DEVELOPING DATA PROTECTION GUIDELINES FOR THE HEALTH SECTOR IN KENYA

Florence A. Ogonjo
Rachel Achieng Odhiambo
Margaret Zalo

Strathmore University
Centre for Intellectual Property and Information Technology Law

Executive Summary

Kenya adopted the Data Protection Act (DPA) in 2019, fortifying individuals' right to privacy and strengthening protection of their personal data. This was, in part, a result of numerous sectors adopting the use of technology in their day to day functioning, among them the health sector. The Data Protection Act introduced new standards for processing of personal data for which health data is a special category, sensitive personal data. It is essential that sector specific guidelines are developed to guide the processing of health data to ensure compliance with the mandates set forth in the DPA.

Introduction

The Kenyan health sector is embracing the use of technology, e–Health, to improve healthcare services and the quality of care. This transition is characterized by the introduction of technologies such as Health Information Systems (HIS), mHealth,[1] and telemedicine to provide health services. Owing to the digitization of health records, mHealth and HIS services have significantly increased the amount of health data they process. It is, therefore, critical to understand how data is managed and protected (in addition to the already existing norms of confidentiality) in these processing activities in the health sector in order to ensure patients' right to privacy are protected.

The Health Act, enacted in 2017, gives powers to the Cabinet Secretary for the Ministry of Health to establish and maintain a comprehensive integrated Health Information System. Further, the Cabinet Secretary is obligated to develop legislation within three years of the Act providing provisions for the protection, management, collection, use, and disclosure of personal health data. The Health Act introduced and recognized eHealth as a form of health service. The increase in the development and adoption of eHealth, mHealth and telemedicine platforms, and emerging technologies such as Artificial Intelligence (AI) to detect, predict and diagnose disease has made health data a commodity. It is in this environment that we analyze the policy structures relating to health data in light of the DPA. It is necessary to understand the legislative gaps that currently exist in health acts and policies enacted prior to the DPA to enable the development of data protection guidelines, specific to the health sector, that ensure compliance with the act.

[1] *The Kenya Standards and Guidelines on mhealth Systems describes mobile health (mhealth) as the use of portable devices such as cellphones to provide health services and information and or, interventions and programs designed to support health service provision through mobile technology and devices.*

Approach

To fully assess which health-specific data protection guidelines are needed, we examined the existing laws and policies that relate to the processing of health data. The assessment identified the areas in the laws and policies that comply with the provisions in the Data Protection Act and areas where there are gaps. The laws and policies analyzed included:

i. The Health Act, 2017.
ii. Health Sector ICT Standards and Guidelines for mHealth Systems.
iii. Standards and Guidelines for Electronic Medical Record Systems in Kenya
iv. Kenya National eHealth Policy 2016-2030.
v. Health Information Systems Policy 2014-2030.
vi. HIV/AIDS Prevention and Control Act.
vii. Standard Operating Procedures in Handling Health Records and Information Management During the COVID-19 Pandemic.

Key Findings

- The Data Protection Act introduced principles that elevated the standard of health data processing. Primarily, the DPA defines health data as a special category of data and establishes data protection principles that must be applied when processing data. Health authorities are now required to ensure that personal data is used fairly, lawfully, and transparently, and only to the extent necessary to pursue health-related public interests, in accordance with the applicable data protection principles under the Data Protection Act.

- The health sector has enacted laws and policies that require and recognize data protection when health data is processed. While these identified laws and policies address distinct issues and acknowledge certain data protection principles, they are, in specific instances, inconsistent with the Data Protection Act. As a result, it is necessary to amend these laws and policies to ensure full compliance with the DPA. Specifically, the Health Act, Health Sector ICT Standards and Guidelines for mHealth Systems, Standards and Guidelines for Electronic Medical Record Systems in Kenya, Kenya's National eHealth Policy 2016-2030, Kenya's National eHealth Policy 2014-2030, and Kenya's Health Information Policy 2014-2030 must be amended.

