list out clear defined parameter for the application of public health. The lack of a clear parameter in what constitutes public Health and consequently what can be a reason for violating a patient's data privacy creates risks most especially to the more vulnerable in the society such a persons living with HIV/AIDS to whom sharing or processing their data can lead to active discrimination.[27]

The importance of striking a balance between patient confidentiality and broadly the protection of individual privacy rights and public health is necessary as without strong laws and policies, there is a possibility of overreach and an eventual weakening of privacy rights within the healthcare data regime.[28] Considering the broad powers that public health authorities have to access the protected health information without the informed consent of the patient, possibilities of collection of vast amounts of data unnecessary to the intended purpose is a foreseeable occurrence.[29] Additionally, there is an increased concerns on the data security of health data considering more entities have access to protected health information.[30] The increasing number of public health authorities is due to the emergence of new health risks necessitating the creation of new and more well informed entities to handle such occurrences. With this increase of entities, there is a corresponding increase in the risks of unchecked processing of data, data breaches and unauthorised access to the privileged information.[31]

The risk of erosion of patient autonomy is another aspect that requires attention while balancing between public health necessity and respect for individual privacy rights. Public health can undermine the patient's autonomy by allowing their data to be shared and processed without

[25] <https://www.cdcfoundation.org/what-public-health> on 13 September 2024.
[26] <https://www.cdcfoundation.org/what-public-health> on 13 September 2024.
[27] Kenya Legal and Ethical Network on HIV&AIDS, *Enhancing Privacy and Confidentiality in the Management of Public Health Data,* 5.
[28] Kenya Legal and Ethical Network on HIV&AIDS, *Enhancing Privacy and Confidentiality in the Management of Public Health Data,* 4.
[29] <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html?form=MG0AV3> on 7 March 2025.
[30] <https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html?form=MG0AV3> on 7 March 2025.
[31] <https://compliancy-group.com/hipaa-public-health-exception/?form=MG0AV3&form=MG0AV3> on 7 March 2025.

their explicit and informed consent.[32] Another risk is the lack of transparency as patients may not be fully aware of how exactly their information is used or shared under the public health exception provided for by legislation.[33]

Strict public health measures were implemented in Kenya during the COVID-19 pandemic under the Public Health Act[34] which included the mandatory reporting of suspected COVID 19 cases by employers and household heads[35], the permitting of public health officials to enter and search premises for COVID-19 cases and report any cases of the disease that they find within the premises.[36] The intended purpose of the enacted Rules was to prevent the spread and contain the infection of COVID-19 within the country, this raises concerns of possible invasion of patients' privacy through the disclosure of their sensitive personal data.

The HIV and AIDS Prevention and Control Act provides for the protection of the confidentiality of individuals' HIV status.[37] There have however been reported cases of such privacy guaranteed by the Act and the overarching right to privacy guaranteed by the Constitution[38] was violated and subsequently challenged in Court. In the case of Kenya Legal and Ethical Network on HIV&AIDS together with 3 other petitioners challenged the President's executive order which required the collection on up to date data on school going children, expectant mother and breastfeeding mothers who were HIV positive.[39] The report was to include the names of the infected children, their guardians and the information of expectant HIV positive expectant mothers and breastfeeding mothers.[40] The respondent, who in this case were the Cabinet Secretary for Health, the National AIDS Control Council, the Attorney General, and 2 others, defended the directive stating that the intention was to improve healthcare service delivery for the vulnerable group as well as to further realise the right to health.[41] The Court ultimately found that the directive did directly violate the right to privacy

[32] <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html?form=MG0AV3> on 7 March 2025.
[33] <https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html?form=MG0AV3> on 7 March 2025.
[34] Public Health (Prevention, Control and Supression of COVID-19) Rules (No.67 of 2020).
[35] Section 2, *Public Health (Prevention, Control and Supression of COVID-19) Rules* (No.67 of 2020).
[36] Section 5, *Public Health (Prevention, Control and Supression of COVID-19) Rules* (No.67 of 2020).
[37] Section 3, *HIV and AIDS Prevention and Control Act* (No.4 of 2007).
[38] Article 31, *Constitution of Kenya* (2010).
[39] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* (2016) eKLR.
[40] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* (2016) eKLR.
[41] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health*

and that the exposure of the individuals' identities and HIV status constituted a violation of law.[42]

Without clear parameters for public health in place, there is a growing risk for the erosion of public trust, increased risk of data breaches and misuse, the blurring of lines of responsibility and accountability as well as hampered innovation and progress[43]. Focusing on the increased risk of data breaches and misuse, without well-defined parameters of public health for the purposes of data security, patient data can be used under the guise of public health becomes vulnerable to misuse by both malicious actors as well as the companies which can manage to get access to the data and control it[44]. Determining culpability in situations involving data breaches or misuse is made more difficult by the lack of precise guidelines. The boundaries of accountability are further blurred by public-private collaborations in digital health, making it more difficult to regulate and supervise organisations that handle private health data[45]. Delineating the roles and duties of stakeholders, as well as ensuring that data security, ethical usage, and breach repercussions are well specified, requires the establishment of clear guidelines.

Statement of the Problem

Section 31 of the Digital Health Act permits the bypassing of patient consent in processing personal healthcare data in providing public health services. However, the lack of proper parameters of public health in the Kenyan Legislation may lead to exploitation of patient data in the guise of public health reasons.

Research Objectives

1. To explore the applicable legislation in Kenya with relation to Digital Health Data processing as well as patient privacy and consent.
2. To analyse the relevant section of the Public Health Act in relation with the Digital

& 4 others (2016) eKLR.

[42] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* (2016) eKLR.

[43] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 22 (122) *BMC Medical Ethic,* 2021, 2.

[44] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 4.

[45] <https://edps.europa.eu/data-protection/our-work/subjects/accountability_en.> on 10th December 2024.

Health Bill and the ambiguity raised by section 31 of the Act.

3. To analyse how the German Digital Health Care framework addresses the matter of balancing between patient consent and privacy and upholding public health standards.

Hypotheses

The study hypothesises the following:

1. Section 31 of the Digital Health Act does not clarify the parameters of public health referred to in order to bypass patient consent therefore creating a legal gap that may lead to compromised data privacy and the eventual misuse of sensitive health data.
2. The lack of clarity in Section 31 of the Digital Health Act due to a lack of clear public health parameters and definition in the Public Health Act makes it difficult to interpret and apply exceptions to patient consent potentially allowing for broad and arbitrary justifications for bypassing patient consent.
3. Proper definition of public health and its applicable parameters as well as streamlining the prevailing patient data protection legislation will ensure a balance between protecting public health and protecting the privacy and confidentiality of healthcare data.

Research Questions

1. Does Section 31 of the Digital Health Act effectively protect patient data in situations where patient consent can be bypassed?
2. Does Section 31 of the Digital Health Act introduce an ambiguity as a result of the Public Health Act's lack of a clear definition of public health?
3. How has Germany's Digital Healthcare Framework successfully balanced patient consent, data privacy and public health and can this model be used within Kenya's Legislative framework?

Justification of the Study

This study will be focused on addressing the need for a comprehensive understanding of legislation governing digital healthcare data. From this evaluation and understanding, proper action can be taken to fill in the gaps within the policies and laws which will in turn benefit various groups of persons and institutions. Healthcare institutions such as hospitals, both private and public, will benefit through the enactment of proper rules of procedure and laws to

govern the keeping of digital medical records making service providence easy and effective. The citizens stand to benefit more as they will be the primary recipient of the effective healthcare services provided by hospitals and other medical institutions. Furthermore, through well drafted and implemented laws and policies, the citizens are guaranteed protection of their collected data as well as effective recourse in the event of a breach. The country stands to benefit from such developments and adjustments, through this benefit is realised in the International plane as it will continually by honouring its obligations to adhere to internationally agreed principles as it provides affordable and efficient healthcare to its citizens.

Theoretical Framework

The research topic of creating effective universal healthcare data governance forms the basis of this work. Important factors include the organisational structures controlling health information, the effectiveness of current legal systems, and the anticipated impact on UHC. Relevant constructs and variables are identified and categorised into independent factors, such legislative frameworks, and dependent variables, like the achievement of UHC, by a thorough examination of related literature.

The health system theory emphasises a systems perspective therefore viewing healthcare as a complex adaptive system rather than just a collection of individual components. The theory highlights complexity, noting that healthcare involves numerous interacting elements, where changes to one aspect can lead to unpredictable consequences. The interdependence of various healthcare components means that problems arise not only from the disregarding or respecting of individual rights but also from how these issues and elements interact. Therefore, to fully understand and improve the healthcare systems, a systems view that shifts focus to broader systemic contexts is required.

The chosen theoretical frameworks sheds light on the connections between data protection and healthcare legislative systems and frameworks and the realisation of UHC, and it is based in the health systems and institutional theories. Healthcare data governance is impacted by laws, customs, and cultural norms, as highlighted by institutional theory. This paradigm, which emphasises isomorphism and institutional pressures, is in line with the research aims and offers a useful lens for examining the relationship between legal frameworks and UHC accomplishment. The study intends to add crucial insights to the conversation on practical

approaches to healthcare data management in the goal of achieving universal health coverage by adopting this viewpoint.

PART TWO: LITERATURE REVIEW

Protecting patient data[46] is of the utmost importance, as highlighted by the European Court of Human and People's Rights, especially in this period of digital healthcare advancement. The relationship between cybersecurity, data privacy, and digital innovation in healthcare is examined in this review of the studies conducted. With an emphasis on the rising number of data breaches, the assessment particularly examines how the legislative frameworks governing data protection are currently structured. In addition, it examines the moral and legal requirements for data privacy while taking into account how digital innovation affects patient confidence and the integrity of the healthcare system. With technology advancing at a rapid pace, this review seeks to offer a succinct analysis of the benefits and problems associated with safeguarding healthcare data.

