Strathmore University
Centre for Intellectual Property and Information Technology Law

The New Wave of eHealth:

AI and Privacy Concerns? A Case Study of Kenya

Joshua Kitili and Natasha Karanja

Background and Purpose

Technological advancement in Low to Middle Income Countries (LMICs) is held to precede regulation, as the government and regulatory bodies lag behind formulating and developing standards and regulations that oversee "technological adoption , implementation usage, access, security and privacy."[1] There is a need for legal standards for innovators who utilise these advancements to develop health solutions in LMICs. Standards are held to be "necessary specifications" that are vital for alignment with national and international regulations, that ensure safe operations of the innovations in a manner that prevents harm. [2]

Specifically looking towards the implementation of Artificial Intelligence (AI), AI in the healthcare sector is held to be a progressive means of achieving equitable access to healthcare. AI innovations are held to have the potential to expedite "the development of affordable, quality and accessible" innovations whilst simultaneously "overcoming the local resource-constrained environment."[3] This is achieved by the innovations mitigating existing shortcomings of the healthcare sector by "leveraging software platforms" that are easily accessible and affordable to the general public.[4] Looking towards the Kenyan context, AI is held to have the "potential" of achieving Kenya's Big Four's Agenda, specifically the agenda of Universal Healthcare.[5]

Despite AI's potential to address health challenges, there is increasing concern about regulation of AI in the healthcare sector, where AI healthcare technologies hold the risk of " negatively" affecting data management , quality and safety of the users.[6] The collection, use, storage and sharing of personal health information raises queries over the "consent, ownership , access" of the data, [7] as there is risk of "privacy violations and discriminatory practices."[8]

Considering the sensitivity of the data that is used and the legal implications that arise, the following study looks towards assessing the rise of Kenyan AI eHealth platforms. Assessment here lies with interrogating whether there are privacy initiatives in place; if so, do the privacy initiatives adhere to the required national legal standards stipulated in strategic policies, acts of parliament and relevant international legal standards. In addition, the study will assess the efficacy of the privacy policies, here factors such as the structure and design will be considered. This will involve evaluating the comprehension of the privacy policies from the viewpoint of an average Kenyan and the barriers that limit comprehension (e.g.; legal jargon, length of the policies..etc).

Objectives of the study

The study objectives were as follows,

- To understand and analyse the implementation of existing privacy initiatives in place that protect the right to privacy and transparency of personal data within Kenyan AI eHealth platforms.

[1]Egwar A A & Nabukanye J , A Conceptual Model for Adaption of eHealth Standards by Low and Middle Income Countries [2018] JHIA, 11th Health Informatics Africa Conference 2018,10
[2]ibid..11
[3]Alami, H., Rivard, L., Lehoux, P. et al., Artificial intelligence in health care: laying the Foundation for Responsible, sustainable, and inclusive innovation in low- and middle-income countries [2020] GH Vol 16:52, 2
[4]ibid
[5] Ministry of Information, Communications and Technology, Emerging Digital Technologies for Kenya, Exploration and Analysis< https://www.ict.go.ke/blockchain.pdf > last accessed 19th June 2022,95
[6]Alami (n3)
[7]ibid
[8]Vayena E, Blasimme A & Cohen I.G, Machine learning in medicine: addressing ethical challenges [2018] PLoS Med.,15(11)

- To supply evidence of the need to remodify current privacy initiatives within the Kenyan AI eHealth platforms.
- To propose necessary remodification of existing legal reforms / privacy initiatives to ensure efficacy of the law and policies are at a satisfactory standard that reflects the interests and needs of all relevant stakeholders.

Methodology

The main method of research used was desk-based research that relied on collecting data from existing sources and building on the information that has already been gathered. This involved mapping the eHealth platforms into relevant categories. To start off, the platforms were grouped into the various types of eHealth platforms present. The platforms were then further grouped into their functional role. Thereafter, the presence of privacy initiatives was assessed, with the focus narrowed down to the analysis of five platforms from a list of fifteen platforms. Justification of the five centered around the depth, presence and quality* of the privacy initiatives present. The analysis looked towards assessing the policies against the national / international legal standards present. A critical approach was also adopted in assessing the efficacy of the structure and design of the privacy initiatives in place.

Literature Review

Research has looked towards the barriers that limit ehealth platforms from being transparent and accountable to their users. In order to mitigate the barriers most recommendations have placed emphasis on privacy policies as a means of providing privacy to patient's data. The policies should be reflective of transparency, accountability and safety of the patient's data.

The definition of electronic health records and eHealth platforms is necessary when conducting a detailed analysis of the privacy measures put in place. According to Juergen Hohmann and Stefan Benzschawel who are the authors of *Data Protection in eHealth platforms*, ehealth platforms enable the improved sharing and exchange of 'relevant health information of each patient.'[9] The authors also discuss important data protection principles that are fundamental when processing health data.