Similarities and Policy Gaps

A comparative analysis of the DPS and existing health acts was done to identify how health data is perceived in the health sector's adoption of new technology and shed light on how, and the extent to which, data protection concerns are addressed during the development and implementation of new technologies for the processing of health data. The following similarities and differences have been identified between the Data Protection Act's provisions and the data protection principles embodied in existing health laws and policies:

Data Protection Act principles relating to health data	Health laws and policies relating to health data, specifically, to processing health data
Integrity and Confidentiality (security): the principle requires the processing of data in a manner that ensures the security of the personal data including protection against unlawful, unauthorized or accidental loss. This requires the implementation of appropriate technical and organization measures to ensure security of the data	With the exception of the Health Act, the laws and policies listed in the 'Approach' section fully capture the integrity and confidentiality principle outlined in the DPA, particularly in relation to data access. The Health Act, however, makes no reference to the security provision. It does recognize the right to privacy and provides that an individual has the right to be treated with dignity and respect and to have their privacy respected in accordance with the Constitution and the Act.
Purpose limitation: this refers to the collection and processing of data for specified, explicit and legitimate purposes with no further processing that is inconsistent with the original purpose for which the data was collected. For example, where health data is collected for the purpose of medical examination and treatment, it cannot be used for research purposes unless consent is obtained and the consent is properly communicated prior to the data collection.	The purpose limitation principle is present only in the Kenya Standards and Guidelines for mHealth Systems. All the other acts examined (listed in the Approach section) make no mention of it.
Data minimization: this refers to the collection of data that is adequate, relevant and necessary in relation to the purpose for which it is collected.	The data minimization principle is only found in the Kenya National eHealth policy. All the other laws and policies examined (listed in the Approach section) make no mention of it.

Data Protection Act principles relating to health data	Health laws and policies relating to health data, specifically, to processing health data
Consent: consent refers to manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject. Consent often forms the legal basis for the lawful collection and processing of personal data and in this context health data. The DPA gives provisions on the conditions for consent.	The principle of consent is addressed in the Health Act (Section 9), the Kenya Standards and Guidelines for mHealth Systems, and the Kenya National Patients' Rights Charter. The first chapter of the Patients' Right Charter discusses patient rights; among these rights, the right to confidentiality, the right to give informed consent to treatment, and the right to information while the second chapter discusses responsibilities, particularly the obligation to provide relevant, accurate information to health care providers.
Rights of a Data subject: in this context these are the rights of a patient exercisable with respect to the processing of their data. The Act provides for the rights of a data subject to include: the right to be informed on the use of their personal data; the right to access their personal data; the right to object processing of their personal data; the right to correct false or misleading data, and the right of deletion of false or misleading data.	This principle is present in the Kenya National Patients' Rights Charter and the Kenya National eHealth Policy. Patient rights are discussed in the Charter, including the right to confidentiality, the right to give informed consent to treatment, and the right to information. The Kenya National eHealth Policy discusses the importance of taking a patient-centered approach to managing and utilizing electronic data in a manner that ensures the confidentiality, integrity, and privacy of patients at all times. All the other acts examined (listed in the Approach section) make no mention of it.
Data Transfer: The Act provides for data transfer in the context of cross border data transfer – that is, the transfer of data outside the Kenyan jurisdiction. Data can only be transferred outside of Kenya in accordance with the provisions prescribed under Section 48 and the establishment of appropriate safeguards under Section 49	This is part of the Kenya National eHealth Policy's goal of increasing access to electronic health services. Among the interventions that must be implemented to ensure electronic health service accessibility are the promotion of cross-border sharing of health information without compromising patient privacy. All the other acts examined (listed in the Approach section) do not address this principle.

In line with the observations made above the following gaps are noted:

Data protection principles:

Section 25 of the Data Protection Act sets out data protection principles which guide the lawful processing of personal data. These principles apply to the processing of health data and must be implemented across all existing laws and policies. While the principles of lawfulness, fairness, and transparency, accuracy, data minimization, purpose limitation, storage limitation, security, and accountability are included in a few policies, they are not adequately addressed when discussing health data processing in all of them. Security is mentioned in all laws and policies except the Health Act, purpose limitation is mentioned only in the Kenya Standards and Guidelines for mHealth Systems, data minimization is mentioned in the Kenya National eHealth Policy, and consent is mentioned in both the Kenya National Patients' Rights Charter and the Kenya Standards and Guidelines for mHealth Systems. Technological advancements affecting data processing, access to data, data retention, and overall data management create new challenges that, if not addressed adequately, could infringe on data subjects' rights, highlighting the importance of laws and policies that comply with the Data Protection Act.

Rights of the data subject:

the rights of the data subject are relevant to the processing of health data. For instance, the principle of accuracy requires that data collected is accurate and, where necessary, kept up to date and all reasonable steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. This principle is only enforceable where data subjects (patients) can exercise these rights. Among the highlighted laws and policies, only the Kenya National Patients' Rights Charter and the Kenya National eHealth Policy make reference to data subjects' rights. These rights must be provided for in all the policies that relate to the processing of health data.