For the purposes of this review, several articles have been studied and considered but ultimately it will focus on three main articles. Several academic databases including, but not limited to PubMed, the were accessed in order to source the relevant information. The articles have been analysed in line with the research objectives and questions as well as incorporating an overview of their individual strengths and weaknesses.

Cybersecurity, Data Privacy, and Digital Innovation in Healthcare

In the realm of digital healthcare, several articles have been written and reviewed by different authors. One such article highlights the emerging digital technologies in healthcare and specifically puts a spotlight on cybersecurity[47]. This article touches on various aspects such as the emergence of digital technologies[48], the vulnerabilities related to those digital technologies, the cybersecurity threats in healthcare and the best practices in the health sector

[46] Protection of patient data can be traced back to the Hippocratic oath which is taken by healthcare professionals as they begin their practice. It is the obligation that privacy and confidentiality shall be upheld by the healthcare professionals. This in the face of digitalisation includes the prohibition on the unintended sharing of the healthcare data of patients.

[47] Arafa, A, Sheerah, H.A, Alsalamah, S. Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review.

[48] Arafa, A *et al, Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity.*

to curb the cybersecurity threats[49]. Focusing on the vulnerabilities related to the emerging digital health technologies, the author outlines cybersecurity, interoperability, regulatory compliance, ethical considerations, provider and patient education as well as infrastructure as the most pressing issues[50].

It is important to note that certain vulnerabilities are interlinked and solving or strengthening one requires another to be tacked. This is evident mainly in the realm of infrastructure. Emerging digital technologies in healthcare can only be adopted and successfully implemented with a strong infrastructure[51], which may not be present in all areas or medical facilities. An electronic health record system, necessary hardware and devices, a stable and fast network to guarantee continuous connectivity and data transfer, and sufficient technical support and upkeep are all crucial elements required for the implementation of digital technologies in medical facilities[52]. Together, these constituents establish the fundamental components required for the seamless assimilation of digital technology into healthcare environments, underscoring the pivotal function of infrastructure in bolstering the progress of digital healthcare[53]. Improving the digital healthcare infrastructure in order to match the demand for a digitalised health system is greatly important as it will ensure the steady and efficient processing of patient data while also protecting the privacy of the patients.

Infrastructure Challenges in Digital Healthcare

One of the biggest obstacles to the adoption of new digital technologies in healthcare is the lack of a strong infrastructure in some areas. For a smooth integration, essential elements such as reliable networks, required hardware, and electronic health record systems are essential[54]. Simultaneously, since digital technology is used more often, a large amount of patient data is generated. This means that strict cybersecurity measures, like data anonymization and encryption, are needed to prevent data breaches[55]. The implementation of comprehensive

[49] Arafa, A *et al, Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity.*
[50] Arafa, A *et al, Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity.*
[51] Shimonski R, *AI in Healthcare: How Artificial Intelligence is Changing IT Operations and Infrastructure Services,* John Wiley & Sons Incorporated,1 ed, Indiana, 2021, 6.
[52] Arafa, A *et al, Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity.*
[53] Arafa, A *et al, Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity.*
[54] Sedenberg E, Mulligan D, 'Public Health as a Model for Cybersecurity Information Sharing', 30 *Berkeley Technology Law Journal* 3, 2015, page 1691.
[55] J. Andrew, R. Jennifer Eunice and J. Karthikeyan, 'An Anonymization-based privacy- preserving data collection protocol for digital health data', *Frontiers in Public Health*, 2023,– Frontiers | An anonymization-based privacy-preserving data collection protocol for digital health data (frontiersin.org) on 22 August 2024.

rules by governments is crucial in safeguarding sensitive information and establishing legal ramifications for cyberattacks. In order to ensure that technology improvements are in line with ethical values and patient well-being, a cautious, transparent, and inclusive approach to the deployment of digital technologies in healthcare is necessary[56].

Cybersecurity Threats and Data Breaches in Healthcare

Something of importance that has not been handled in the first article is the impact of data breaches to both the clients and the organisations affected. Healthcare data breaches have serious repercussions for patients and organisations alike. Customers may be harmed if private information about them is made public, as this could result in identity theft, financial fraud, and other types of abuse[57]. Furthermore, falsifying medical records during security breaches may lower the standard of care by leading to inaccurate diagnosis and treatments. The consequences for organisations include severe financial losses, harm to their reputation, and a decline in customer confidence. Costs associated with healthcare data breaches are higher than those of general data breaches,[58] especially in industrialised nations.[59] The Health Insurance Portability Act[60] lays out certain data protection rules which institutions are mandated to adhere to.

Another aspect that has been extensively discussed is the possibility of data breaches due to unauthorised internal disclosures and the increased rate of such unauthorised disclosures within as the years go by. The study further shows that in the past four years, out of a total 843 unauthorised internal disclosures which have been flagged, 64.29% of these disclosures were reported within the last four years[61]. More alarming is that out of the 542 cases, sixteen percent were reported in the year 2019 alone which was a significant increase from the previous year of 2018[62].

---

[56] J. Andrew, R. Jennifer Eunice and J. Karthikeyan, 'An Anonymization-based privacy- preserving data collection protocol for digital health data', *Frontiers in Public Health*, 2023,– Frontiers | An anonymization-based privacy-preserving data collection protocol for digital health data (frontiersin.org) on 22 August 2024.
[57] Mählmann L, Reumann M, Evangelatos N, Brand A, 'Big Data for Public Health Policy-Making', 20 *Public Health Genomics Journal* 6, 2017, page 313.
[58] The cost of data breaches across other industries has been estimated at $4.45 million while the cost of healthcare data breaches has been estimated to cost the highest at about $10.93 million as of 2023.
[59] <https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/> on 6 March 2025.
[60] Health Insurance Portability and Accountability Act.
[61] Hussein A, Zarour M, Alenezi A, Krishna A, Agrawal A, Kumar R, Ahmed R, *Healthcare Data Breaches: Insights and Implications,* 8.
[62] Hussein A *et al, Healthcare Data Breaches: Insights and Implications,* 9.

From the papers analysed and discussed, certain things are of common concern and should therefore be considered by nations and institutions when moving from traditional healthcare management to digital healthcare. This is of specific importance to Kenya with the recent increase in ransomware-related cyberattacks which have increased by a shocking 755%.[63] As recent as 2021, nearly half of healthcare information technicians respondents have either claimed or reported phishing attacks[64] citing it as the cause of the biggest security flaws.[65]

Ethical Consideration in Digital Healthcare

The issue of ethical considerations[66] is one that has been tackled as well. When incorporating digital health technologies, ethical considerations are highlighted as particularly important. The importance of patient autonomy[67] is underscored by the requirement for control over medical records and treatment decisions. Usable technology that doesn't exacerbate already-existing healthcare disparities is necessary for reliability and justice. Such reliability and predictability of an already working healthcare system with a supplementary digital healthcare system are meant to improve patient autonomy[68].

Conclusion

Such considerations include the infrastructure available to support the systems as this is the core of the digitalisation move, the strength of the legal framework in place in order to regulate such systems as well as the ethical aspect of the data collection and storage. The need for a stable legal framework aimed at preventing data breaches should also be complemented with a suitable and working procedure guided by laws enacted by the parliament to effectively and proportionally hold those responsible for certain offences such as unauthorised release and disclosure of private patient data accountable. Such legislation should also be aimed at restitution of those who have been affected by healthcare data breaches as well as have

[63] <https://datarecovery.co.ke/rising-data-protection-challenges-to-healthcare-in-kenya/?form=MG0AV3> on 6 March 2025.
[64] Phishing is a common type of cyberattack which aims to trick the recipient to fall for the attackers desired actions which normally include revealing their financial information, login credentials and other desirable sensitive information.
[65] <https://datarecovery.co.ke/rising-data-protection-challenges-to-healthcare-in-kenya/?form=MG0AV3> on 6 March 2025.
[66] Cordeiro JV, *Digital Technologies and Data Science as Health Enablers: An Outline of Appealing Promises and Compelling Ethical, Legal, and Social Challenges.*
[67] Corderio, *Digital Technologies and Data Science as Health Enablers,*1.
[68] Ganesan D, 'Human Rights Implications of the Digital Revolution in Health Care in India', 24 *Health and Human Rights Journal* 1, 2022, 11.

procedures to recover lost data and emergency protocols in the event of a breach to ensure continuous provision of services in the midst of a data breach, whether minor or major.

PART THREE: RESEARCH DESIGN

Research Methodology

The research will be conducted through doctrinal research methodology. This study shall therefore rely on primary and secondary legal sources for data. The primary sources analysed will include the legal framework in digital healthcare and data protection in Kenya. The secondary sources will include existing literature, institutional and governmental reports, research and working papers as well as online resources relevant to the study.

Limitations

The study will be faced with certain limitations as it is carried out. One such limitation is the lack of Kenyan cases touching on the application of Section 31 of the Digital Health Act and the processing patient data without the patient's consent. Similarly, there has not been vast literature on the ambiguous nature of Section 31 of the Digital Health Act as it has been recently enacted.

Chapter Breakdown

Chapter one will serve as an introduction to the study. I will constitute the background, statement of the problem, research question, the study hypotheses focused on, justification of the study, the theoretical framework, literature review, and the methodology. The chapter will give context to the study that will build a foundation for the other chapters.

Chapter two will answer the first research question. It will explore the Kenyan Digital Health Act, in particular section 31 of the Act which lays out the instances in which patient consent can be bypassed for matters of public health. This will assist in interrogating whether the section is sufficient to protect patient data in the face of a public health.

Chapter three will answer the second research question. It will analyse the Public Health Act in conjunction with section 31 of the Digital Health Act to reveal the issues of definition ambiguity within the Public Health Act. This will give insight to whether the two legislations can sufficiently safeguard the data of citizens as a move to digital health under Universal Health Coverage in

anticipation by the Kenya Government

Chapter four will answer the third research question. It will do so by analysing the difference between the Kenyan and German Digital Healthcare Frameworks and explore the provisions allowing the bypassing of patient consent and its limitations.