The protection of personal data around the world has taken time to develop. Jurisdictions with well-established privacy laws can be found for instance in European countries. African countries have enacted privacy laws recently and therefore existing international laws and non-binding agreements play a fundamental role in informing lawmakers on how privacy laws should be drafted. A report by the World Health Organisation analysed the ethical and legal aspects of privacy in healthcare. The international laws analysed include the Universal Declaration of Human Rights, the European Convention on Human Rights and the European Union Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[10]

A data processor should adhere to the principles of data protection since they handle personal data and in this case health data which may be extremely sensitive. Enzo Maria Le Fevre and Giselle Heleg

[9]Roy G. Berane(ed), Legal and Forensic Medicine (Springer 2013)

[10]WHO, Legal Frameworks for eHealth <http://apps.who.int/iris/bitstream/handle/10665/44807/9789241503143_eng.pdf;jsessionid=7C370A2902734882A75EC2A05F1D-1C92?sequence=1 > accessed 21 November 2022

address this in their article *Artificial Intelligence in Medicine:Laws, Regulations and Privacy.* Some of the principles they emphasize on include transparency, purpose, minimization, accuracy, suppression, need for collection and safety.[11]

Other authors have discussed the importance of having privacy policies in place so as to protect the personal data of patients. Naipeng Dong, Hugo Jonker and Jun Pang note the importance of privacy policies and also three main approaches that need to be taken to protect patients' privacy.[12] The three main approaches include patient privacy by access control, by architectural design and through cryptographic approaches.[13] The approaches discussed are fundamental in illustrating the data security measures that can be enforced to ensure that patients' data is protected.

In relation to the AI aspect, there is appreciation that patient data is of sensitive nature, hence recommendations here are around applying data protection laws around management of data to ensure patient rights are upheld.

Analysis

Definition of e-Health

In Kenya, the Health Act of 2017 defines e-health as the 'combined use of electronic communication and information technology in the health sector including telemedicine.'[14] The term is synonymous with digital health in Kenya.[15]

[11]Carlo N. De Cecco, Marly van Assen and Tim Leiner (eds), Artificial Intelligence in Cardiothoracic Imaging (Springer 2022)
[12]Naipeng Dong, Hugo Jonker and Jun Pang, Challenges in eHealth: From Enabling to Enforcing Privacy < https://satoss.uni.lu/members/jun/papers/FHIES11.pdf > accessed 21 November 2022
[13]ibid
[14]Health Act 2017 (No 21 of 2017), Sec 2
[15]International Comparative Legal Guides, Digital Health 2020 ; A practical cross- border insight into digital health law 1st Edition<https://tripleoklaw.com/wp-content/uploads/2021/01/DIGH20_Chapter-18_Kenya.pdf > accessed 2nd August 2022

Emerging technologies in e-Health

Some of the emerging technologies in this area of health include:

- **Telehealth** - This entails the 'use of telecommunications and virtual technology to deliver healthcare outside of traditional healthcare facilities.'[16]
- **Telemedicine** - This involves the 'remote delivery of healthcare services over telecommunication infrastructure for instance through video conferencing.'[17] The Kenyan government launched an initiative in May 2015 that deals with telemedicine targeted towards the poor and marginalized to help in tackling non-communicable diseases.[18]
- **Mobile health (mHealth)** - This entails the delivery of medical services through the use of mobile technologies.
- **Integrated Hospital Management Information System (HMIS)** - This is 'an element of health informatics that focuses mainly on the administrational needs of hospitals.'[19]

Regulations Applicable to e-Health in Kenya

The applicable laws in healthcare and specifically e-health in Kenya include:

i. **The Constitution of Kenya**- It provides that 'every person has the right to the highest attainable standard of health, which includes the right to healthcare services…'[20]The right of privacy is also

[16]ibid
[17]ibid
[18]ibid
[19]ibid
[20]Constitution of Kenya 2010, Article 43 (1) (a)

fundamental especially when it comes to information concerning private affairs or communication. The Constitution provides that 'every person has the right to privacy which includes the right not to have information relating to their family or private affairs unnecessary required or revealed or privacy of their communications infringed.'[21]

ii. **The Health Act, 2017**- The purpose of the legislation is to regulate health products and health technologies. Section 1 of the Act defines what e-health entails. The Act recognises e-Health as a mode of health service according to section 103. The Act recognises the need for an e-legislation as section 104 lays down the need for legislation that provides for, 'administration of health information banks including interoperability framework, data interchange and security, collection and use of personal health information, management of disclosure of personal health information, protection of privacy, health service delivery through m-Health, E-learning and telemedicine..'[22] Section 105 of the Act mandates the Ministry of health to facilitate the establishment of a comprehensive integrated health information system.

iii. **Access to Information Act 2016**- The Act gives effect to Article 35(1) of the Constitution which provides that, 'every citizen has the right of access to:

a. information held by the State; and
b. information held by another person and required for the exercise or protection of any right or fundamental freedom.

