NOT FOR SALE

DATA PROTECTION ACT

AND

DIGITAL HEALTH ACT

Transform Health KENYA

HEALTH FOR ALL IN THE DIGITAL AGE

KELIN

Reclaiming Rights, Rebuilding Lives

Transform Health KENYA

HEALTH FOR ALL IN THE DIGITAL AGE

A 101 GUIDE TO

Kenya's Digital Health Act & Data Protection Act

TRANSFORM HEALTH KENYA

Transform Health KENYA
HEALTH FOR ALL IN THE DIGITAL AGE

TABLE OF CONTENTS

Kenya's Digital Health Act & Data Protection Act

FULL LEGISLATION

Page numbers follow the numbering printed in the guide.

THE TWO LAWS AT A GLANCE

The Digital Health Act

Provides the legal framework for digital health systems in Kenya.

Explains exactly how Kenya's digital system **should work**.

The Data Protection Act

Protects personal data, including health data, and gives people rights over how their information is collected, used and shared.

Explains how people's personal information **should be protected.**

2 WHAT IS THE DIGITAL HEALTH ACT?

The **digital health act** is a kenyan law that provides a framework for the use of technology in healthcare. it establishes the **digital health agency**, whose role is to support, manage and coordinate digital health systems in the country.

The act also supports the creation of a comprehensive integrated health information system. this is intended to help manage health information, support health service delivery, moving Kenya from fragmented paper-based and disconnected health records to a more coordinated digital health system.

Different systems should "talk to each other" securely.

3 What does the Digital Health Act seek to achieve?

01. promote the use of digital technology in healthcare.

02. establish the digital health agency.

03. create standards for digital health systems.

04. support secure sharing of health information.

05. improve the quality and accessibility of health records.

06. Enable health data portability, meaning a person can access and use their health information across different health facilities.

07. support policy, planning, research and decision-making in the health sector.

08. Certify or approve digital health solutions so that they meet required standards.

09. Improve interoperability, meaning different digital health systems can exchange information safely and accurately.

> ***Your health records will be easier to access, safer to manage, and more useful when moving from provider to provider.***

4 What is the Data Protection Act?

The **Data Protection Act** is the main law in Kenya that protects personal information. It applies to any person or organization that collects, stores, uses, shares or processes personal data.

The Data Protection Act requires organizations to handle personal data lawfully, fairly and responsibly. It also establishes the **Office of the Data Protection Commissioner**, which oversees compliance with data protection law in Kenya.

In simple terms, the Data Protection Act gives people control over their personal information and places duties on organizations that collect or use that information.

PERSONAL DATA MEANS INFORMATION THAT CAN IDENTIFY A PERSON.
THEY INCLUDE:

- Name
- ID Number
- Location Data
- Biometrics
- Photos
- Biometrics
- Medical Records
- Financial Records

Health information is treated as especially sensitive because it can reveal private details about a person's body, health condition, treatment, family history, disability, reproductive health, HIV status, mental health or lifestyle.

5 How the Two Laws Work Together

The Digital Health Act and the Data Protection Act are connected

The digital health act allows Kenya to build and operate digital health systems. however, because these systems use personal and sensitive health data, they must comply with the **data protection act.**

A hospital, clinic, laboratory, digital health platform, insurer, government agency or any other organization handling health data must respect data protection principles.

The Digital Health Act builds the digital health infrastructure.
The Data Protection Act protects the person behind the data.

Hospitals & Clinics

A hospital should not collect more information than necessary.

Mobile Health Apps

A health app should clearly explain why it is collecting your data..

Digital Platforms

A digital health platform should secure your records from hacking or misuse.

Public Agencies

A public health agency should only use health data for lawful and legitimate purposes.

Laboratories

A laboratory should not share your test results with unauthorized people.

Patients

A patient should be able to request access to their own health information.

6 What Rights Does a Patient Have? (1/2)

Under **data protection principles**, every person has rights over their personal information.
In the health sector, these rights are very important. A person should generally have the right to:

a) Right to Be Informed

You should be told when your personal or health information is being collected. You should also be told why it is being collected, how it will be used, who may access it, and whether it may be shared..

b) Give consent where required

In many cases, your information should not be used or shared without your knowledge or consent, unless the law allows it for a valid reason such as emergency treatment, public health protection, legal obligation or another lawful basis.

c) Access your information

You should be able to request access to your health records. This helps you understand your treatment, seek a second opinion, move to another facility, or correct mistakes.

d) Correct inaccurate information

If your personal or health information is wrong, incomplete or outdated, you should be able to request correction.