Chapter five is the final chapter of this study. It will summarise the previous chapters of the study. It will also highlight the findings and conclusions of the first four chapters as well as offer recommendations and present a final conclusion to the study.

Timeline

SECTION	**ESTIMATED SUBMISSION**
Chapter One	August 2024
Chapter Two	September 2024
Chapter Three	September 2024
Chapter Four	November 2024
Chapter Five	December 2024
Final Dissertation Submission	December 2024
Defence of Dissertation	March 2025

CHAPTER TWO

Introduction

This chapter explores Kenya's legal system that oversees digital health. The first step is examining Kenya's Constitution, which lays forth the right to privacy as a fundamental tenet of digital healthcare. The domestic legal system and the regulatory framework that was put in place as a result of it are then examined in the chapter, which clarifies the legal issues in this field. This answers the first research question of the study.

Regulatory Framework of Healthcare Data Protection in Kenya.

Constitution of Kenya, 2010

The Constitution addresses healthcare and digital safety in various articles starting with the most important, Article 26, which provides for the right to life. This guarantees that all life must be protected by all means necessary[69]. From the right to life, the right to healthcare under Article 43(1)(a) arises. The Constitution provides that every person has the right to the highest attainable standard of health which includes the right to healthcare services, including reproductive healthcare[70]. This essentially means that no Kenyan will be denied basic healthcare in any private or public health institution. Article 31 of the Constitution steps in to guarantee the privacy of all citizens. The Article goes further to explain that each person has the right to not have their information relating to family or private affairs unnecessarily required or revealed[71]. This is important as healthcare data as it stands is regarded as personal and private affairs of the human person. Article 47 ties everything together by introducing fair administrative action which extends to decisions related to healthcare services ensuring that each citizen is treated equally and fairly in all situations including those involving the use of their personal healthcare data[72].

The Constitution is aimed at providing the basic rights owed to each citizen which includes the

[69] Article 26, *Constitution of Kenya* (2010).
[70] Article 43(1)(a), *Constitution of Kenya* (2010).
[71] Article 31, *Constitution of Kenya* (2010).
[72] Article 47, *Constitution of Kenya* (2010).

right to health and the right to privacy. On the side of right to health, it is recognised as a socio-economic right and therefore under Article 33[73], there is an obligation for progressive realisation of the right unlike other civil and political rights which are directly owed to the people. This gives leeway for the laid back implementation of health related rights and in this case digital health as well.

Data Protection Act, 2019

The Data Protection Act whose implementation commenced on the 25 of November 2019, is an Act of Parliament that breathes life into Article 31 of the Constitution, specifically Article 31(c) and 31(d). It gives guidelines on the regulation of the processing of personal data, provides the rights of data subjects as well as outlines the obligations of data controllers and processors.

Section 2 of the Act defines sensitive personal data as data that reveals the natural person's health status, genetic data, biometric data among other properties therefore legally classifying healthcare data as sensitive personal data[74]. The processing of such sensitive data is not permitted according to Section 44 unless all conditions under Section 25 are fulfilled[75]. Section 25 of the Act provides that for sensitive personal data to be processed, it has to be done in accordance with the right to privacy of the data subject[76]. Section 26 goes ahead to outline the rights of a data subject and explicitly states that the data subject has to be informed of the use to which the personal data is to be put as well as the right to object to the processing of all or part of their personal data[77]. This requires the data subject to not only be informed but to give informed consent to the processing of the data as well as to refuse the processing of their health data.

Consent is covered under Section 32 of the Act in which the data subject is granted the right to a written withdrawal of given consent at any time. In order to determine whether the consent was given freely, an account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of

[73] Article 33, *Constitution of Kenya* (2010).
[74] Section 2, *Data Protection Act* (Act No.159 of 2019)
[75] Section 44, *Data Protection Act* (Act No.159 of 2019)
[76] Section 25, *Data Protection Act* (Act No.159 of 2019)
[77] Section 26, *Data Protection Act* (Act No.159 of 2019)

personal data that is not necessary for the performance of that contract[78].This means that the consent will be deemed to be freely given if the provision of a service or performance of a contract is dependent upon agreeing to data processing that is not necessary for that service. Section 46 further provides that the conditions for the processing of health data is deemed to be met if the processing is necessary for the reasons of public interest in the area of public health[79]. Finally, Section 51 outlines the general exemptions on data processing with one of the exceptions being public interest[80].

Digital Health Act, 2023

The Digital Health Act is aimed at providing guidance in the provision of digital health services and the establishment of a comprehensive integrated digital health information system in line with Articles 31(1)(a), (d) and 43 of the Constitution of Kenya.

Section 19 of the Act breaks down the various classifications of health data with sensitive personal health data being among the classifications[81]. Section 27 outlines the use of sensitive personal data. The use of data to assess and address public health needs is listed as one of the uses of this classification of data[82]. Section 33 of the Act calls for a duty by data controllers to ensure the privacy, confidentiality and security of sensitive personal data which included the verification of user identities and restricting unauthorised access and use[83]. Consent to process sensitive personal data must be obtained unless in situations where a health service is provided for public health in accordance with the Public Health Act and in compliance with any other statutory requirements[84]. This is in accordance with Sections 31(1) and (2) of the Act. This creates a space for consent of the data subject to be bypassed for the general health of the public as deemed by statute.

The Digital Health Act is aimed at providing guidance at the proper processing of any and all digital data collected. However, the Act is inadequate in defining precise guidelines for processing sensitive personal data for public health objectives without obtaining data subjects'

[78] Section 32, *Data Protection Act* (Act No.159 of 2019)
[79] Section 46, *Data Protection Act* (Act No.159 of 2019)
[80] Section 51, *Data Protection Act* (Act No.159 of 2019)
[81] Section 19, *Digital Health Act* (Act No.15 of 2023)
[82] Section 27, *Digital Health Act* (Act No.15 of 2023)
[83] Section 33, *Digital Health Act* (Act No.15 of 2023)
[84] Section 31, *Digital Health Act* (Act No.15 of 2023)

agreement. The Public Health Act, which is relied on as an avenue to bypass patient consent, lacks precise definitions and criteria about what qualifies as a public health necessity[85], which leads to ambiguity even while the Acts provide the waiver of consent in circumstances judged necessary for public health. Without sufficient protections or accountability systems to guarantee that such exclusions are appropriate and justified, this loophole runs the risk of being abused or overreached, thus jeopardising people's privacy and autonomy[86].

Health Act, 2017

The Health Act commenced in 2017 and revised by the 24th Annual Supplement in December 2022 seeks to establish a unified health system, to coordinate the inter-relationship between national and county government health systems and more in context to provide regulation of healthcare service providers, health products and health technologies.

Section 103 of the Act recognises E-Health as a mode of health service[87]. E-Health is defined as the combined use of electronic communication and information technology in the health sector including telemedicine[88] according to Section 2. Section 104 mandates the Cabinet Secretary to ensure the enactment of legislation that provides for the collection, use, and management of personal health information as well as the protection of privacy among other necessities[89]. Section 105 further requires the Ministry of Health to facilitate the establishment and maintenance of a comprehensive integrated health information system[90]. These sets of sections are meant to provide guidance in navigating e-health and big data in the form of digital health information.

Despite being progressive, the Health Act's provisions for e-health and digital health information are neither explicit enough or urgent enough to handle the complexity of digital health systems. A crucial vacuum in the regulation of quickly developing technology is left by Section 104, which requires the Cabinet Secretary to pass laws on the gathering and safeguarding of personal health information but does not provide a timeframe or framework.

[85] Public health necessity generally refers to the essential and justifiable measures required to protect and improve the health and well-being of communities and the population as a while and is often involving interventions that may be considered as restrictive but necessary to promote health.
[86] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 22 (122) *BMC Medical Ethic,* 2021, 2.
[87] Section 103, *Health Act* (Act No.85 of 2017)
[88] Section 2, *Health Act* (Act No.85 of 2017)
[89] Section 104, *Health Act* (Act No.85 of 2017)
[90] Section 105, *Health Act* (Act No.85 of 2017)

Comparably, even though Section 105 mandates that the Ministry of Health create an integrated health information system, the Act makes no mention of specific guidelines or protections for handling big data, which raises questions regarding data security, interoperability, and patient privacy in the context of digital health.

Public Health Act, 1921

The Public Health Act amended in 2022 is an Act of parliament that was enacted with the purpose of securing and maintaining health.

In relation to disclosure of sensitive personal data, the Act is the reference legislation for the bypassing of the consent of the patient under the Digital Health Act. The Act mandated Health Authorities under section 13, to take all reasonable measures to prevent outbreaks of infectious diseases, safeguarding public health and execute duties to public health under the Act[91]. Section 10 further mandated Medical Departments under the Director-General for Health with various tasks including publishing public-health related reports and statistics[92]. These provisions ensure that public health is monitored and ultimately decisions to protect and preserve the general health of the public are made.

The Public Health Act's public health protection provisions are devoid of precise and unambiguous definitions of what public health is. Because public health choices may be subject to wide interpretation, this ambiguity poses serious dangers of abuse and overreach[93]. In addition to making responsibility and monitoring more difficult in situations when sensitive personal data is revealed or used without agreement, the Act may unintentionally jeopardise individual privacy and confidence[94] if its limitations are not clearly established.

Regulations and Policies

The Guidance Note on the Processing of Health Data, 2023

The Office of the Data Protection Commissioner released guidance notes on the processing of health data. The scope and purpose of the guidance note is to provide the healthcare institutions

[91] Section 13, *Public Health Act* (Act No.790 of 1921)
[92] Section 10, *Public Health Act* (Act No.790 of 1921)
[93] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 3.
[94] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 4.

with a proper understanding of their obligations under the data protection laws of Kenya[95]. The note is to apply to all healthcare facilities[96] including hospitals and clinics, laboratories, pharmaceutical service providers, health insurance providers, health researchers and training institutions, and professional health bodies[97]. The note further seeks to extend to the processing of digital health processing platforms that comply with the traditional in-person health services[98].