This provision guarantees the right of access to medical records and also information shared on the e-health platforms.

iii. **Data Protection Act** – The Act contains important provisions that govern the processing of personal data and the rights of data subjects. The data controller or processor is required to observe certain requirements and uphold the principles of data protection enshrined in the legislation. Section 25-43 consists of the principles and obligations of personal data protection. E-health platforms that collect personal data are required to adhere to the obligations imposed on them as provided for in the Act. Section 46 (1) of the Act deals with personal data relating to health and provides that personal data relating to the health of a data subject may only be processed: (a) by or under the responsibility of a health care provider or (b) by a person subject to the obligation of professional secrecy under any law.'

iv. **Kenya National eHealth Policy 2016-2030**- The policy describes the status of eHealth in Kenya and this includes the legal and ethical requirements in place. Some of the standards and guidelines in place include the eHealth Strategic Plan (2011-2017), ICT Policy (2006), Kenya Communications Act (2012) and the standards and guidelines for the Electronic Medical Records (EMR) 2010. The policy also describes some of the eHealth challenges that hinder the implementation of eHealth systems in Kenya. Some of the policy priorities

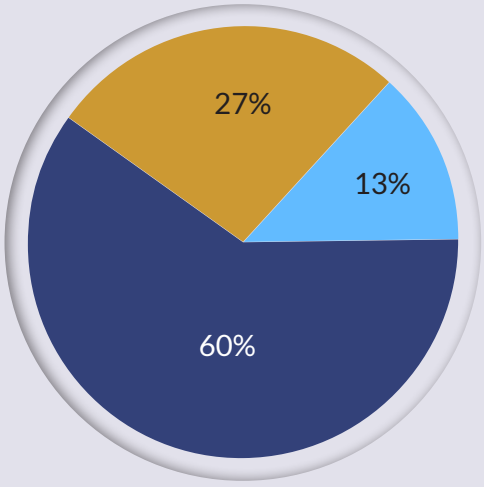
[21]ibid..Article 31 (c) and (d)
[22]Health Act (n13) , Section 104

include the sharing of health information and the interventions that the Ministry of Health shall take to secure the sharing of patients' health records and this includes supporting the creation and enforcement of legislations. Another priority of the policy deals with securing the transfer of health information and the intervention that the Ministry of Health shall implement. The policy also discusses the interventions that shall be implemented by the government to secure the privacy, confidentiality and integrity of patient health information.

Ehealth Platforms Assessment

Assessing the Kenyan eHealth AI landscape, there are 15 active AI system eHealth platforms. They range from; mHealth, telemedicine and health information systems. These eHealth platforms are as listed below:

- Totohealth
- Antarahealth
- Keheala
- SIHA AI app
- Ilara Health
- Healthy Moms
- Asknivi
- AskDoki
- Sophiebot
- AfyaPap
- Afya Rekod
- Access Afya
- Health E Net
- Kenyan covid chatbox
- Zuri Health



`Figure 1: The image above details the number of Kenyan AI eHealth Platforms. The total number 15; 9 are mHealth platforms, 2 are Telemedicine, and 4 are Health Information Systems.

We can further categorise these platforms them by functionality:

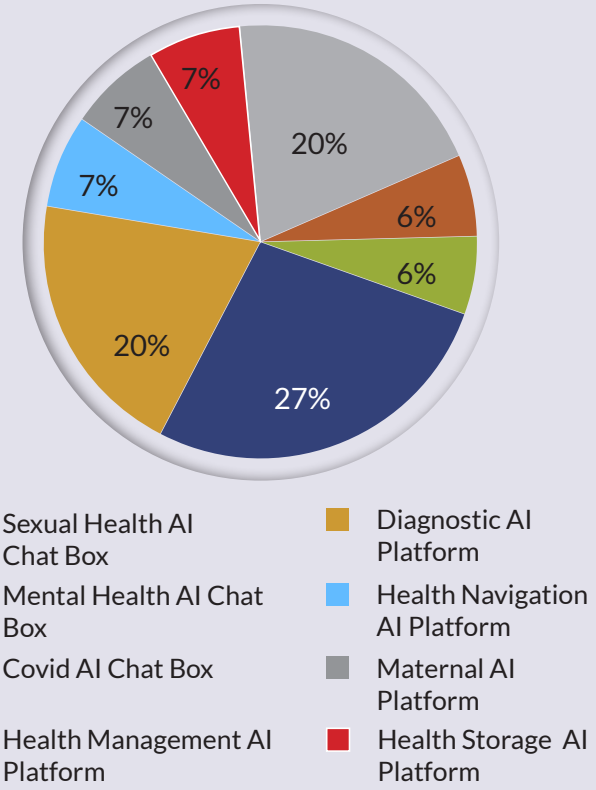


Figure 2: The image above groups the estimated 15 AI eHealth Kenyan Platforms based on their functionality.

