Kenya Medical Association

Championing the Welfare of Doctors and Quality Healthcare in Kenya

---

DATA PROTECTION POLICY

Introduction

The Kenya Medical Association recognizes that handling personal data appropriately is critical and has adopted appropriate data systems, privacy, and security measures to ensure that it shall not knowingly violate the rights of data subjects through its processing and handling of data.

This Data Protection Policy is based on globally accepted, basic principles on data protection. KMA recognizes data protection as a foundation of trustworthy relationships necessary to build the Associations reputation as a credible organization. This policy is designed to be consistent with Kenyan and other international laws and regulations including:

- The Constitution of Kenya (2010);
- The Kenya Data Protection Act, No. 24 of 2019 and Regulation;
- The 2016 International ethical guidelines for health-related research involving humans;
- The U.S. Department of Health and Human Services, regulations (45 CFR 46.116);
- National Guidelines for Ethical Conduct of Research Involving Human Subjects (2008);
- Kenya Access to Information Act No. 31
- The EU General Data Protection Regulation (GDPR) 2016/679;
- African Union Convention on Cyber Security and Personal Data; and
- The UN Guidelines for the Regulation of Computerized Personal Data Files.

This policy provides guidance on procedures to secure individuals' personal data, regulate the collection, usage, transfer, and disclosure of the said data. The definition of terms used in this policy have been listed in appendix A.

Policy Statement

KMA has a responsibility to protect confidential, restricted, and/or sensitive data from unwarranted disclosure, loss, or damage to avoid adversely affecting our staff and stakeholders from whom we collect data. Handling personal data in an ethical manner is in line with KMA's values and the Association will apply all necessary resources to ensure that the rights of individuals are protected.

Application

This Policy applies to all KMA representatives (staff, partners, contractors, fellows, and Board members).

For the purposes of this policy, the term "staff" refers to all persons who have signed a contract with KMA to work in any capacity at any given time (on regular or temporary terms, interns, volunteers, and consultants), including outsourced staff. "Partners" refers to individuals or institutions with whom KMA has a contractual agreement to deliver all or part of a project and not lead institutions on a grant where KMA is a sub-awardee.

The Policy applies to all personal data that KMA holds relating to identifiable individuals. The Association may obtain, hold, and process the personal data of data subjects in order to implement and manage all services and without which, the Association might not be able to provide its services to these individuals or to its clients.

This data includes.

- Personal details such as; name, gender, race, family and social circumstances, signatures, contact details, photos and/or videos, passport information or other travel related information, education and training records, employment and financial records.
- Details of any criminal allegations against a data subject obtained during routine due diligence checks.
- An assessment of creditworthiness of a person or an estimate of work performance by an employer.
- Any other personal data routinely collected by KMA in its operations including during recruitment and other HR processes, provision of ICT support, finance and other Association-organized activity through which personal data is collected.

The Policy applies to data in the Associations possession, collected from individuals within or outside the Association as part of the following functional categories;

- Personal data of employees/applicants: The Association collects and processes personal and Special Category data of job applicants and employees as described in the Kenya Data Protection Act (DPA), 2019, and the GDPR. The Associations Information is transmitted between and among internal units and divisions for necessary operational purposes.
- Personal data of current/prospective fellows: The Association will collect personal and Special Category of Data for prospective or enrolled fellows into its programs including

the CARTA fellowship program, in order to implement and manage all services and processes relating to its fellows, without which, the Association may be unable to provide its services to these individuals or others.

- Personal Data of Human Research Subjects: As part of its core mandate, and to implement and manage all services and processes relating to research, including research subject enrollment, testing of interventions or interaction with research subjects, publishing of research data, and other services, the Association holds the personal and Special Category Data of human research subjects'/data subjects.

Guiding Principles

KMA will adhere to the principles for processing personal data as set out in various Kenyan and international laws and regulations and relate to data subjects and data from other KMA stakeholders. These principles include:

- Privacy: KMA recognizes the right of a data subject to have control over how his or her personal data is collected, used, and/or disclosed. The association will only process data provided by a data subject willingly and, or with a legal basis as required by the law.
- Confidentiality: The Association will take reasonable measures to ensure that data in its possession is kept safe and only accessed by authorized individuals.
- Integrity: The Association will maintain accurate records and where required, take necessary steps in providing the assurance of data accuracy and consistency of data in its possession.
- Autonomy: The Association recognizes and protects the rights of data subjects to make informed decisions about when to have their data collected and for what it may be used for. The association will put in place measures that enable data subjects to exercise these rights.
- Beneficence and maleficence: The Association will process its data in a responsible way and will not knowingly process data in a way that causes harm to data subjects.
- Justice: KMA will process all data that is in its possession lawfully, fairly, and in a transparent manner. In this regard, the Association will collect personal data for specified, explicit, and legitimate purposes.

Policy implementation

Data systems

The Association will establish systems to ensure the security of personal data of any form in line with the ICT policy and as outlined in the Data Sharing Guidelines and Procedures and the Research Handbook.

Oversight and compliance

It is the responsibility of all KMA representatives to adhere to this policy and exercise utmost care when handling any personal data in their possession.

In line with the Kenya DPA 2019, KMA will appoint a Data Protection Officer (DPO) to coordinate the implementation of this policy across the Associations various functions. The DPO will liaise with staff in critical data-heavy positions in the Operations and Program Divisions to ensure compliance with this and other related policies.

Data handling at KMA

Data safety and privacy

The Association will take technical and institutional measures against unauthorized or unlawful access, processing, accidental loss, destruction, or damage to secure all its data and data systems. As such, KMA uses a wide range of security measures as outlined in its ICT Policy to safeguard personal data against unauthorized access and disclosure and will continually evaluate them to ensure they are effective.