Under the guidance note, personal data in the healthcare sector is said to include sensitive health data such as medical histories, test results, and treatments. The note goes further to mention that the entities allowed to process such data include healthcare providers, insurers and researchers[99]. Certain principles are outlined by the note such as lawfulness, fairness and transparency of processing data[100], data minimization[101], purpose limitation[102], storage limitation and integrity and confidentiality[103]. These principles are set out in order to ensure that the information being collected is lawful and in line with the laws in place and to ensure that breaches and unauthorised storage and usage or data is avoided. Though the policy discusses in principles governing data processing, have not been provided for or adequately incorporated in discussing the processing of health data.[104]

In relation to Health Data specifically, the guidance note outlines certain special considerations such as the explicit requirement of informed consent for processing[105], compliance with data localisation mandates to ensure that the health data is stored within the country unless there are

[95] Guidance Note on Processing Health Data, Page 8
[96] Guidance Note on Processing Health Data, Page 8
[97] Professional Health Bodies are organisations that ensure healthcare professionals are qualified, licensed, and trained to a certain standard. Their roles are to regulate and hold professionals accountable, representing the grievances of the profession, maintaining the standards of the profession and developing expertise within the profession.
[98] These generally include systems such as Health Management Information Systems, eHealth and mHealth applications.
[99] Guidance Note on Processing Health Data, Page 31.
[100] Guidance Note on Processing Health Data, Page 11.
[101] The data minimization principle in the health sector refers to the idea that personal data should be limited to what is necessary for a specific purpose, and should not be collected, used, or retained beyond that purpose. This means collecting only the minimum amount of data required to achieve the health purpose for which it is being collected.
[102] The purpose limitation principle in the health sector means that personal data should only be collected and processed for specific and legal purposes and should not be used for any other purpose inconsistent with the identified legal purposes/basis.
[103] Guidance Note on Processing Health Data, Page 18.
[104] Guidance Note on Processing Health Data, Page 18.
[105] Guidance Note on Processing Health Data, Page 20.

certain conditions met, and requirements for heightened protection against misuse including ensuring accuracy, limiting access to authorised entities, and anonymising data where need be[106].

For Public Health related matters, the note outlines the goals for the usage of the collected medical data for disease monitoring, research and innovation as well as policy planning[107]. The Guidance Note also discusses the need for a balance especially between the ethical and legal side[108]. The note points out that the processing of health data for public health purposes must balance individual privacy rights and societal health benefits[109].

While the guidelines actively acknowledge the importance of personal health data to be processed for the benefit of public interest under public health or in the exercise of official authority, it lacks specificity which could lead to potential overreach.[110] The guidelines do not provide specific instances and circumstances where bypassing patient consent for public health purposes.

Regulatory Structure of Digital Health in Kenya

Cabinet Secretary for Health

The Cabinet Secretary for Health after appointment in accordance with the Constitution of Kenya is mandated by the Digital Health Act to perform various functions including but not limited to establishment of a health data governance framework[111], establish security measures in the system to protect sensitive personal data[112], establishment of national health data bank[113], develop regulations for the disposal of sensitive personal data[114], and develop guidelines and standards for the E-Health platform[115].

[106] Guidance Note on Processing Health Data, Page 17.
[107] Guidance Note on Processing Health Data, Page 13.
[108] Guidance Note on Processing Health Data, Page 23.
[109] Guidance Note on Processing Health Data, Page 23.
[110] <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html?form=MG0AV3> on 7 March 2025.
[111] Section 21, *Digital Health Act* (Act No.15 of 2023).
[112] Section 24, *Digital Health Act* (Act No.15 of 2023).
[113] Section 26, *Digital Health Act* (Act No.15 of 2023).
[114] Section 34, *Digital Health Act* (Act No.15 of 2023).
[115] Section 41, *Digital Health Act* (Act No.15 of 2023).

Digital Health Agency

The Agency is established under the Act[116] with the aim of developing standards for digital health system interoperability, monitoring the compliance with digital health regulations, promoting innovation and research within the digital health technologies, and providing accreditation to digital health service providers among other functions[117]. The Agency is also granted various powers under the Act in order for it to adequately perform its intended purpose[118].

Role of the Cabinet Secretary and Other Key Officials under the Digital Health Act

Under the Digital Health Act, the Cabinet Secretary for Health is responsible for overseeing, regulating, and implementing digital health systems. In accordance with national health policy and international best practices, the Cabinet Secretary is charged with developing regulations and policies for the use of digital health systems[119]. The Cabinet Secretary and the Agency in consultation, are mandated to establish a framework for administration and management of the system and shall ensure the maintenance of the integrity and security of the system[120]

The Digital Health Agency under the Act is responsible for establishing rules and regulations to control Kenya's digital health systems[121]. Its responsibilities include monitoring adherence to set standards, accrediting digital health service providers, and guaranteeing interoperability across digital health platforms. The authority is also responsible for enabling the integration of digital health services into county and national healthcare systems and encouraging innovation and research in digital health technologies.

The Agency's management and administration fall within the purview of the Board. The Public Procurement and Assets Disposal Act gives the Agency the authority to manage and control its assets in a way that advances its goals[122]. The National Assembly must give its prior assent before any immovable property can be charged or disposed of. To achieve its goals, the Agency

[116] Section 5, *Digital Health Act* (Act No.15 of 2023)
[117] Section 6, *Digital Health Act* (Act No.15 of 2023)
[118] Section 7, *Digital Health Act* (Act No.15 of 2023)
[119] Section 21, *Digital Health Act* (Act No.15 of 2023)
[120] Section 15, *Digital Health Act* (Act No.15 of 2023)
[121] Section 6, *Digital Health Act* (Act No. 15 of 2023)
[122] Section 7, *Digital Health Act* (Act No.15 of 2023)

may also collaborate with groups inside or outside of Kenya. As stipulated by the Act, it is also permitted to invest its money that is not urgently required[123].

Is the Digital Health Framework missing the mark with data privacy?

The Digital Healthcare framework is expansive and covers many different areas but an area of concern is that of data privacy and the protection of the data subject's sensitive personal data. The Data Protection Act emphasises that the data subject is granted the right to a written withdrawal of given consent at any time. This is restated in the Digital Health Act under Section 31. The Digital Health Act goes further to issue the instances where the consent of the data subject can be bypassed by authorised data processors. Under these instances, matter of Public Health are mentioned[124].

The Public Health Act though geared to protect and uphold the general health of the populations does not give any definition of public health and nor does the Health Act. This then creates a grey area in which the sensitive personal data of the data subject can be processed without their consent thus opening an avenue of abuse of the term "Public Health" by authorised data processors and all those with access to the health data of the citizens. To ensure that there is accountability[125] for the data being processed, clear parameters of public health must be set up by the relevant statutes and regulations. Besides having clear cut parameters of public health instances which could qualify for the bypass, there is need for the strengthening of the protection of patient privacy and the confidentiality of their healthcare data. This will promote public trust and decrease the risk of misuse of processed data[126].

[123] Section 7, *Digital Health Act* (Act No. 15 of 2023)
[124] Section 31, *Digital Health Act* (Act No 15. of 2023)
[125] Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 5.
[126]Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 2.

CHAPTER THREE

Introduction

This chapter will work to answer the second research question on whether Section 31 of the Digital Health Act introduces and ambiguity as a result of the Public Health Act's lack of a clear definition of public health. In answering this question, this chapter will look at the definition of public health, its parameters, the interrelation between data privacy and public health as well as the look into the current situation in Kenya.

The Definition of Public Health

Over the years, public health has been defined in various ways[127] and the definition has changed over the decades to reflect the growing advancement in scientific understanding, the changing patterns of disease and mortality such as epidemiological transitions and the impact on social and environmental factors, evolving societal values and public expectations and the ever growing impact of global events and public health emergencies[128]. The current agreed upon definition started taking shape from the 20th Century with C.E.A. Winslow offering a comprehensive definition of public health to encompass prevention, health promotion and lifespan extension with an emphasis on collective community action and particularly in sanitation, infection control and personal hygiene control[129]. In 1988, the Institute of Medicine provided a more concise definition that retains the focus on community efforts while incorporating the application of scientific knowledge in disease prevention and health promotion[130].

Different definitions have also been offered by different schools such as the Indian Academy of Public Health which defined it as Public health is the science and art of promoting health, preventing disease and prolonging life, to maintain a healthy and economically productive life so as to realize the birth right of each individual, by organizing a social machinery of community development to maintain a healthy environment, empower the people for

[127] Norick LF and Morrow CB, *Defining Public Health: Historical and Contemporary Development*, Jones and Bartlett Publishers,4
[128] Norick and Morrow, *Defining Public Health*, 5.
[129] Norick and Morrow, *Defining Public Health*, 5.
[130] Norick and Morrow, *Defining Public Health*, 5.

maintaining a healthy lifestyle and behaviour, prevent epidemics, control communicable and non-communicable diseases, addressing the social, economic and cultural determinants influencing health and disease, and also organizing a personal care and public health service for caring the sick and disabled specially during man made or natural calamities and epidemics[131]. This definition can be further broken down into three distinct parts with the first being the goal of public health which is to prevent diseases and to prolong life, to maintain a healthy and economically productive life so as to realise birth right of each individual through a combination of science and art knowledge and skill[132]. The second part introduces how the goal set in the first section will be achieved and this is by organising a machinery of community development[133]. The third and final part outlines the specific health intervention activities which are aimed at maintaining public health[134].

Throughout the development of the definition, the widely accepted definition is that public health refers to the science of protecting and improving the health of people and their communities[135]. By this, public health focuses on improving and protecting community health and well-being and mostly emphasising on the prevention of diseases among people[136]. In general, regardless of the definition used, the core aspects of public health is the organised efforts directed at the health of the broader community as opposed as the individual[137].