We assessed the presence of privacy policy/ commitments:

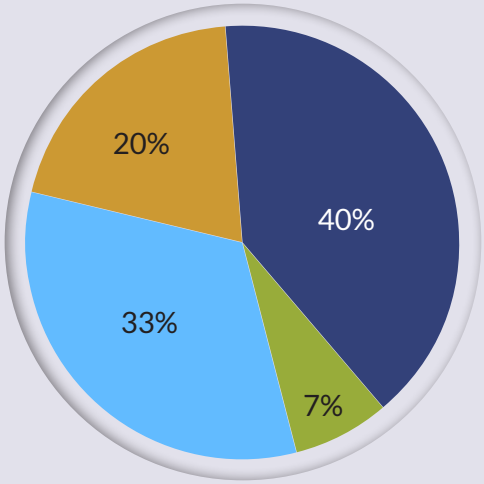


Figure 3: The image above comprises the assessment of the Kenyan AI eHealth platforms and the privacy initiatives present within the platforms.

The privacy measures employed by these platforms to protect the data of its users can be analysed by looking mainly at the privacy policy and the website of these specific platforms. Upon assessment, out of the 15 ehealth platforms, we have identified that only 5 platforms have privacy policies and privacy commitments

An analysis of these e-Health platforms was done and the platforms which were identified as having an existing website and privacy policy or commitment include:

a. Keheala
b. Ilara Health
c. AfyaRekod
d. Access Afya
e. Zuri Health

E-Health Platform	Type of AI Health tool
1. Access Afya Kenya	Diagnostic
2. Afya Rekod	Disease management & Diagnostic
3. Ilara Health	Diagnostic
4. Keheala	Disease management
5. Zuri Health	Diagnostic

Table 1: E-Health platforms picked for assessment and their functionality type

The methodology and assessment of determining whether privacy of a patient's data is adequately provided by the e-health platforms entails analysing the privacy policies to find out if they adhere to principles of data protection provided in section 25 of the Data Protection Act. Data processors are supposed to make sure that the personal data collected is processed according to the data protection principles provided in the Act. The assessment criteria will also involve analysing whether data subjects are accorded their rights as provided for in section 26 and 32 of the Act.

Privacy Score Assessment for the E-Health platforms

The assessment criteria assist the user with a means of measuring the level of privacy and trust the eHealth platforms have to offer.

Therefore, the assessment criteria for the privacy of the e-health platforms involve checking whether the following parameters are fulfilled:

I. Compliance with privacy best practices by

having an accessible and noticeable privacy policy.

II. Duty to notify as provided in section 29 of the Data Protection Act (DPA)

III. Mention of third parties with whom personal data is shared.

IV. The implementation of data security measures by the various eHealth platforms to protect personal data from being misused or tampered with.

A score of 1 is awarded to each parameter that is fulfilled. A score of 1 is equivalent to 20 % where the compliance assessment is for all the eHealth platforms. When it comes to individual assessment of the eHealth platform, a score of 1 which is equivalent to 25% is awarded to each parameter fulfilled. The fulfilment of each parameter awards the eHealth platform(s) with a total percentage score of 100%. The parameters used for assessment are described in detail below:

i. Compliance with privacy best practices (An accessible and noticeable privacy policy)

In order to obtain a score under this parameter, the eHealth platform must have a noticeable and comprehensive privacy policy that showcases how the personal data they share is handled. The policy should be drafted in a manner that is easily understood by the average individual. Thus, factors such as legal jargon and length of the policy are assessed against the reasonable perception of the average individual.

ii. Duty to Notify

In order to earn a score in this category, the eHealth platform should fulfill the provisions of section 29 of the Data Protection Act. In order to fulfill this provision, the eHealth platform should inform the data subject of at least the following:

a. The right of the data subject as provided in section 26 of the Data Protection Act.
b. The purpose for collection of personal data
c. The fact that personal data is being collected
d. The contacts of the data controller or data processor.
e. The data storage duration as provided in section 25 (g) of Data Protection Act.

iii. Mention of third parties with whom personal data is shared with

In order to earn a score under this category, the eHealth platform must inform the data subject of the third parties that personal data will be transferred to as provided in section 29 (d) of the Data Protection Act and the eHealth platform should also comply with section 72 (3) (b) of the Data Protection Act which prohibits unlawful disclosure of personal data to third parties. Some eHealth platforms may not disclose the parties that they may share personal data with and this may cause the personal data to be vulnerable to data breach thereby infringing on the rights of a data subject. This may also lead to loss of trust between the data subjects and the data processors who in this case are the eHealth platforms that collect and process personal data.

iv. Practice Robust Security

To earn a score under this category, the identified eHealth platform should describe the data security measures implemented to protect personal data as provided in section 29 (f) of the DPA. The data processor should take all steps to ensure that personal data is protected from unauthorised access, misuse, erasure or destruction of personal data. Data security measures assure data subjects using the platforms that appropriate measures have been implemented to ensure the security of personal data.

