Data Protection in the Processing of Health Data through EMR Systems in Kenya

By Florence Ogonjo, Margaret Zalo, and Rachel Achieng Odhiambo

Policy Brief

Strathmore University
Centre for Intellectual Property and Information Technology Law

Executive Summary

Electronic Medical Record (EMR) systems are heavily integrated into the Kenyan health sector. EMR systems serve as data management tools in health facilities, storing patients' health data for the course of their treatment and beyond. The Standards and Guidelines on the Implementation of EMR Systems governs the development and implementation of EMR systems in Kenya. It was developed long before the enactment of the country's 2019 Data Protection Act (DPA) and there are significant deviations in the data protection provisions in the DPA and the Standards and Guidelines. Although confidentiality, security and privacy provisions are in the Standards and Guidelines, they largely pertain to the technical systems and do not reflect certain data protection safeguards and principles, such as data minimization and storage limitation, outlined in the DPA. The Standards and Guidelines on the Implementation of EMR Systems must be revised to match the letter and spirit of the DPA. This policy brief summarizes findings from our study on the subject and outlines policy recommendations.

Introduction

As healthcare facilities adopt the use of EMR systems to record, maintain and transfer patients' medical history, keeping this data secure from corruption, compromise or loss and in adherence with the patients' fundamental right to privacy and related regulations becomes critically important.

2010

The Standards and Guidelines on the Implementation of EMR Systems in Kenya was developed in 2010 to guide the development and implementation of EMR systems.

2019

Nine years later, the DPA was enacted. The sensitive nature of health data presupposes a degree of care in the manner in which it is processed. Consequently, health data is categorized as sensitive personal data and accorded special protection under Kenya's DPA. The DPA sets out data protection principles and other fundamental considerations such as data subjects' consent, rights of data subjects, and privacy by design and default.

Approach

A comparative analysis of the DPA and the Standards and Guidelines was done to identify deficiencies, if any, in the latter, in deference to the data protection provisions outlined in the former.

Key Findings

Overall, the analysis identified that:

the Standards and Guidelines fail to substantively incorporate certain data protection principles and provide for the implementation of the rights of data subjects.

the Standards and Guidelines do not fully meet the requirements on confidentiality, privacy and security mandated in the DPA; inadequacies that may be rectified by incorporation of specific data protection principles from the DPA.

The Comparative Analysis

Comparative analysis of the DPA and the Standards and Guidelines identified deficiencies in the Standards and Guidelines in the following principles: data minimization; lawfulness, fairness and transparency; storage limitation, and integrity and confidentiality.

- The principle of data minimization, requires the collection, processing and storage of data only to the extent to which the information is required.
- The principle of data minimization, requires the collection, processing and storage of data only to the extent
- The principle of storage limitation, meanwhile, requires that data is not stored for longer than is required and where timeframes are indefinite, necessary measures are taken to ensure that the data cannot be directly linked to individuals.
- The principle of integrity and confidentiality, on the other hand, requires that all necessary technical and organizational measures are taken to prevent the unlawful destruction, sharing and tampering of data.

The specific deficiencies in the Standards and Guidelines as relates to the above principles are as follows:

1. lack of protocols on reporting data breaches as and when they occur;
2. no guidelines or provisions for creating EMR systems that conform to privacy by design and default provisions;
3. lack of Data Protection Impact Assessment (DPIA) plans;
4. issues surrounding consent and rights of the data subject;
5. no protocols governing the appointment of Data Protection officers (DPO).

Detailed analysis of the findings is presented in the annexed table.

Policy Recommendations

The following policy recommendations are proposed to fully align the Standards and Guidelines with the DPA's data protection principles:

in regards to data minimization: establishment of specific categories of pre-coded data restricted in terms of use, access and reference.

in regards to lawfulness, fairness and transparency: establishment of robust protocols and guidelines as it directly relates to the ability of a patient to give informed consent in the processing of their data; sharing of patient data by health care professionals; future data extraction, and recording of consent decisions in EMR systems.

in regards to storage limitation: establishment of a set of guidelines that govern the retention of data; explicit reasons and timeframes should be outlined and protocols for the pseudonymisation of health data where data has to be stored for an indefinite period.

in regards to integrity and confidentiality: establishment of proper protocol for the notification and communication of a data breach, mitigation of the effects of data breaches, and the appointment of a Data Protection Officer (DPO).

establishment of guidelines through which data subjects can exercise their rights to information, access, rectification, erasure and data portability.