Parameters of Public Health

Having understood the basic principle of public health is to protect community health, it requires parameters so as to prevent it from being either too invasive or too ineffective to protect the general well-being of the community. Though these boundaries are not fixed but rather work as guiding principles[138].

---

[131] Norick and Morrow, *Defining Public Health*, 5.

[132] Norick and Morrow, *Defining Public Health*, 5.

[133] It is the responsibility of the state to look after the health of the nation and such principles which drive it should be enshrined in the constitution and relative legislation.

[134] These activities include maintaining a healthy environment, a healthy lifestyle and behaviour as well as preventing epidemics, controlling communicable and noncommunicable diseases, addressing the social, economic and cultural determinants influencing health and diseases and also organising personal care and public service for caring for the sick and disabled during manmade or natural disasters and epidemics.

[135] <https://www.waldenu.edu/programs/health/resource/what-is-public-health-and-why-is-it-important> on 20 Jamuary 2025.

[136] <https://www.waldenu.edu/programs/health/resource/what-is-public-health-and-why-is-it-important> on 20 Jamuary 2025.

[137] Defining Public Health: Historical and Contemporary development

[138] Norick and Morrow, *Defining Public Health*, 5.

The basis of public health lies on the orientation towards populations and communities rather than individuals. Since health is impacted by elements that function at a collective level, its goal is to enhance the health and well-being of entire groups[139]. Clinical medicine, on the other hand, concentrates on diagnosing and treating each patient individually. The goal of public health is to identify and address the root causes of illness and health inequalities that impact entire communities[140]. This shift to population oriented health helps identify and address health issues affecting communities broadly.

The prevention and promotion of health is a major cornerstone of public health alongside promoting community health[141]. Public health aims to lower the burden of sickness and enhance health outcomes for all populations by giving priority to initiatives that prevent disease and advance well-being. In the past, measures like immunisation campaigns, access to clean water, and sanitation upgrades have greatly slowed the development of infectious and waterborne diseases[142]. This proactive strategy is being used today through initiatives like health education, early disease detection programs, healthy lifestyle promotion, and support for policies that promote health[143].

Public health relies heavily on an evidence-based strategy that is supported by data and science. In order to comprehend health challenges and guide remedies, epidemiology—the study of illness patterns and factors in populations—is essential[144]. The field's capacity to develop focused and successful methods is aided by other disciplines like biostatistics, environmental science, social and behavioural sciences, policy analysis, and mathematical modelling. This dependence on data and research guarantees that public health initiatives are both evidence-based and adaptable to changing requirements.

Being flexible and sensitive to changes is crucial in the ever-evolving profession of public health. As life expectancy has increased and disease patterns have changed, public health has

[139] Norick and Morrow, *Defining Public Health*, 5.
[140] Norick and Morrow, *Defining Public Health*, 5.
[141] Norick and Morrow, *Defining Public Health*, 5.
[142] Beishuizen BH, Stein ML, Buis JS, Tostmann A, Green C, Duggan J, Connolly MA, Rovers CP, Timen A, 'A systematic literature review on public health and healthcare resources for pandemic preparedness planning' BMC Public Health, 2024,1.
[143] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 2.
[144] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 6.

refocused its efforts on treating chronic problems rather than infectious diseases[145]. Recognising the influence of social and economic factors on health outcomes, there is now an increasing focus on equity and social determinants of health. Experiences with pandemics, natural catastrophes, and other crises have also increased the field's emphasis on emergency preparedness and response[146].

Public health also recognises that a variety of factors outside of traditional hospital settings interact to impact health. Health outcomes are significantly influenced by social determinants of health, including housing, work, education, and socioeconomic status. Public health is also greatly impacted by environmental variables such as safe housing, access to green spaces, and the quality of the air and water[147]. Collaboration between several sectors, including governmental organisations, healthcare providers, community organisations, educational institutions, corporations, and the general public, is necessary to address these linked concerns[148].

Public health actively strives with the help of science and data, to uphold community health and the core principles it operates under in order to respond to new and emerging threats, incorporate emerging technologies and complex scientific knowledge as well as to address the determinants of health. Public health is a shared duty. Collaboration between people, communities, healthcare professionals, legislators, and governmental organisations is essential to its success. Together, these parties may establish and maintain healthy surroundings, encourage healthy lifestyle choices, and guarantee that everyone has access to necessary medical care.

Relevance of Data Privacy in Public Health

One of the core ethical tenets of healthcare is the preservation of patient autonomy and privacy. By providing clear and thorough information about risks and options, informed consent guarantees people the freedom to make their own decisions about their health and treatment[149].

[145] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 6.
[146] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 2.
[147] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 7.
[148] Beishuizen BH et al, 'A systematic literature review on public health and healthcare resources,' 7.
[149] Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub– on 20 January 2025.

This rule also applies to health data; unless there is a compelling legal or ethical reason, it should not be gathered, processed, or shared without express consent. Essential components of privacy include ownership of one's identity and information, freedom of choice, and bodily integrity. These facets of autonomy and individual dignity are jeopardised in the absence of robust privacy safeguards, hence eroding faith in healthcare institutions.

The possible misuse of health data is another important concern. Large volumes of data are produced by digital technologies, frequently without people's understanding or awareness. Sensitive health information can be deduced from this data through combination and analysis, and it can then be utilised for things like political influence, insurance discrimination, and targeted advertising[150]. Without strong laws, these kinds of practices can lead to an unlegislated situation where there is little control and personal health data is exploited. To ensure that personal information is secured, it is crucial to have clear and enforced data privacy rules that place restrictions on the use, access, and objectives of health data.

The success of public health initiatives depends on public trust, and robust data privacy safeguards are essential to preserving that trust. When people believe that their health data is being collected or used without their consent or proper protections, it can cause widespread mistrust of public health authorities and healthcare systems, which can discourage participation in vital public health activities like disease research and surveillance and even increase litigation[151]. Public health authorities can effectively advance public health efforts by ensuring robust data privacy.

Public health surveillance, for example, is essential for monitoring and controlling diseases, but it frequently involves data collection without explicit consent. Such practices must be governed by strong ethical and legal frameworks to ensure proportionality, legitimacy, and respect for privacy. Public health authorities must act as responsible stewards of the data,

[150] Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub– on 20 January 2025.

[151] Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub– on 20 January 2025.

collecting only the minimum information necessary and anonymising it where possible[152]. Strong privacy laws are necessary to ensure that public health interventions are conducted transparently, ethically, and with comprehensive respect for individual privacy.

Solid data privacy regulations are necessary to protect individual liberty, stop data abuse, preserve public confidence, strike a balance between the rights of individuals and public health requirements, and handle the particular difficulties of the digital age. These regulations must guarantee that people are shielded from damage and discrimination and maintain sovereignty over their health information. The objectives of individual liberty and public health could be jeopardised in the absence of such protections.

Cross reference with Kenya's Public Health and Data Privacy Regime

The Public Health Act of Kenya outlines the duties of the Medical Department with strong emphasis placed on advising local authorities, promoting public health, and preventing contagious diseases[153]. Additionally, it gives health authorities the authority to protect public health by implementing measures like disease control and sanitation, and it requires the gathering and dissemination of information on infectious diseases[154]. However, the Act's current scope largely focuses on infectious diseases and physical health dangers, paying little consideration to contemporary issues like patient permission, data privacy, and the moral use of medical information. Public health must adjust to new issues in the current digital era, especially those pertaining to the management of health data[155].

A contemporary definition of public health ought to be included in order to fortify the Act and stop data breaches and abuse[156]. The ethical gathering, storing, and use of health data should be specifically included by this concept, which recognises public health as a shared duty that upholds individual liberty and privacy. The Act would be in line with modern conceptions of public health, which increasingly take into account a wider range of social, environmental, and

[152] Grande D, Marti XL, Feuerstein-Simon R, Merchant RM, Asch DA, Lewson A, Cannuscio CC, 'Health Policy and Privacy Challenges Associated with Digital Technology' *Publishing Platform*, 2020, page 9.
[153] Section 10, *Public Health Act* (Act No.790 of 1921)
[154] Section 13, *Public Health Act* (Act No.790 of 1921)
[155] Petteway R, Rebanal D, Raphael C, Matsuoka M, 'Public Health', in Raphael C, Matsuoka M (eds), *Ground Truths: Community-Engaged Research for Environmental Justice,* University of California Press, California, 2024
[156] Petteway R *et al*, 'Public Health'

digital elements, by broadening the field's focus beyond the control of infectious diseases[157].

Clear standards for avoiding consent in some, strictly specified situations, such as actual emergencies or public health crises, should be established under the Act[158]. To prevent misuse of this authority, measures like data anonymization and ethical supervision must be in place even in these circumstances. Emergency protocols should reduce privacy rights violations by making sure that actions are appropriate, reasonable, and subject to stringent rules[159]. Such clear and concise parameters will ensure the proper enforcement of Section 31 of the Digital Health Act in situations of actual emergencies.

The Kenyan Public Health Act can be updated to take into account the moral and practical issues surrounding data privacy by implementing these changes. This would safeguard the rights of citizens while guaranteeing the efficient and moral accomplishment of public health objectives. Public trust may be damaged in the absence of a strong legal framework, which would compromise the effectiveness of public health programs. A revised Act would take into account how public health is changing and make sure it is current and adaptable to the demands of the digital era.

Conclusion

In order for public health to achieve its intended goal of promoting and protecting community health and for the privacy of all citizens to be maintained, there needs to be clear and concise instances where public health can be invoked as a reason to bypass consent in processing one's data. Regardless of the validity of the claim of public health, there needs to be guidelines to ensure that such an avenue cannot be abused and misused by data processors and by the relevant authorities in general.

[157] World Health Organisation, *Organisation and Financing of Public Health Services in Europe*, 82

[158] Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub– on 20 January 2025.

[159] Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub– on 20 January 2025.