E-Health Platforms

The AI eHealth platforms website assessed below contain a website and privacy policy or website and privacy commitment. These platforms were:

1. Access Afya
2. Ilara Health
3. Afya Rekod
4. Keheala
5. Zuri Health

The table below gives an overall performance score across each indicator by all the eHealth platforms. It also shows how each eHealth platform performed individually in all the parameters and finally, it shows an average percentage score of the total performance. The data collection and analysis of the platforms identified was conducted from October 3,2022 to November 4, 2022.

	Parameters	Access Afya	Ilara Health	Afya Rekod	Keheala	Zuri Health	Total Score	Percentage Score
1.	Complies with privacy best practices (An Accessible and Noticeable Privacy Policy)	1	1	0	1	1	4	80%
2.	Duty to notify(Rights of data subjects)	1	0	0	0	1	2	40%
3.	Mentions third parties with whom personal data is shared with	1	0	0	1	1	3	60%
4.	Practice Robust Data Security	1	1	0	1	1	4	80%
	Total Score	4	2	0	3	4	-	**Average Score- 65%**
	% Score	**100**	**50**	**0**	**75**	**100**	-	**Average Score-65%**

Table 2: Performance score of the eHealth Platforms.

Summary of the findings

	Parameters	E-health platforms general performance
1.	Existence of an accessible and noticeable privacy policy	Out of the 5 eHealth platforms analysed, only one did not obtain a score. The overall performance is therefore good.
2.	Duty to Notify	Only 2 of the eHealth platforms complied with this requirement each earning a score. 3 of them did not comply with the requirement and therefore the overall performance is below average
3.	Mentions third parties with whom personal data is shared with	3 out of the 5 eHealth platforms complied with this provision therefore each earning a score for compliance. Only 2 of them did not have this provision and the performance is therefore average.
4.	Practise Robust Data Security	4 of the eHealth platforms indicated data security measures they have implemented in ensuring personal data is protected therefore earning a score. Only one eHealth platform did not earn a score under this category. The overall performance is therefore good.

Table 3: Summary of the overall privacy compliance assessment.

Overall Percentage Score

The overall average percentage score of all the eHealth platforms as indicated in Table 1 is 65%. The highest performing compliance score is in the existence of a privacy policy which is found in almost all eHealth platforms. The second-best performance is in the existence of data security measures to be employed where 4 out of 5 eHealth platforms have mentioned the data security measures to be used to protect personal data.

Overall Compliance of the eHealth platforms

An Accessible and noticeable privacy policy

Practice Robust Data Security

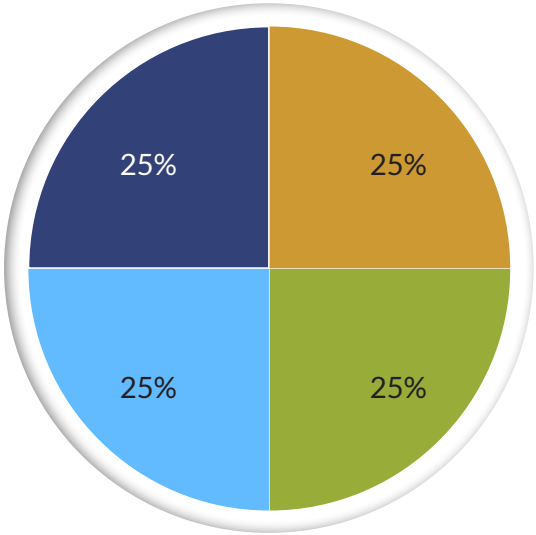
Mentions third parties with whom data is shared with

Duty to notify

Average performance

Analysis of the Score

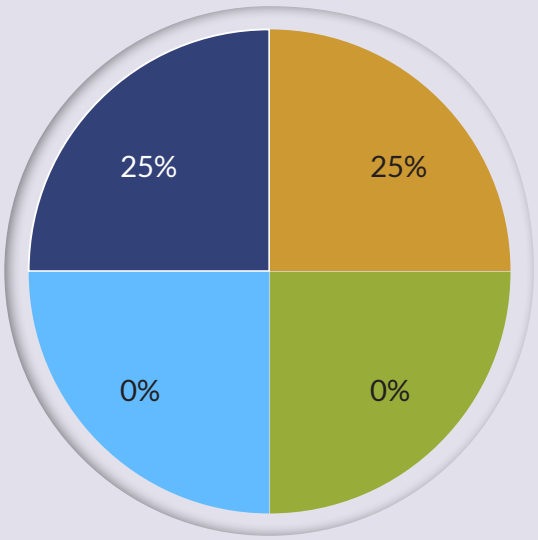
Assessment



- Practice Robust Data Security
- An Accessible and noticeable privacy policy
- Mentions third parties with whom data is shared with
- Duty to notify

1. Access Afya

Access Afya is held to have a comprehensive and noticeable policy. The policy is simplistic in nature allowing individuals to appreciate; their exclusive right to be aware and comprehend how sensitive data is utilised and stored. The policy incorporates transparency as it expounds on scenarios in where third parties would engage with the personal information shared. Assessing the measures on data security, the information is relatively vague, as there is just mention of protecting personal information through a system of organisational and technical security measures.