What Rights Does a Patient Have? (2/2)

e) Withdraw Consent

Where your information is being processed based on consent, you should be able to withdraw that consent. For example, if you allowed a facility or platform to use your information for a certain purpose, you may later decide to withdraw that permission.

f) Object to Misuse

You can object to having your health information used in ways that are unfair, unlawful, excessive, or unrelated to the clinical reason it was collected.

g) Expect confidentiality and security

Your health records should be protected from unauthorized access, accidental loss, misuse, disclosure or tampering.

7 What responsibilities do health providers and digital health actors have?

Any organization handling health data has serious responsibilities. These include hospitals, clinics, pharmacies, laboratories, insurance providers, health technology companies, researchers and government agencies.

They should:

- Collect data only for a clear and lawful purpose. Keep health data accurate and up to date. Limit access to authorized staff only.
- Explain to patients why information is being collected.
- Use passwords, access controls, encryption and other security measures.
- Avoid sharing health data without lawful justification.
- Train staff on confidentiality and data protection.
- Report serious data breaches where required..
- Dispose of health records safely when they are no longer needed.
- Respect the rights of patients and data subjects.
- Comply with standards issued under the digital health framework.

Simply put, anyone who handles health data must treat it with **care, confidentiality** and **accountability.**

8 What is Health Data Portability?

Health data portability means that a person should be able to access and move their health information from one provider to another in a usable format.

for example

YOU RECEIVE TREATMENT FROM HOSPITAL A

Records are created during the care.

→

RECORDS MOVE WITH YOU

*Medical records should not be locked away in **one facility**.*

↓

CONTINUITY OF CARE IN HOSPITAL B

*Records should be available to support **continuity of care***

This can help reduce repeated tests, improve diagnosis, avoid medication errors and make referrals easier.

However, portability does not mean anyone can **freely access your data.** Access must still follow the law, respect confidentiality and comply with data protection requirements.

9 What Does Consent Mean in Digital Health?

Consent means a person knowingly agrees to the collection, use or sharing of their personal information for consent to be meaningful, **it should be:**

- Clear.
- Specific.
- Voluntarily.
- Based On Enough Information.
- Capable Of Being Withdrawn.

For children or people who **cannot legally give consent,** a parent, guardian or legally authorized person may give consent in their best interests.

For example, a patient may consent to their information being used for treatment. But that does not automatically mean the information can be used for marketing, research or sharing with third parties unless there is a lawful basis.

10 What are the risks the laws try to prevent?

The two laws are meant to prevent risks such as:

- **Unauthorized access to medical records.**
- **Sharing patient information without permission.**
- **Selling or commercializing health data unfairly.**
- **Using health data for discrimination.**
- **Poor cybersecurity in hospitals or health apps.**
- **Inaccurate records leading to wrong treatment.**
- **Lack of accountability when data is lost or leaked**
- **Excluding people from services because of poor digital systems**
- **Using digital health systems without proper standards.**

These risks are serious because health data is not ordinary information. It touches on dignity, privacy, equality, access to healthcare and public trust.

11 What Should Citizens Look Out For?

Before sharing health information, ask:

- Why is this information needed?
- Who will access it?
- Will it be shared with anyone else?
- How will it be protected?
- Can I access or correct my information?
- Can I withdraw consent?
- Is the platform or provider legitimate?
- Is there a privacy notice or data protection statement?

These risks are serious because health data is not ordinary information. It touches on dignity, privacy, equality, access to healthcare and public trust.

12 Compliance Steps for Health Organizations

Health organizations should take practical steps to comply with the law. **These include:**

- Develop a simple privacy notice.
- Appoint or identify a person responsible for data protection.
- Train staff on patient confidentiality.
- Keep records of how personal data is processed.
- Use secure digital systems.
- Limit access to sensitive health data.
- Have clear consent forms where needed.
- Put in place a data breach response plan.
- Review contracts with technology vendors.
- Ensure digital health tools meet legal and technical standards.
- Respect patient rights when they request access, correction or deletion where applicable.

Compliance is not just about avoiding penalties. It is about building trust in the health system.

13 Why this matters for health rights

Digital health can improve access to healthcare, especially where records are portable, services are better coordinated, and decisions are based on reliable data.

However, digital health must be people-centered. Technology should not undermine privacy, dignity, equality or access to services

The law therefore tries to balance two goals:

1. Promoting innovation and better healthcare through digital systems.
2. Protecting people from misuse of their personal and health information

A strong digital health system must be secure, inclusive, transparent and accountable.
Your health data belongs to you. Health providers and digital platforms may use it to support care and improve health services, but they must protect it, explain how it is used, and respect your rights

Transform Health KENYA

HEALTH **FOR ALL** IN THE DIGITAL AGE

FULL ACTS FOR REFERENCE

The following pages contain the full text of Kenya's Digital Health Act and Data Protection Act for readers who would like to explore the laws in more detail.