CHAPTER FOUR

Introduction

This chapter will explore how has Germany's Digital Healthcare Framework successfully balanced patient consent, data privacy and public health. Additionally, the chapter will analyse whether the approach taken by Germany can effectively be used within Kenya's Legislative framework in order to more adequately protect patient data.

Justification for choosing Germany for this comparative analysis

Germany's extensive legal and regulatory framework makes it a useful topic for comparative study in the fields of public health and health. The nation has a comprehensive healthcare regulatory framework, with laws specifically addressing patient rights, digital health (DigiG, GDNG), and data privacy (BDSG)[160]. Together with the EU's General Data Protection Regulation (GDPR), these rules establish a structured framework that facilitates a better comprehension of how policy and practice interact. Germany's dedication to legal clarity guarantees that healthcare laws are precise and strike a balance between the need for developments in digital health and data protection.[161]

In its health sector, Germany is also aggressively pursuing digitalisation through programs designed to facilitate data sharing, enhance patient access, and encourage creative applications.[162] Germany is therefore an interesting case study to examine the potential and

[160] Bolcato V, Franzetti C, Fassina G, Basile G, Martinez R, Tronconi L, 'Comparative Study on Informed Consent Regulation in Health Care among Italy, France, United Kingdom, Nordic Countries and Spain', 103, *Journal of Forensic and Legal Medicine,* 2024,4.

[161] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.

[162]<https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.

difficulties of incorporating digital technologies into healthcare.[163] Additionally, its strong public health infrastructure—which includes a decentralised public health service (ÖGD) made up of state and local health departments—offers important insights on how to efficiently plan, fund, and integrate public health services into a national healthcare system.[164]

Both Germany and Kenya through having difference in legal systems and economic structures, have faced fundamental problems in creating a legal framework that protects data privacy while at the same time allowing for the use of public health initiatives and research. This shared objective, despite the differences has provided a strong foundation for comparison between the two jurisdictions. Germany's implementation of their General Data Protection Regulation includes how it has addressed public health exceptions and the use of personal health data for research.[165] Such legislation can offer much needed insights for Kenya as it refines its own data protection and digital health strategies.[166]

With laws like the Digital Act (DigiG) and the Health Data Use Act (GDNG), Germany has acknowledged the issue of fragmented health data and is attempting to digitise it. While guaranteeing adherence to data protection laws, these laws seek to improve the use of health data for public health and research.[167] In a similar vein, Kenya is promoting digital health with the Digital Health Act, while Germany's experience provides insightful guidance on how to efficiently aggregate and use health data. Notably, Kenya's developing digital health framework can learn a lot from Germany's difficulties integrating data and managing a variety of practice management systems.

Public health legislation in Kenya and Germany outline the duties and authority of public health officials. The Public Health Act of Kenya[168] and the Infection Protection Act of Germany provide legal frameworks for the prevention and management of disease. How each nation incorporates these public health laws with its own data privacy frameworks to establish

[163] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[164] < https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ > on 15 March 2025.
[165] Bolcato V *et al,* 'Comparative Study on Informed Consent Regulation in Health Care among Italy, France, United Kingdom, Nordic Countries and Spain', 5.
[166] Bolcato V *et al,* 'Comparative Study on Informed Consent Regulation in Health Care among Italy, France, United Kingdom, Nordic Countries and Spain', 5.
[167] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 4.
[168] Public Health Act

exceptions for essential public health initiatives is a crucial area of comparison. Germany's approach, where the Infection Protection Act interacts with GDPR Article 9(2)(i), is a particularly pertinent reference point because Kenya's Digital Health Act clearly relates public health exclusions to the Public Health Act.

From its early beginnings to more recent reforms, Germany's health system's historical development offers a rich context for comprehending the opportunities and difficulties facing the country's healthcare and public health sectors today.[169] The nation is well-positioned for comparative research on cross-border healthcare and data sharing due to its active participation in European Union programs like the European Health Data Space (EHDS) and its involvement in transatlantic data collaborations.[170]

The German Legal Framework in regards to Data Protection, Digital Health and Public Health

Data Protection Framework

The General Data Protection Regulation (GDPR)[171], the fundamental piece of data protection law throughout the European Union (EU), largely oversees Germany's data protection system. All EU member states must adhere to the same data protection standards set forth by the GDPR, which guarantees that personal information is handled fairly, legally, and openly. The Act gives definition for important terms like controller, processor, data subject, personal data, and processing. The GDPR also defines some types of sensitive data, including genetic, biometric, and health data, that need further protection since they may affect people's rights and liberties.

The Federal Data Protection Act (BDSG)[172], which Germany passed in order to supplement the GDPR, offers extra national requirements that are relevant to certain situations, most notably data processing connected to employment. The BDSG explains some exclusions from the legislation, such as actions taken by natural persons for exclusively domestic or personal

[169] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[170] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[171] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[172] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.

reasons. This guarantees the protection of individual privacy without placing an undue burden on people to comply with regulations in private settings. Additionally, the BDSG improves GDPR regulations for German law enforcement, government agencies, and private sector enterprises, permitting more stringent national standards as needed.[173]

According to the GDPR and BDSG's data protection principles, processing personal data is normally forbidden unless there is a valid reason. These legal justifications include the data subject's express consent, contractual requirements, legal duties, safeguarding vital interests, the public interest, or legitimate interests that a controller or third party is pursuing.[174] Additionally, data must be gathered for clear, specific, and justifiable purposes, and any subsequent processing must not conflict with the initial intent. Purpose limitation is a principle that makes sure that personal information isn't used in ways that can infringe on people's right to privacy.[175]

The GDPR's protection of individual rights with regard to personal data is one of its most important features. A wide range of rights are granted to individuals, also known as data subjects, such as the ability to access their personal information, correct errors, request erasure (also known as the "right to be forgotten"), limit processing, exercise data portability, object to processing, and receive information about how their information is gathered, used, and stored.[176] These rights enable people to keep more control over their personal information and to take legal action when those rights are infringed.

Digital Health Care Framework

In order to promote digital healthcare, increase data accessibility, and guarantee robust patient data protection, Germany has passed a number of important laws. Among these, the Digital Act (DigiG)[177] is essential for using digital solutions to streamline healthcare. Improving the

[173] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[174] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[175] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[176] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[177] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.

electronic patient record (ePA), a centralised digital repository for patient health data, is one of its main goals.[178] Because of its user-friendly design, the ePA makes sure that vital medical information, including prescription drugs, allergies, and similar patient data, is kept safe and readily available.[179] Additionally, the DigiG requires electronic prescriptions, which lessens the need for paper prescriptions and increases drug management effectiveness. Additionally, it incorporates digital health applications (DiGAs) into routine care, increasing patient and healthcare provider access to digital solutions.[180]

The Health Data Use Act (GDNG)[181], which aims to make it easier to use health data for research, is another important piece of legislation. The GDNG creates a central data repository and a point of coordination to manage and supervise access to health data in order to do this.[182] Germany's adherence to the European Health Data Space (EHDS), a program designed to promote cross-border health data interchange inside the EU, is being facilitated by this legislation. The GDNG guarantees that researchers and policymakers can access high-quality, anonymised health data while maintaining stringent privacy controls by establishing a well-organised infrastructure for health data use.[183]

The Patient Data Protection Act (PDSG)[184] strengthens security protocols for patient data while introducing cutting-edge digital applications. All healthcare facilities that use telematics infrastructure—which creates a safe online network between hospitals, clinics, pharmacies, and insurance companies—are subject to this law.[185] Through strict security protocols, the PDSG guarantees that patient data stored electronically is safeguarded, promoting confidence in digital healthcare services and facilitating effective data sharing across healthcare providers.[186]

Public Health Framework

Germany's federal structure has a significant impact on its public health legal and regulatory

[178] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[179] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[180] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 34.
[181] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[182]Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[183]Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[184] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[185] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[186] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.

system because the Federal Ministry of Health (BMG) sets the national legal framework and creates public health policies, regulations, and strategies.[187] The Länder define legal parameters, responsibilities, and the organisation of local public health authorities, which results in variations in implementation across different regions.[188]

Important federal laws that have shaped Germany's public health system include the Infection Protection Act (IfSG), which establishes hygiene standards, mandates reporting protocols for communicable diseases, and governs the prevention and control of infectious diseases by defining the roles of public health authorities and healthcare providers.[189] The Robert Koch Institute (RKI) serves as the main national advisory body for disease surveillance and outbreak response under the IfSG.[190] Social services, public health welfare, and health insurance are all governed by the German Social Code (SGB). It guarantees fair access to healthcare and high standards of quality while outlining the obligations of healthcare providers.[191]

The 2015 Preventionsgesetz, or Act to Strengthen Health Promotion and Prevention controls vaccination programs, financing for public health initiatives, and expanding health checkups, thus further improving preventative healthcare.[192] However, since statutory health insurance providers (SHI) are crucial to its execution, it is still unclear how ÖGD will fit into the picture. The 2013 Patient's Rights Act is the law that indirectly improves public health by encouraging openness and patient autonomy, even if its primary focus is on informed consent and the relationships between individual patients and providers. Finally, public health laws are passed by every federal state creating variations in regional health policies and service delivery.

Germany's Legal and Regulatory Standpoint of Patient Consent

According to Germany's extensive regulation, patient consent is a mandatory requirement prior to any healthcare activity.[193] While consent can be given orally or in writing, written consent is required for major health risks, such as surgery. The German legal framework emphasises

[187] < https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/> on 15 March 2025.
[188] European Observatory on Health Systems and Policies, *Germany: Health System Summary 2024,* 12.
[189] European Observatory on Health Systems and Policies, *Germany: Health System Summary 2024,* 12.
[190] European Observatory on Health Systems and Policies, *Germany: Health System Summary 2024,* 12.
[191] < https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ > on 15 March 2025.
[192] < https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ > on 15 March 2025.
[193] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.

that the patient must always be given the necessary information in a personal consultation before giving consent.[194] This information must clearly explain the nature, significance, and implications of the treatment, including alternative treatments and associated risks, in a comprehensible and appropriate manner.[195] Moreover, a sufficient period for reflection should be ensured for more significant interventions.