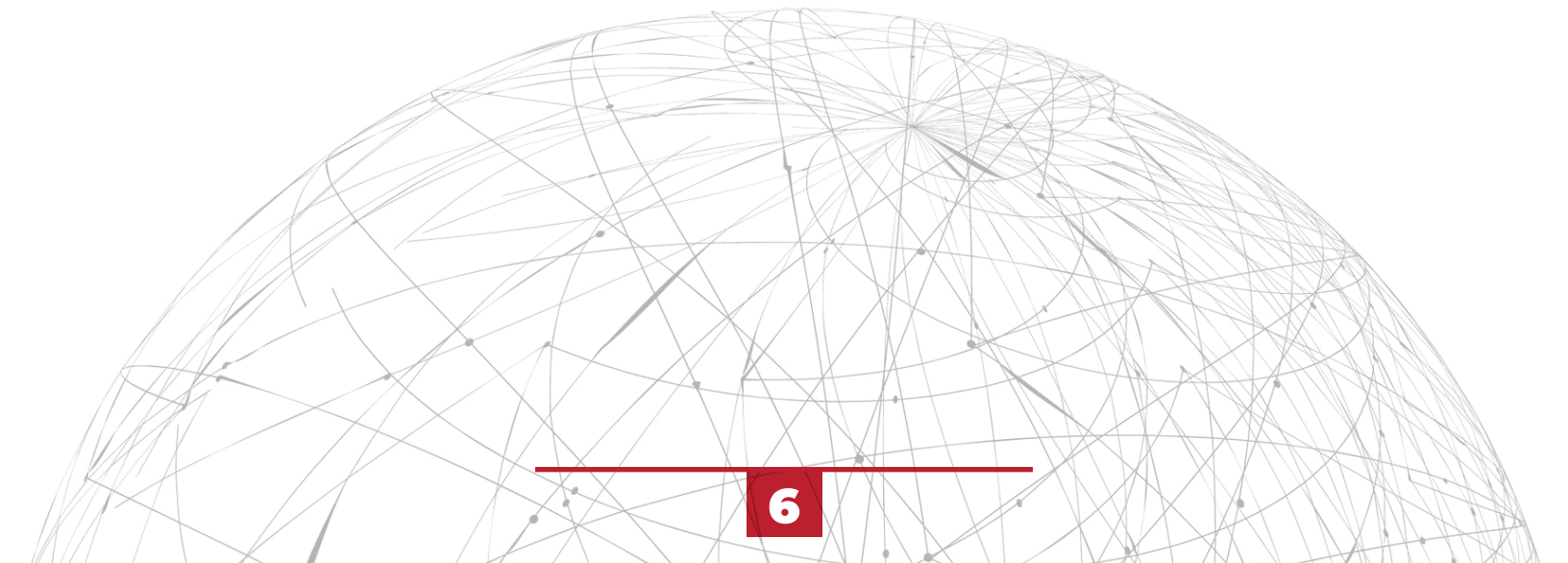
re-evaluation of EMR system implementation protocols to ensure that privacy by design and default is considered throughout the process by EMR system developers and program managers in EMR implementing agencies.

tablishment of mandatory Data Protection Impact Assessment (DPIA) plans to identify potential risks and provide relevant mitigation measures.

Conclusion

The Standards and Guidelines need to be revised to holistically reflect the DPA. Alignment of the Standards and Guidelines with relevant provisions under the DPA through revision or, the development of a new set of regulations will strengthen data protection in the functioning and use of EMR systems. Section 74 (1) of the DPA, which gives the Data Protection Commissioner mandate to develop sector-specific guidelines in consultation with relevant stakeholders in various areas including health, may be invoked for purposes of developing new regulations.