Data transfer and sharing:

Health care involves a diverse set of public and private data collection systems. The existing laws and policies attempt to provide the necessary standards and guidelines for the processing of health data across these systems. The Kenya National eHealth Policy identifies data transfer as a goal for expanding access to electronic health services. It is notable, however, that the laws and policies fall short in adequately providing for data transfer not only across borders where the circumstances would merit but also across data collection systems, as might occur in the case of referrals.

Third party data- sharing:

Health data is not only relevant to health care professionals in carrying out their respective duties. This information can be shared with third party entities within the healthcare system for example, insurance companies and government agencies like NHIF. The laws and policies note in different contexts the duty of privacy and confidentiality for those who directly process health data but fail to give provisions and guidance where third parties are likely to be involved. This is not only necessary for data sharing with public or private insurance companies; it is especially relevant with the recognition of mHealth services and the use of eHealth systems.

Policy Recommendations

- The Cabinet Secretary for Health (MOH), the Office of the Data Protection Commissioner (ODPC), and the Medical Practitioner Board should collaborate to develop standardized data protection guidelines for the health sector. The guidelines should provide guidance on the implementation of the data protection principles in the health sector, consent, exercise of data subjects rights, responsibilities of healthcare institutions in data processing, the responsibilities of health care practitioners in the processing of data, data transfer, and data sharing.

- Revision of the identified policies in line with the identified gaps in the following manner:

I. **The Health Act** should include a provision addressing the integrity and confidentiality of data access (security). While it recognizes the right to privacy and states that an individual has the right to be treated with dignity and respect and to have their privacy respected in accordance with the Constitution and the Act, it should be revised to include this principle and to require the implementation of appropriate technical and organizational measures to ensure data security.

II. **The Standards and Guidelines for EMR Systems** should incorporate minimum implementation requirements that are consistent with the data protection principles in the Data Protection Act. These include: lawfulness, fairness, and transparency, accuracy, data minimization, purpose limitation, storage limitation, security, data retention, and accountability, as outlined in Section 25 of the Data Protection Act.

III. **Health Information Systems Policy 2014 - 2030:**

a. Revision of the policy to include an implementation strategy for the data protection principles especially with the continued application and use of ICT in data processing in light of the enactment of the data protection act.

b. Revision of the policy objectives to promote the processing of health data in a manner consistent with the provisions in the DPA and institute data protection guidelines that ensure compliance with the DPA.

c. Revision of the policy to adequately recognize the right to privacy of individuals in relation to their health information by recognizing the rights of data subjects, i.e., patients, in the processing of their data and providing for an implementation criterion on the exercise of the patients' rights as prescribed under the DPA.

d. Revision of the Health Information Systems Policy to reflect the data protection legislation noting the changes it will have on the processing of health data through the HIS. In line with this, defining the roles of health institutions as data processors, identifying data controllers and the need for trained and skilled data protection officers.

IV. **Kenya National eHealth Policy 2016-2030**:

a. Revision of the policy to recognize the DPA as one of the legislations regulating the use of eHealth in the collection, retrieval, processing, storage, use and disclosure of personal health information.