A unique rule on informed consent was adopted in Germany by the Patients' Rights Act (2013), emphasising the relationship between the patient and the healthcare professional.[196] With respect to the flexibility of public health to handle patient data without consent, German law permits exceptions to the need for express consent within the framework of the EU's GDPR and state laws such as the BDSG.[197]

Comparative analysis of Public Health Exceptions for Bypassing Patient Consent in Kenya and Germany

In general, Germany takes a firmer stance than Kenya when it comes to protecting patient privacy and the requirements for processing medical records without authorisation. This is mostly because of the extensive framework set up by the GDPR of the European Union and the particular national legislation of Germany that apply and enhance it. High standards for data protection are set by the GDPR, especially when it comes to sensitive personal data, such as health information.[198] In contrast, Germany's general legislative framework, enforcement procedures, and built-in safeguards seem more solid, even though Kenya's Data Protection Act (DPA) similarly classified health data as sensitive personal data.[199]

The necessity for explicit consent for processing health data is a significant difference

[194] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[195] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[196] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[197] <https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions> on 16 March 2025.
[198] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[199] Section 19, *Digital Health Act* (Act No. 57 of 2023).

between the two systems. The GDPR requires that the fundamental legal basis for handling particular categories of personal data, such as health data, be explicit consent. This criterion guarantees that people are fully aware of and consent to the use of their personal health information.[200] The GDPR places a greater emphasis on express consent, even though Kenya's DPA acknowledges the necessity of consent for processing health data.[201] Clear, unequivocal, and informed consent from the data subject, along with the ability to revoke consent at any time, are requirements for valid consent under the GDPR. Compared to Kenya's Data Protection Act, which is protective but does not seem to give explicit consent the same legal weight as the GDPR, these requirements establish a greater standard of protection.

Although Germany's legal system places more stringent requirements and protections, both countries allow the collection of health data without consent for public health purposes. The GDPR permits data processing when there is a significant public interest, but this must be justified by Union or Member State law, guaranteeing that any exceptions are reasonable, uphold fundamental rights to data privacy, and include individual safeguards.[202] By raising the bar for public health exemptions, this makes sure that private information isn't exploited for ambiguous purposes.

Kenya's Digital Health Act, on the other hand, permits the processing of health data when it is required to carry out a task that serves the public interest.[203] Although this is in line with the idea of public health necessity, it does not, as the GDPR does, mandate proportionality evaluations or establish a significant public interest criterion. Furthermore, the GDPR framework is used by Germany's Infection Protection Act, which regulates public health measures.[204] As a result, any data processing for public health purposes must still abide by the GDPR's rules and regulations. This multi-layered strategy makes sure that exemptions for the public interest don't erode the rights to data protection.

[200] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[201] Section 30, *Data Protection Act* (Act No. 24 of 2019).
[202]< https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ > on 15 March 2025.
[203] Section 31, *Digital Health Act* (Act No.57 of 2023)
[204] < https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ > on 15 March 2025.

Germany has passed laws like the Patient Data Protection Act that specifically address the protection of digital health data.[205] This law ensures that digital health records are managed with strict safeguards by establishing precise security and handling criteria for electronic patient files. Additionally, the PDSG establishes national standards for the security of electronic health records and requires secure telematics infrastructure.[206] Although Kenya is likewise building out its digital health infrastructure, the country's laws governing data security in digital healthcare systems are not as clear. Kenya's present legal system lacks comprehensive safeguards aimed at safeguarding digital health records, in contrast to Germany's PDSG. As a result, there may be a vulnerability in providing robust safeguards for digital patient data.

The GDPR framework in Germany requires "data protection by design and by default," which means that privacy protections must be incorporated into digital health systems from the beginning.[207] Instead of establishing robust privacy measures after data processing has started, this approach guarantees that organisations proactively implement them. By requiring businesses to adopt the most stringent privacy settings by default, the GDPR lowers the possibility of unauthorised data exposure.[208] While privacy by design and default are mentioned in Kenya's ODPC Guidance Note, organisations are legally required to adhere to these principles under the GDPR. Thus, compared to Kenya, privacy protections in Germany are more enforced due to their structural integration into digital health systems.

Germany and Kenya both include exceptions to the consent requirements in order to safeguard the public's health. Nonetheless, there are notable differences between the two nations in the extent, protections, and legislative coherence of these exclusions.

The Public Health Act of Kenya gives public health officials extensive authority to take the required steps to stop and manage the spread of illnesses.[209] Building on this, the Digital Health Act, which is presently being considered, expressly offers a consent exemption for public health reasons. In particular, consent is not necessary "for public health in accordance with the

[205] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[206] Federal Ministry of Health, *Germany's Digitalisation Strategy,* 2023, 33.
[207] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[208] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 2.
[209] Section 64(3), *Public Health Act*

Public Health Act," according to Section 31(2) of the Act. This indicates that in certain situations, requirements related to data protection may be superseded by those related to public health. The absence of a precise threshold for need or proportionality in the Act, however, may allow for a subjective interpretation.

In order to improve public health outcomes, Kenya's ODPC Guidance Note encourages the sharing of health data with organisations like government agencies, healthcare providers, and researchers.[210] However, it stresses that, unless specifically exempted by law, such processing should still adhere to confidentiality, privacy, and consent principles. In the Kenya Legal and Ethical Network on HIV/AIDS (KELIN) & 3 others v. Cabinet Secretary Ministry of Health & 4 others[211] case, the court addressed a government directive that aimed to divulge HIV status without informed permission, highlighting the significance of legal scrutiny in such circumstances. The case brought to light the conflict between individual privacy rights and public health requirements, highlighting the need for a more precise legislative balancing process.[212]

GDPR Article 9(2)(i),[213] which allows the processing of sensitive health data "for reasons of public interest in the area of public health," serves as the foundation for the public health exceptions to consent in Germany. As long as processing is supported by Union or Member State law and incorporates suitable safeguards to protect individual rights, this includes protection against significant cross-border health threats or guaranteeing high-quality healthcare. Germany carries out this clause through a number of strong legislative tools, including the Federal Data Protection Act (BDSG), which permits exceptions under specific circumstances in the areas of public interest, scientific research, and public health monitoring.[214]

The Infection Protection Act (Infektionsschutzgesetz) authorises data processing required for public health measures and offers a thorough legal foundation for illness prevention, surveillance, and response. Crucially, it functions within the scope of the GDPR, guaranteeing

[210] ODPC Guidance Note on Processing of Health Data
[211] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* (2016) eKLR.
[212] *Kenya Legal and Ethical Network on HIV&AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* (2016) eKLR.
[213] Article 9(2)(i), *General Data Protection Regulation* (Germany).
[214] Section 22, *Federal Data Protection Act* (Germany).

that even exemptions for the public interest are still subject to the standards of proportionality, necessity, and safeguarding. Germany's main organisation for disease management, the Robert Koch Institute, is essential to carrying out this legislative requirement.[215]

Furthermore, with recent laws like DigiG and the GDNG, Germany has taken aggressive measures to capitalise on the value of health data.[216] In order to integrate data privacy regulations with public health objectives, the GDNG creates a centralised data repository that makes anonymised health data easier to access for study and policymaking. In order to strengthen privacy even in digital healthcare settings, the PDSG also requires strict security and interoperability standards for electronic health records.

Conclusion

Kenya and Germany both have a strong commitment to protecting patient data, but it seems that Germany's structure offers more thorough protections. A more robust and legally enforceable system is produced by the GDPR's emphasis on explicit consent, tight cross-border data transfer requirements, multi-layered enforcement mechanisms, particular digital health data protection legislation, and strict conditions for public interest exemptions.

Although Kenya's Data Protection Act has a solid basis, it is devoid of several of the more comprehensive and binding clauses contained in Germany's data protection framework. Adopting some of Germany's more stringent data protection rules could improve patient privacy and security in Kenya's healthcare industry while the country develops its own digital health regulations.

[215] European Observatory on Health Systems and Policies, *Germany: Health System Summary 2024,* 12.
[216] Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024, 5.

CHAPTER FIVE

Introduction

This Chapter summarises the findings of the study as developed and broken down in previous Chapters. Recommendation will be made in this Chapter that will help in addressing the issue of balancing individual patient data rights and public health necessity. The chapter will therefore conclude the research paper.

Summary of Findings

This study has examined the digital health framework and the potential risk of abuse by means of public health in Kenya. It has sought to determine whether public health can be protected and upheld without interfering with the confidentiality of patient data.

Chapter one formed the basis of this research project. It establishes the existence of a legal gap in the law addressing the exceptions to the processing of patient data without consent on the premise of Public Health exceptions. The chapter set out the objectives of the research, established the specific questions that are relevant to the study, laid out the conceptual framework and reviewed relevant scholarly studies and academic work that are applicable with regard to the subject matter of the study. The first research question sought to understand the scope of the Digital Health Act and how it governs the processing of patient data without explicit consent. The second research question sought to investigate the applicable law in Kenya in relation to digital health, data protection and public health. The third research question sought to determine how Germany has considered the interplay between protecting patient data and explicit consent in processing health data and the public health necessity.

Chapter Two explored the legal, policy and regulatory frameworks in Kenya with regards to protection of patient data, digital health and public health. The chapter disclosed that though

Kenya does have legislation that covers all three areas, the framework does not adequately provide parameters for which public health can be a necessary reason for the processing of patient data without the data subjects consent.

Chapter Three investigated the public health legislation in depth and in regards to the exception provided for under the Digital Health Act to process patient data for the purposes of upholding public health in line with the Public Health Act. The chapter identified the need for stronger guidelines to ensure that the avenue provided by law cannot be abused and misused by data processors and by the relevant processors. The chapter ultimately established that the law was not clear in addressing the issue of processing patient data for public health purposes.