Successful harmonization of the regulations will only be achieved through the involvement of all relevant stakeholders particularly, the Office of the Data Protection Commissioner, the Ministry of Health and other stakeholders in the health sector.



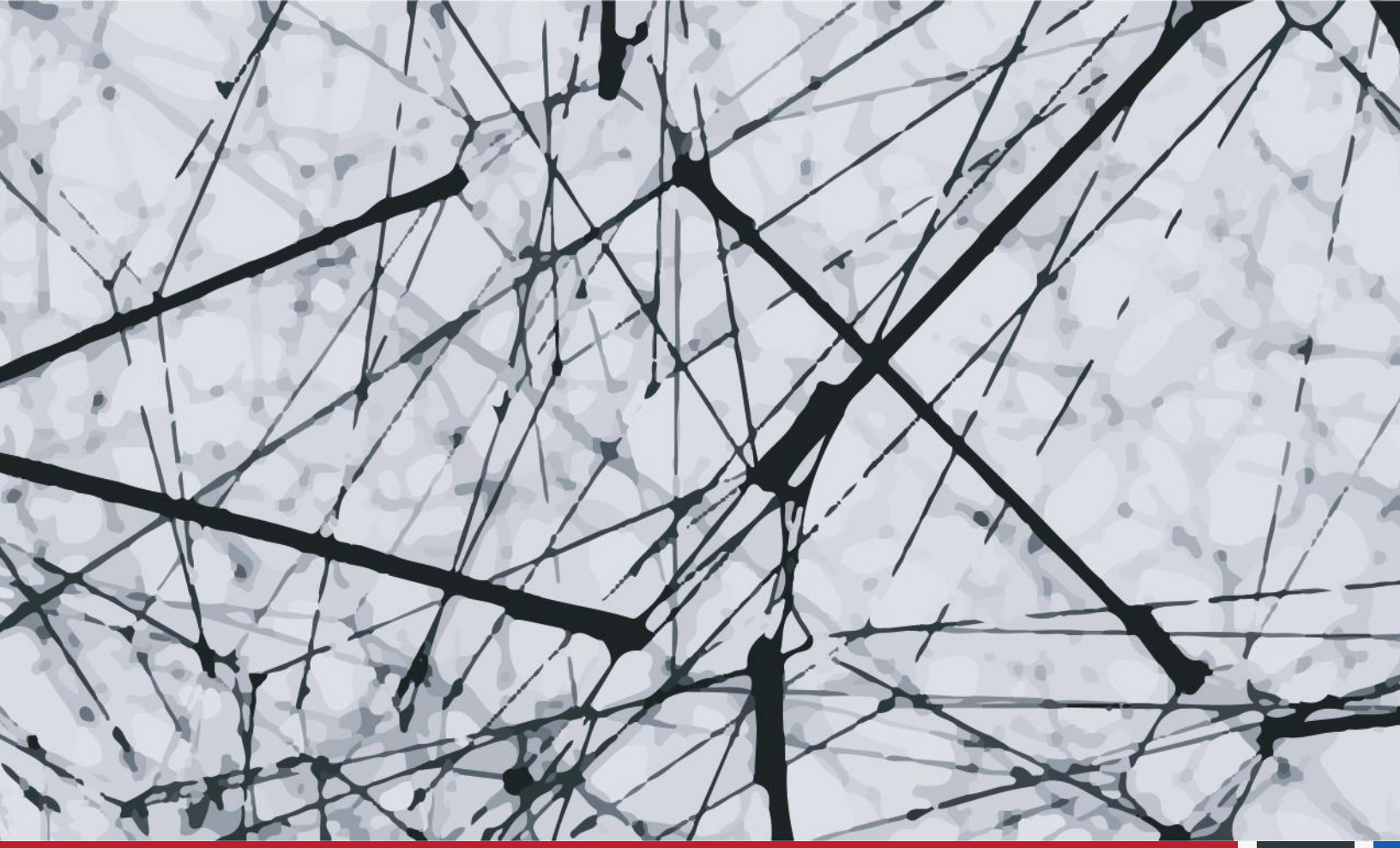
ANNEX 1: Comparative Analysis

Comparative Analysis of the Standards and Guidelines on the Implementation of EMR Systems and the 2019 Data Protection Act (DPA)