An Accessible and noticeable privacy policy

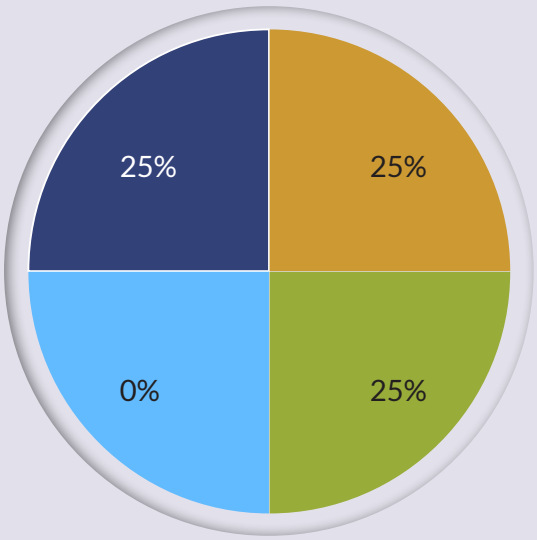
Duty to Notify

Mentions third parties with whom data is shared with

Practice Robust Data Security

2. **Ilara Health**

Ilara does have a policy, however the structure of the policy limits the average individual from fully engaging with the policy. There is currently no duty to notify, within the policy, however in relation to third parties and sharing of information there is mention of how data is stored and utilized. There is a clear stand on not storing and processing information that is collected by a third party, without the presence of consent. The policy looks towards providing caution as to the possibility of personal information being an asset transferred to or acquired by a third party in scenarios that involve a change of ownership. Assessing data security, there is clarity as to the measures the platform takes to safeguard the data of its patients. There is mention of stringent safeguards that touch on administrative, physical and technical barriers that form a protective firewall around the information stored.



An Accessible and noticeable privacy policy

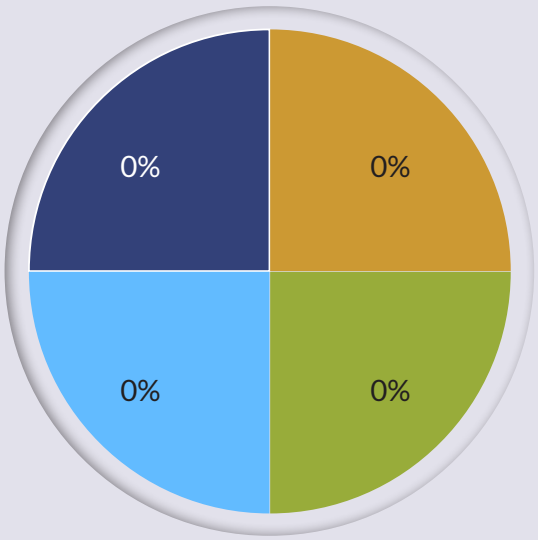
Duty to Notify

Mentions third parties with whom data is shared with

Practice Robust Data Security

3. **Keheala**

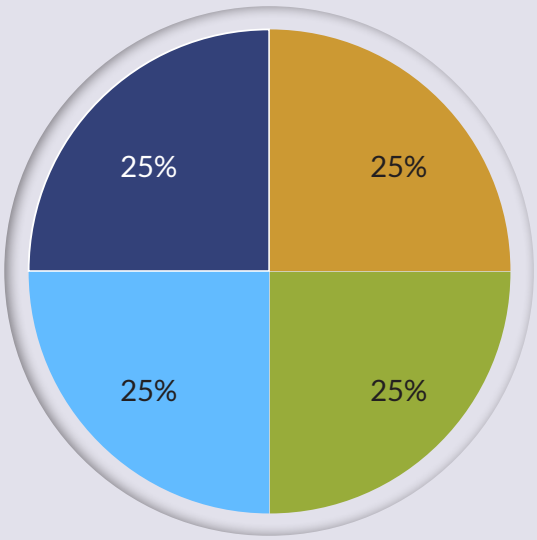
The privacy policy is comprehensive, where there is clarity on various ways in which Keheala collects, stores and utilises personal data. The policy is structured and simple in nature, as the average individual can comprehend and apply their privacy rights. The policy also expounds on various definitions of terms used making it easier for the consumer to understand. In relation to duty to notify, the policy has an exhaustive list of scenarios of when to notify the patient. There is no mention of third parties. This limits the policy of achieving a perfect score, as there is need to mention how they interact with third parties and utilize their personal data. In relation to data security, there is mention of the measures they have undertaken to secure personal information; however, the description is vague as they do not expound as to what those measures amount to.



- An Accessible and noticeable privacy policy
- Duty to Notify
- Mentions third parties with whom data is shared with
- Practice Robust Data Security

4. AfyaRekod

There is no privacy policy in place, as information pertaining to the privacy of the patients is found within the frequently asked questions (FAQS). The FAQS vaguely deal with how information is stored and whether it is secure. In general, there is lack of compliance with the Data Protection Act.