Chapter Four introduces a comparative analysis of patient privacy and consent laws within the digital health framework between Kenya and Germany. It starts by looking at the legal and regulatory framework in Germany and how such legislation addresses the issue of bypassing patient consent in processing the patient's data for public health reasons. In comparing the two legislative frameworks, it is evident that the German framework defines the parameters for processing patient data more clearly and has stricter guidelines to prevent the abuse of patient data and balances public health necessities and individual rights far better than the Kenyan legal framework.

Chapter five concludes the analysis of this study by summarising the findings and offers recommendations to address the issue of balancing patient privacy rights and public health necessity in Kenya. It will also identify the applicable policies and insights from Germany and how it can be transferred into the Kenyan space.

Recommendations

The study proposes the following recommendations:

1. The Digital Health Act, being the primary legislation in the digital healthcare framework in Kenya, under section 31, can be amended to include the relative and allowable public health parameters for the bypassing of patient consent that it provides for. By making such an amendment, this will introduce stricter regulation of public health exceptions. The GDPR in Germany sets a high threshold by requiring

that public interest justifications be proportionate, necessary and to provide adequate safeguards. The Digital Health Act should introduce similar safeguards to prevent misuse of public health exceptions. Additionally, the Public Health Act should explicitly define public health and set out clearer parameters for when patient consent can be bypassed as the absence of such creates an ambiguity that makes it difficult to determine the boundaries within which personal health data can be processed without consent.

2. Establishment of an independent oversight body distinct from the Office of the Data Protection Commissioner to guarantee accountability and openness in the use of public health data. This body would have the express responsibility of keeping an eye on how health data is gathered, stored, shared, and used in government agencies and healthcare initiatives. To guarantee that data protection principles are applied consistently and contextually across public and private healthcare players, sector-specific norms for health data governance should be created and put into effect. These rules ought to address fundamental topics including anonymisation, informed consent, data minimisation, access controls, and safe data storage. Standardising data-sharing processes across all government health departments is also crucial to prevent fragmented or inconsistent practices. This will facilitate the successful implementation of digital health projects under Universal Health Coverage (UHC), improve interoperability, and guarantee data integrity.

3. The judicial system must take a proactive role in ensuring that individual rights are not violated in the pursuit of public health objectives. A specialised tribunal within the ODPC should be established to resolve health data issues swiftly and properly. This will create a faster resolution process and expert jurisprudence on digital health data regulation. Furthermore, judicial review mechanisms must be established to allow individuals to dispute decisions involving their health data, including cases in which their data is shared without their consent or utilised in automated decision-making processes. Such reviews would act as a key safeguard against potential abuse or overreach. To keep up with the complexity of evolving digital health systems, constant training for court officers is required. These capacity-building activities should

concentrate on emerging technologies, privacy standards, and international best practices to ensure that data protection decisions are well-informed and equitable.

4. The corporate sector and civic society play critical roles in improving health data governance and cultivating a culture of data accountability. Healthcare institutions, civil society organisations, and technology providers must work together to define ethical norms, promote privacy-enhancing technologies, and establish rigorous accountability mechanisms. Joint initiatives can enhance government efforts by providing practical solutions and peer-based compliance tools. Furthermore, public awareness efforts are necessary to educate citizens about their data privacy rights, especially in the context of public health programs and catastrophes. Informed citizens are better able to provide meaningful consent and seek remedy in the event of a breach. Finally, industry actors can help to create capacity among health-care workers by providing ongoing training in data protection principles, cybersecurity, and digital health ethics. This will improve responsible data handling and boost trust in health data systems overall.

Conclusion

This study finds that balancing public health imperatives with confidentiality requires a nuanced, well regulated and transparent approach and by integrating mechanisms that safeguard both patient data and public health, the healthcare delivery system can develop to serve the society better.

BIBLIOGRAPHY

Chapters in Books

Petteway R, Rebanal D, Raphael C, Matsuoka M, 'Public Health', in Raphael C, Matsuoka M (eds), *Ground Truths: Community-Engaged Research for Environmental Justice,* University of California Press, California, 2024.

Aman, Haque M, 'Big Data Analytics in Health Sector: Need , Opportunities, Challenges, and Future Prospects'. in Tanwar P, Jain V, Liu C (eds), '*Big Data Analytics and Intelligence: A Perspective for Healthcare*', Emerald Publishing Limited, Bingley, 2020.

Journal Articles

Batko K, Slezak A, 'The Use of Big Data Analytics in Healthcare,' *PubMed Central.*

Hussein A, Zarour M, Alenezi A, Krishna A, Agrawal A, Kumar R, Ahmed R, 'HealthCare Data Breaches: Insights and Implications', 8 *Healthcare Journal* 2, 2020.

Davis S, 'The Trojan Horse: Digital Health, Human Rights, and Global Health Governance', 22 *Health and Human Rights Journal* 2, 2020.

Wilson D, Sheikh A, Görgens M, Ward M, 'Technology and Universal Healthcare Coverage: Examining the Role of Digital Healthcare,' 11 *Journal of Global Health,* 2021.

Murdoch B, 'Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era', 22 (122) *BMC Medical Ethic,* 2021.

Arafa, A, Sheerah, H.A, Alsalamah, S. Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review.

Shimonski R, *AI in Healthcare: How Artificial Intelligence is Changing IT Operations and Infrastructure Services,* John Wiley & Sons Incorporated,1 ed, Indiana, 2021.

Sedenberg E, Mulligan D, 'Public Health as a Model for Cybersecurity Information Sharing', 30 *Berkeley Technology Law Journal* 3, 2015.

Tse D, Tong C, Ly T, Tam K, Chow C, The Challenges of Big Data Governance in Healthcare, *International Conference on Trust, Security and Privacy in Computing and Communications,* 2018.

Mählmann L, Reumann M, Evangelatos N, Brand A, 'Big Data for Public Health Policy-Making', 20 *Public Health Genomics Journal* 6, 2017.

Cordeiro JV, *Digital Technologies and Data Science as Health Enablers: An Outline of Appealing Promises and Compelling Ethical, Legal, and Social Challenges.*

Ganesan D, 'Human Rights Implications of the Digital Revolution in Health Care in India', 24 *Health and Human Rights Journal* 1, 2022.

Evans B, 'In the Medical Privacy of One's Own Home', in Cohen G, Kramer D, Milstein J, Shachar C (eds), *'Digital Healthcare Outside of Traditional Clinical Setting,* Cambridge University Press, Cambridge, 2024

Hussein A, Zarour M, Alenezi A, Krishna A, Agrawal A, Kumar R, Ahmed R, *Healthcare Data Breaches: Insights and Implications.*

Norick LF and Morrow CB, *Defining Public Health: Historical and Contemporary Development*, Jones and Bartlett Publishers.

Beishuizen BH, Stein ML, Buis JS, Tostmann A, Green C, Duggan J, Connolly MA, Rovers CP, Timen A, 'A systematic literature review on public health and healthcare resources for pandemic preparedness planning' BMC Public Health, 2024.

Grande D, Marti XL, Feuerstein-Simon R, Merchant RM, Asch DA, Lewson A, Cannuscio

CC, ‘Health Policy and Privacy Challenges Associated with Digital Technology’ *Publishing Platform*, 2020.

Bolcato V, Franzetti C, Fassina G, Basile G, Martinez R, Tronconi L, ‘Comparative Study on Informed Consent Regulation in Health Care among Italy, France, United Kingdom, Nordic Countries and Spain’, 103, *Journal of Forensic and Legal Medicine,* 2024

Reports

Kenya Legal and Ethical Network on HIV&AIDS, *Enhancing Privacy and Confidentiality in the Management of Public Health Data.*

World Health Organisation, *Organisation and Financing of Public Health Services in Europe.*

Cybersecurity and Data Privacy Update, *EU and Germany Lay Groundwork for the use of Medical Data for research and AI training,* 2024.

Federal Ministry of Health, *Germany’s Digitalisation Strategy,* 2023.

European Observatory on Health Systems and Policies, *Germany: Health System Summary 2024.*

Other Internet Sources

<https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far>

<https://www.techtarget.com/searchdatamanagement/definition/big-data>

<Healthcare Data Breach Statistics (hipaajournal.com)>

<Thousands of patients hit by NHS data breaches | The Independent>

<Data of 14,200 people with HIV leaked online by US fraudster who was deported from Singapore | The Straits Times>

<https://www.cdcfoundation.org/what-public-health>

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html?form=MG0AV3>

J. Andrew, R. Jennifer Eunice and J. Karthikeyan, 'An Anonymization-based privacy-preserving data collection protocol for digital health data', *Frontiers in Public Health*, 2023,– Frontiers | An anonymization-based privacy-preserving data collection protocol for digital health data (frontiersin.org)

<https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/>

<https://datarecovery.co.ke/rising-data-protection-challenges-to-healthcare-in-kenya/?form=MG0AV3>

<https://www.waldenu.edu/programs/health/resource/what-is-public-health-and-why-is-it-important>

Bolcato V, Franzetti C, Martinez RM, Fassina G, Tronconi LP, 'Comparative study on informed consent regulation in health care among Italy, France, United Kingdom, Nordic Countries, Germany, and Spain' *Journal of Forensic and Legal Medicine,* 2024— https://www.sciencedirect.com/science/article/pii/S1752928X24000362?via%3Dihub

<https://iclg.com/practice-areas/data-protection-laws-and-regulations#:~:text=ICLG%20%2D%20Data%20Protection%20covers%20common,and%20processors%20%E2%80%93%20in%2031%20jurisdictions>

< https://www.endpointprotector.com/blog/all-you-need-to-know-about-germanys-patient-data-protection-act/ >

Faridoon A, Kechadi M, 'Healthcare Data Governance, Privacy and Security: A Conceptual Framework', *University College Dublin Law Journal,* 2024, 5, Healthcare Data Governance,

Privacy, and Security - A Conceptual Framework (arxiv.org)