This section is included for reference and deeper reading.

THE REPUBLIC OF KENYA

LAWS OF KENYA

THE DATA PROTECTION ACT

CAP. 411C

Revised and published by the National Council for Law Reporting
with the authority of the Attorney-General as gazetted by the Government Printer

www.kenyalaw.org

Kenya

Data Protection Act

Cap. 411C

Legislation as at 31 December 2022

FRBR URI: /akn/ke/act/2019/24/eng@2022-12-31

Data Protection Act (Cap. 411C)
Contents

DATA PROTECTION ACT

CAP. 411C

Published in Kenya Gazette Vol. CXXI—No. 156 on 15 November 2019

Assented to on 8 November 2019

Commenced on 25 November 2019

[Revised by 24th Annual Supplement (Legal Notice 221 of 2023) on 31 December 2022]

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes

Part I – PRELIMINARY

1. Short title

This Act may be cited as the Data Protection Act.

2. Interpretation

In this Act, unless the context otherwise requires—

"anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

"biometric data" means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters relating to information, communication and technology;

"consent" means any 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;

"data" means information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

(d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or

(e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"Data Commissioner" means the person appointed under section 6;

"data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"data subject" means an identified or identifiable natural person who is the subject of personal data;

"encryption" means the process of converting the content of any readable data using technical means into coded form;

"filing system" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"health data" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services;

"identifiable natural person" means 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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

"national security organs" has the meaning assigned to it under Article 239 of the Constitution;

"Office" means the office of the Data Protection Commissioner;

"person" has the meaning assigned to it under Article 260 of the Constitution;

"personal data" means any information relating to an identified or identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements;

"pseudonymisation" means the 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, and such

additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"register" means the register kept and maintained by the Data Commissioner under section 21;

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject; and

"third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. Object and purpose of this Act

The object and purpose of this Act is—

(a) to regulate the processing of personal data;

(b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;

(c) to protect the privacy of individuals;

(d) to establish the legal and institutional mechanism to protect personal data; and

(e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

4. Application

This Act applies to the processing of personal data—

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means:

Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;

(b) by a data controller or data processor who—

(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

(ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.

Part II – ESTABLISHMENT OF THE OFFICE OF DATA PROTECTION COMMISSIONER

5. Establishment of the Office

(1) There is established the office of the Data Protection Commissioner which shall be a body corporate with perpetual succession and a common seal and shall in its corporate name, be capable of—

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;

(c) entering into contracts; and

(d) doing such other legal acts necessary for the proper performance of the functions of the Office.

(2) The Office is designated as a State Office in accordance with Article 260(q) of the Constitution.

(3) The Office shall comprise the Data Commissioner as its head and accounting officer, and other staff appointed by the Data Commissioner.

(4) The Office shall ensure reasonable access to its services in all parts of the Republic.

(5) The Data Commissioner shall in consultation with the Cabinet Secretary, establish such directorates as may be necessary for the better carrying of the functions of the Office.

6. Appointment of the Data Commissioner

(1) The Public Service Commission shall, whenever a vacancy arises in the position of the Data Commissioner, initiate the recruitment process.

(2) The Public Service Commission shall, within seven days of being notified of a vacancy under subsection (1), invite applications from persons who qualify for nomination and appointment for the position of the Data Commissioner.

(3) The Public Service Commission shall within twenty-one days of receipt of applications under subsection (2)—

(a) consider the applications received to determine their compliance with this Act;

(b) shortlist qualified applicants;

(c) publish and publicise the names of the applicants and the shortlisted applicants;

(d) conduct interviews of the shortlisted persons in an open and transparent process;

(e) nominate three qualified applicants in the order of merit for the position of Data Commissioner; and

(f) submit the names of the persons nominated under paragraph (e) to the President.

(4) The President shall nominate and, with approval of the National Assembly, appoint the Data Commissioner.

7. Qualifications of Data Commissioner

(1) A person shall be qualified for appointment as the Data Commissioner if that person—

(a) holds a degree from a university recognized in Kenya in—

(i) data science;

(ii) law;

(iii) information technology; or

(iv) any other related field;

(b) has knowledge and relevant experience of not less than ten years;

(c) meets the requirements of Chapter Six of the Constitution; and

(d) holds a Master's degree.

(2) The Data Commissioner shall be appointed for a single term of six years and shall not be eligible for a re-appointment.

8. Functions of the Office

(1) The Office shall—

(a) oversee the implementation of and be responsible for the enforcement of this Act;

(b) establish and maintain a register of data controllers and data processors;

(c) exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(d) promote self-regulation among data controllers and data processors;

(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;

(f) receive and investigate any complaint by any person on infringements of the rights under this Act;

(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;

(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;

(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;

(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals; and

(k) perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of this Act.