- An Accessible and noticeable privacy policy
- Duty to Notify
- Mentions third parties with whom data is shared with
- Practice Robust Data Security

5. Zuri Health

The privacy policy in place is extensive, where all the necessary factors are present and explained thoroughly. The structure of the policy is coherent and simplistic, allowing the average patient to understand and apply their rights. In addition, the policy expounds on the privacy rights and choices of the patients which is not seen in other platforms, we have assessed.

Recommendations

General recommendations from the privacy policies assessment

The analysis of the identified eHealth platforms indicates the general performance in terms of compliance with the privacy policy parameters that should be included. However, from our findings, e-health platforms are still lagging in terms of data protection requirements that are crucial in order to ensure that the privacy of data subjects is guaranteed. To address this, below are some of the recommendations that can be implemented in the privacy policies:

1. All e-health platforms need to have a comprehensive and noticeable privacy policy considering the sensitivity of health data. This is because the existence of a privacy policy builds trust between the data subject and the data processors of the e-health platforms. Having a privacy policy also illustrates that the e-health platforms are adhering to privacy laws.

2. The e-health platforms should incorporate the applicable data protection laws of the country they operate in. This ensures that the data protection and privacy requirements of the country they operate in are adhered to and that a data subject can institute an action against a data processor where there has been a breach of fundamental rights and principles. Some of the e-health platforms analysed adhere to foreign data protection laws for instance Afya Rekod and Zuri Health and are therefore not compliant with the Kenya Data Protection Act.

3. The privacy policies should have an elaborate description of the data security measures put in place which should also include the exact technology used. They should also assure data subjects of adequate cybersecurity measures put in place to prevent the circumvention of privacy settings or security measures. Having this in place illustrates that the e-health platform is committed towards protecting personal data which might be sensitive. This also assures the data subject that stringent security measures have been put in place to safeguard personal data.

4. The various eHealth platforms should include all the rights of the data subjects in the privacy policy without limiting when they can be exercised. The importance of this is that it ensures that a data subject has full control over his or her personal data and can also seek legal recourse where there has been a breach of the rights by the data processor.

5. The legal basis for processing personal data should be indicated in the privacy policy. This is because it is a requirement especially by the Data Protection Act 2019 and it enables the data subject to know instances when processing of personal data is necessary.

6. The privacy policies of the various e-health platforms should clearly indicate the data storage duration and where the data needs to be retained for a reasonable period, the privacy policy should state clearly what the reasonable period entails.

7. Third parties with access to the personal data should be clearly stated so as to ensure accountability of the information shared and protect misuse of personal data by people with access to it.

8. The privacy policy should adopt a user-oriented approach where the design of the privacy policy should be user friendly. This would assist with making it easier for users to

identify and understand their privacy rights.

Proposed Legal Reforms

The e-health bill is an important legislation which needs to be enacted into law. The purpose of the e-health bill is to 'provide a framework for implementation of section 104 of the Health Act 2017, the provision of telemedicine services and the establishment and management of e-health infrastructure…'[23] The bill provides that the Cabinet Secretary shall prescribe privacy and security standards which are important when implementing e-health systems.[24] The bill also lists the information rights of recipients of health care services. Some of these rights which are fundamental to the protection of privacy include access to electronic health records and access to their personal health records and also management.[25] The bill also gives provisions on how e-health information should be handled which is covered in part IV of the bill. The increased use of e-health platforms now demand legislation that will address issues concerning e-health. The bill is now overdue since it was supposed to be enacted into law three years[26] after the Health Act came into operation.

Due to the nature and sensitivity of health data, privacy policies need to be simple and understandable to data subjects. To ensure compliance by e-health platforms of this requirement, the Data Protection Act should include a provision that deals with the structure of privacy policies. An example of this is the Nigeria Data Protection Regulation 2019 which provides in part 2.5 that 'any medium through which personal data is collected or processed shall display a simple and conspicuous privacy policy…'The inclusion of this in the Data Protection Act will not only ensure compliance by e-health platforms but also other online platforms that process personal data.

The analysis of the privacy policies indicate that the data security measures described are vague and lack depth as to how the security measures will be enforced. To address this, the Data Protection Act should borrow a leaf from the General Data Protection Regulation (GDPR) and expound on the security measures that data processors can implement to protect personal data. The GDPR enumerates the technical and organisational measures that can be implemented and they include: the pseudonymisation and encryption of personal data,[27] ability to ensure 'ongoing confidentiality, integrity, availability and resilience of processing systems and services,'[28] ability to access personal data in a timely manner in cases of a physical or technical incident[29] and regularly assessing and evaluating the technical and organisational measures.[30]

The analysis of the e-health platforms shows that the performance in the duty to notify and third party sharing of personal data parameters was not good. These provisions are incorporated in the Data Protection Act. However, in order to ensure compliance by e-health platforms, the e-health bill should incorporate detailed provisions of the two provisions before it is enacted into law. The inclusion of these provisions will also be fundamental in protecting health data which is sensitive.