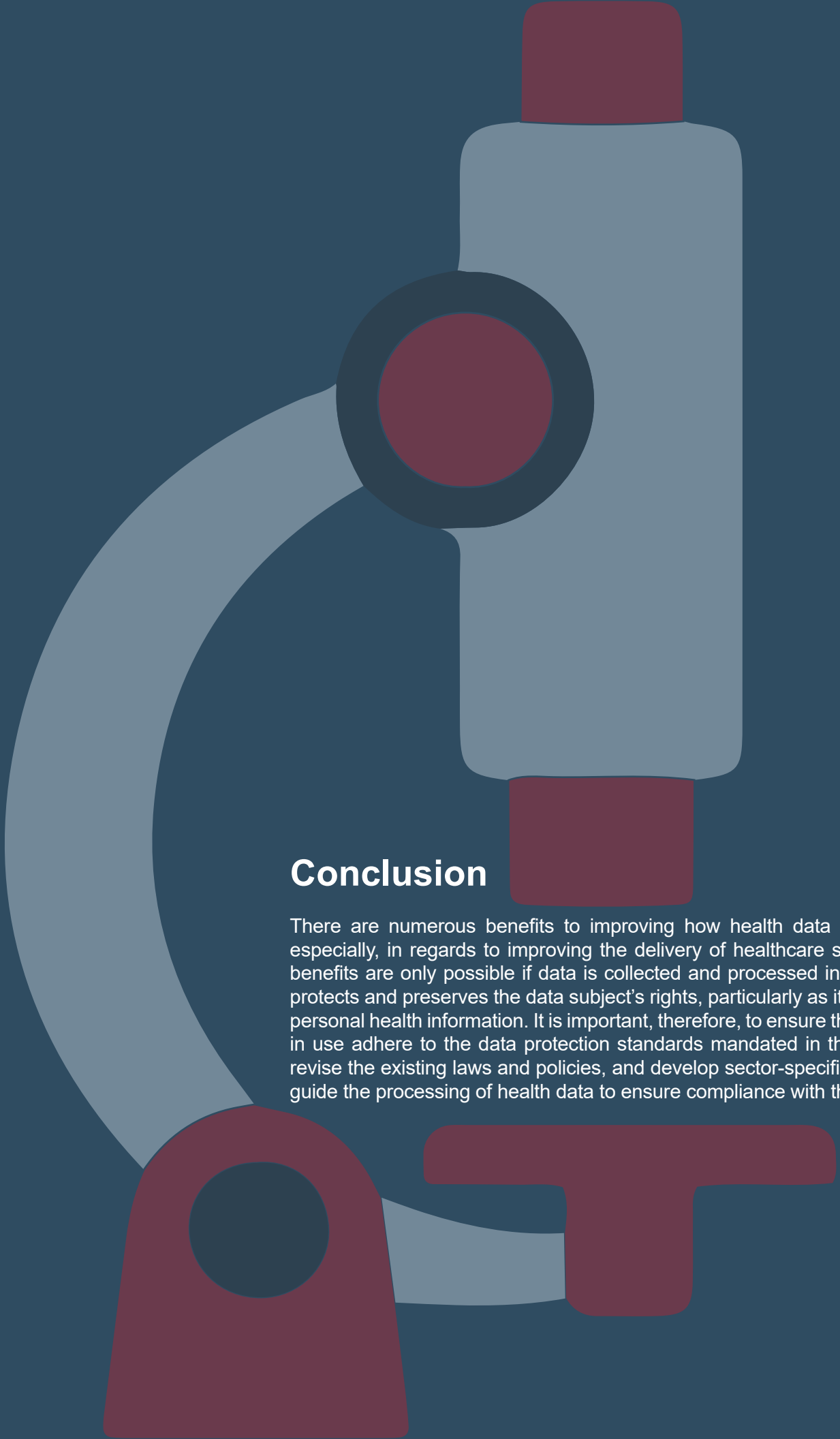
b. In addition to recognizing the right to privacy of patients, revision of the policy to include the importance of exercising patient rights while utilizing eHealth systems. These rights should be exercisable in line with the data subject's rights as prescribed in the DPA.

c. Revision of the policy to include guidance on third party data sharing when using eHealth systems. In addition, revision of the policy priority areas to ensure cross border data sharing of health information is in accordance with the provisions of the DPA. Guidelines on the same will be necessary in achieving proper implementation.

d. Revision of the policy to include a policy priority area on privacy by design and default. This will encourage due diligence in ensuring eHealth systems in use have the necessary technical safeguards and adhere to the prescribed data protection standards in the processing of health information.

V. **The Kenya Standards and Guidelines for mHealth Systems** specifies a criteria for judging the operation of mHealth systems ("non-functional requirements") as including security, interoperability, scalability, usability and data validation. For purposes of security, it identifies confidentiality, integrity and availability of mhealth systems to users as its crucial elements and enlists compliance requirements. Taking account of the data protection principles introduced in the DPA, the Standards and Guidelines for mHealth Systems should be revised to explicitly recognize the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, and storage limitation, along with crosscutting complementary measures to be adopted in processing data in mhealth systems and by which the performance of mhealth systems can be evaluated. Presently stated functional and non-functional requirements can be integrated with the data protection principles as some already align with them.

VI. **The HIV and AIDS Prevention and Control Act** permits the Minister for Health to formulate privacy guidelines for the processing of records relating to HIV; hinting at anonymity as one of the measures that can be adopted to ensure privacy. Given that this is yet to come to fruition, the Cabinet Secretary for Health should take the prescription of the Act up by formulating guidelines in conjunction with the Office of the Data Protection Commissioner and other relevant players to safeguard the privacy of HIV records in line with the DPA.



Conclusion

There are numerous benefits to improving how health data is processed - especially, in regards to improving the delivery of healthcare services. These benefits are only possible if data is collected and processed in a manner that protects and preserves the data subject's rights, particularly as it relates to their personal health information. It is important, therefore, to ensure that the systems in use adhere to the data protection standards mandated in the DPA, and to revise the existing laws and policies, and develop sector-specific guidelines, to guide the processing of health data to ensure compliance with the act.

This study was made possible by a grant provided by the Hewlett Foundation. We thank the organization for their continued support.