DPA Provision	Guidelines
Data minimization (Adequacy limitation) -This principle provides that the collection and processing of personal data should be relevant and not excessive of the purposes for which it is collected. This is highlighted in Section 25(d) of the DPA.	Mandate data minimization in input mechanisms - system must use pre-coded data and choice selection, where applicable, to minimize data input efforts. However, no specification(s) on the categories of pre-coded data is given which is vital in ensuring that the EMR systems only collect, process and store data that is relevant and required.
Lawfulness, fairness and transparency(Valid explanation) - Under section 25(e) of the DPA, data controllers and processors(health care institutions, health researchers) must provide a valid explanation for the purpose for processing, the existence and extent of access to the data by both the data subjects(patients) and data controllers and processors.	No specific guidelines on the principle of valid explanation are outlined.
Storage limitation - This principle requires that data should be stored for no longer than is necessary as provided for in Section 25(g) of the DPA.	No provisions for the retention of health data are outlined.
Security (integrity and confidentiality) - This principle requires processing of data in a manner that ensures appropriate technical and organizational safeguards are in place to protect the data against accidental or unlawful destruction or unauthorized disclosure. This is enforceable through Section 43 of the DPA	The Standards and Guidelines are quite extensive as regards technical safeguards; however, it fails to establish directives or protocol for reporting data breaches, and mitigating the effects of data breaches as and when they occur.

DPA Provision	Guidelines
Rights of the data subject - The rights are provided under section 26 and include, • The right to information: this is the right to be informed on how data collected will be used. • The right of access: this is the right to access data in possession of the data controller or processor. • The right to object processing: this could be processing of all or part of their personal data. • The right of rectification: this right enables a data subject correct any false or misleading data • The right of erasure: this right enables the data subject request for deletion of false or misleading data about them.	Do not provide specific means by which data subjects can exercise the rights as reflected under the DPA.
Privacy by Design and Default - Highlighted under Section 41, it requires implementation of technical and organizational safeguards at the earliest stages of design to implement the data protection principles in an effective manner and integration of necessary safeguards for the purpose of processing.	The Standards and Guidelines extensively detail measures (from implementation to utilization) for technical safeguards relating to EMR systems which covers privacy by design. However, data protection principles from the DPA relating to the processing of health data are not adequately incorporated in these measures making the implementation of privacy by design and default incomplete.
Consent - Section 32 prescribes the relevant conditions for consent which are also tied to the principle of lawfulness, fairness and transparency.	The Guidelines mention consent only in reference to electronic signatures in EMR systems as a means of signing a consent form, no further guidance is given as regards the nature of the consent form, whether it relates to medical directives or whether it relates to the processing of patient data.

DPA Provision	Guidelines
Data Protection Officer (DPO) - Provided under Section 24, the appointment of a DPO may be required for specified reasons among which include, circumstances where the core activities of the data controller or the data processor consists of processing of sensitive categories of personal data. Responsibilities of the DPO primarily relate to ensuring compliance with the provisions of the Act.	The Standards and Guidelines mention that staff may include: data entry personnel, the data manager (Health records Information Officer) and data officers, though their responsibilities are limited to the technical functionality of the EMR system. The responsibilities do not cover data protection or compliance with the provisions of the DPA.
Data Protection Impact Assessment (DPIA) - Provided for under section 31, carrying out a DPIA is relevant where processing is likely to result in high risk to the rights and freedoms of data subjects (patients) by virtue of the nature of data collected. A DPIA is important in assessing risk and creating measures to safeguard personal data (health data/ patient data) and to demonstrate compliance with the DPA.	The Guidelines provide for a number of assessments i.e., EMR readiness assessment and assessment of security needs (facility readiness); however, no guidance is given in assessing the EMR systems as regards cyber security risks and other risks that may negatively impact health data and the rights of the patient as it relates to preserving the right to privacy.



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