Considering that health data may be extremely sensitive, e-health laws and the Data Protection Act in Kenya should incorporate detailed provisions

[23]The County E-health Bill, *2021* ,*Preamble*
[24]ibid Section 20 (b)
[25]ibid Section 17(1) (b) and (c)
[26]The Health Act 2017(n24) Section 104
[27]General Data Protection Regulation, Article 32(1) (a)
[28]ibid Article 32 (1) (b)
[29] ibid Article 32 (1) (c)
[30]ibid Article 32 (1) (d)

on anonymisation[31] and de-identification of personal data. The Data Protection Act defines what anonymisation is but does not expound what it entails and how it should be enforced. It is crucial to use anonymisation and de-identification mechanisms so as to ensure that the privacy of data subjects is not breached. De-identification is elucidated well in the Victorian Privacy and Data Protection Act 2014 and according to it, de-identification of personal data occurs when that data 'no longer relates to an identifiable individual or an individual who can reasonably be identified.'[32] The same Act also states that organizations should take 'reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.'[33] Anonymisation is also a 'subcategory of de identification.'[34] The incorporation of these provisions will ensure compliance by data controllers and enhanced protection of personal data.

In addition to the privacy policies, the bill should look towards incorporating normative principles that have been developed by various international organizations to AI eHealth applications. This would assist with regulating Artificial Intelligence and its technologies in a manner that provides transparency, security and accountability to ensure there is ethical application of AI. Key illustrations include; The OECD five principles on AI, the applicable principles would be ensuring 'AI systems function in a robust and safe way throughout their life cycles' and ensuring that 'organizations and individuals that develop, deploy and operate AI systems should be held accountable for their proper functioning'

Conclusion

The rise of eHealth platforms in Kenya play a key role in facilitating the achievement of the Universal Healthcare agenda. However, although these developments improve the lives of people, the AI and privacy concerns of these platforms cannot be neglected. This study has managed to analyse existing eHealth platforms in Kenya and also the privacy concerns in the identified platforms. With rapid advancements in technology and AI innovations, data collectors and data processors should implement the appropriate safeguards to secure the data belonging to data subjects from misuse or unauthorised access. Data subjects on the other hand should also assess the data security safeguards and legal compliance of the platforms they use before they share their data. Although Kenya already has existing laws that are applicable to e-health, legislators should enact any pending e-health bills to law to ensure that users of e-health platforms are adequately protected. Finally, the recommendations made in this study will be pivotal in improving the e-health landscape in Kenya.

This study has managed to analyse existing eHealth platforms in Kenya and also the privacy concerns in the identified platforms.

[31]Data Protection Act 2019, section 2 ; provides that anonymisation is the 'removal of personal identifiers from personal data so that the data subject is no longer identifiable.'
[32]Privacy and Data Protection Act 2014, Section 3
[33] ibid Principle 4(4.2) of schedule 1
[34]BCLP Law, At a glance: *Deidentification, anonymization and pseudonymization* (28 February 2016) <https://www.bclplaw.com/en-GB/insights/at-a-glance-de-identification-anonymization-and-pseudonymization.html#:~:text=Key%20Definition%3A%20%E2%80%9CAnonymization%E2%80%9D%20of,code%2C%20algorithm%2C%20or%20pseudonym. > accessed 18 November 2022

APPENDIX

Appendix 1

Privacy Policy Assessment Matrix

The Data Protection Act 2019 governs the processing of personal data, including the name, postal address, e-mail address, telephone number, and other personal details of a data subject. As a result, e-health platforms are required to inform the public of the nature, scope, and purpose of the personal data they collect, use, and process, and to inform data subjects of their rights. In compliance with the Data Protection Act, the assessment matrix below evaluates the components of the privacy policies of the selected e-health platforms.

	Component of the privacy policy	Yes/No
1.	Is there an effective date?	
2.	Does the privacy policy mention that personal data is being collected?	
3.	Does the privacy policy explain why the data is collected?	
4.	Does the privacy policy mention the applicable law?	
5.	Does it mention how you, as the data subject, can withdraw consent at any time?	
6.	Can you access and correct your information?	
7.	Can you request the deletion of your personal information?	
8.	Can you restrict or object to the processing of your personal information?	
9.	Does the privacy policy specify how long the data is retained?	
10.	Does the privacy policy mention data sharing with third parties?	
11.	Does the privacy policy mention that personal data will be anonymised?	
12.	Does the privacy policy mention in detail the data security measures it will implement?	
13.	Does the entity's contact information appear in the privacy policy?	
14.	Does the privacy policy state whether you will be notified if there are any changes to it?	
15.	Is the privacy policy in simple, understandable language?	

This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organization for their continued support.

Canada

Centre for Intellectual Property and Information Technology