Data access, sharing, and transfer

KMA premises its data access and sharing practices on the principle that data is a public good and should be made available to all authorized users in a timely manner and in a user-friendly format. Any individual or organization using or seeking to access KMA research data will be required to abide by the provisions of the Associations Data Sharing Procedures and Guidelines and Research Handbook.

Storage limitations

KMA will store personal data in line with the provisions of various laws and regulations guiding the storage of different types of data. KMA will store raw research data in the form of

questionnaires for a minimum of seven years. Cleaned, processed, and anonymized research data will be stored for as long as is necessary. Employee data will be stored for as long as is necessary in line with the provisions of the DPA 2019.

Marketing and commercialization of data

The Association has no intention of selling personal data or deriving any financial benefit from handling personal data. With unambiguous consent or as otherwise permitted by applicable law, KMA may use personal information for purposes relating to the marketing of our products and services, or those of our partners.

Roles and responsibilities

All KMA representatives have a role to play in ensuring compliance with this Policy. Effective Data protection requires the participation and support of every KMA employee and affiliate who deals with data and data systems. It is the responsibility of every user to familiarize themselves with this policy and adhere to it.

The following individuals have specific roles in relation to the Associations Data Protection Policy as below:

The board of directors

- Ensure the Association keeps pace with evolving data protection trends and practices.
- Ensure that potential risks are monitored and appropriate mitigation efforts are put in place.
- Bolster management's ability to apply appropriate safeguards to help minimize data breaches and other privacy mishaps, third party lawsuits, and potential negative reputational risk.

Executive leadership team

- Oversee the implementation of the Policy by developing appropriate programs and guidelines, establishing systems and processes to protect personal data in the Associations possession.
- Ensure that KMA representatives are sensitized on the Policy and compliance procedures.
- Exercise appropriate oversight to ensure that the Association adequately assesses data protection risks and implements risk mitigation procedures and processes.

- Monitor trends in data protection and institute appropriate measures.
- Data measurement and evaluation team
- Develop databases/software used to safely capture, manage, store data collected from research studies at the Association;
- Ensure compliance with the Association ICT policy in the development of data management, processing, and storage tools and platforms
- Liaise with the DPO to ensure the safety of personal research data
- Oversee the Associations data-sharing systems and processes, ensuring compliance with laws and regulations governing ethical use of human subjects' data.

Data protection officer

- Advise the organization and KMA representatives on data processing requirements provided under the DPA 2019 or any other written law.
- Ensure on behalf of the organization that the DPA is complied with.
- Facilitate capacity building of staff involved in data processing operations.
- Cooperate and seek the guidance of the Data Protection Commissioner on any matters relating to data protection.
- Record all data breaches and notify the Office of the DPC within 72 hours, where it is established that the breach may result in real harm to affected data subject(s).
- Conduct a data protection impact assessment as required by the DPA 2019 and related regulations.

Internal auditor

- Perform an independent risk assessment biannually that identifies relevant risks and the adequacy of processes and controls in place to mitigate them.

Legal and development officers

- Review and advise on any changes in the law relating to data protection
- Draft and review contracts with partners and third parties to ensure compliance with the data protection policy.
- Ensure contracts with partners embody Data Protection principles.

ICT manager

- Notify relevant staff in case of a data breach
- Secure data from loss, unauthorized access, and inconsistencies.

- Ensure data availability and accessibility.

All KMA staff

- Handle data related to the organization as required by the applicable laws and align with the principles outlined in this policy.
- Report data incidences, breaches, and malpractice to the DPO within 24 hours of being aware.

Non-compliance

Disciplinary measures will be taken against KMA staff and partners who knowingly attempt to circumvent the administrative, physical, and technical safeguards that have been put in place to protect personal data of any type. Disciplinary measures will be as outlined in the HR Policies and Procedures manual. Disciplinary action does not preclude formal legal action by the affected or referral by the Association to government authorities in accordance with the law.

Related policies

- KMA ICT Policy.
- KMA Research Handbook.
- Data Sharing Procedures and Guidelines.
- Human Resource Policies and Procedures Manual.

Monitoring and review

The Internal Audit Unit and the Data Protection Officer will monitor the implementation of this policy, regularly considering its suitability, adequacy and effectiveness.

Policy revision

This policy is subject to revision whenever legal, pragmatic, or technological developments make revision necessary. In any case, the Policy will be reviewed at least every three years.

Annex A

Definition of Terms

- Consent - means any manifestation of express, unequivocal (unambiguous), free, specific, and informed indication of the data subject's wishes by a statement or by clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.
- Data controllers - natural or legal persons, public authorities, agencies, or other bodies which, alone or jointly with others, determine the purpose and means of the processing of personal data. Data controllers have the overall say and control over the reason (the why) and purposes (the how) behind data collection and the means and method of any data processing.
- Data processors - natural or legal persons, public authority, agency, or other body, which processes personal data on behalf of the data controller.
- Data protection impact assessment - an assessment of the impact of the envisaged processing operations on the protection of personal data.
- Data subject - an identifiable natural person who is the subject of personal data.
- Encryption - the process of converting the content of any readable data using technical means into coded form.
- Identifiable natural person - a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more specific factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
- Personal data - any information relating to an identified or identifiable natural person. e.g., names, GPS locations, IMEI numbers, etc.
- Personal data breach - breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- Pseudonymisation - processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Such additional information is kept separately and is subject to technical

and organizational measures to ensure that personal data is not attributed to an identified or identifiable natural person.