(2) The Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs.

(3) The Data Commissioner shall act independently in exercise of powers and carrying out of functions under this Act.

9. Powers of the Office

(1) The Data Commissioner shall have power to—

(a) conduct investigations on own initiative, or on the basis of a complaint made by a data subject or a third party;

(b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate;

(c) facilitate conciliation, mediation and negotiation on disputes arising from this Act;

(d) issue summons to a witness for the purposes of investigation;

(e) require any person that is subject to this Act to provide explanations, information and assistance in person and in writing;

(f) impose administrative fines for failures to comply with this Act;

(g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and

(h) exercise any powers prescribed by any other legislation.

(2) The Data Commissioner may enter into association with other bodies or organisations within and outside Kenya as appropriate in furtherance of the object of this Act.

10. Delegation by the Data Commissioner

The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to a regulator established through an Act of Parliament.

11. Vacancy in the Office of the Data Commissioner

The Office of the Data Commissioner shall become vacant, if the Data Commissioner—

(a) dies;

(b) resigns from office by notice in writing addressed to the President;

(c) is convicted of an offence and sentenced to imprisonment for a term exceeding six months without the option of a fine;

(d) is removed from office on the grounds of—

(i) inability to perform the functions of office arising from mental or physical infirmity;

(ii) non-compliance with Chapter Six of the Constitution;

(iii) bankruptcy;

(iv) incompetence; or

(v) gross misconduct.

12. Removal of the Data Commissioner

(1) A person desiring the removal of Data Commissioner on any ground specified under section 11(d) may present a complaint to the Public Service Commission setting out the alleged facts constituting that ground.

(2) Subject to Article 47 of the Constitution, the Public Service Commission shall consider the complaint and, if satisfied that the complaint discloses a ground under section 11(d), shall—

(a) investigate the matter expeditiously;

(b) report on the facts; and

(c) make a recommendation to the Cabinet Secretary.

(3) Prior to any action under subsection (2), the Data Commissioner shall be—

(a) informed, in writing, of the reasons for the intended removal; and

(b) offered an opportunity to put in a defence against any such allegations.

13. Staff of the Office

The Data Commissioner shall in consultation with the Public Service Commission, appoint such number of staff as may be necessary for the proper and efficient discharge of the functions under this Act or any other relevant law.

14. Remuneration of the Data Commissioner and staff

The Data Commissioner and staff of the Office shall be paid such remuneration or allowances as the Salaries and Remuneration Commission may advise.

15. Oath of office

The Data Commissioner shall take the oath set out in the First Schedule on appointment.

16. Confidentiality agreement

The Data Commissioner, or any staff of the Office, shall not, unless with lawful authority, disclose any information obtained for the purposes of this Act.

17. Protection from personal liability

The Data Commissioner or any staff of the Office shall not be held liable for having performed any of their functions in good faith and in accordance with this Act.

Part III – REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

18. Registration of data controllers and data processors

(1) Subject to subsection (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner.

(2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider—

(a) the nature of industry;

(b) the volumes of data processed;

(c) whether sensitive personal data is being processed; and

(d) any other criteria the Data Commissioner may specify.

19. Application for registration

(1) A data controller or data processor required to register under section 18 shall apply to the Data Commissioner.

(2) An application under subsection (1) shall provide the following particulars—

(a) a description of the personal data to be processed by the data controller or data processor;

(b) a description of the purpose for which the personal data is to be processed;

(c) the category of data subjects, to which the personal data relates;

(d) contact details of the data controller or data processor;

(e) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data;

(f) any measures to indemnify the data subject from unlawful use of data by the data processor or data controller; and

(g) any other details as may be prescribed by the Data Commissioner.

(3) A data controller or data processor who knowingly supplies any false or misleading detail under subsection (1) commits an offence.

(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

(5) A data controller or data processor shall notify the Data Commissioner of a change in any particular outlined under subsection (2).

(6) On receipt of a notification under subsection (5), the Data Commissioner shall amend the respective entry in the Register.

(7) A data controller or data processor who fails to comply with the provisions of this section commits an offence.

20. Duration of the registration certificate

A registration certificate issued under section 19 shall be valid for a period determined at the time of the application after taking into account the need for the certificate, and the holder may apply for a renewal of the certificate after expiry of the certificate.

21. Register of data controllers and data processors

(1) The Data Commissioner shall keep and maintain a register of the registered data controllers and data processors.

(2) The Data Commissioner may, at the request of a data controller or data processor, remove any entry in the register which has ceased to be applicable.

(3) The register shall be a public document and available for inspection by any person.

(4) A person may request the Data Commissioner for a certified copy of any entry in the register.

22. Cancellation or variation of the certificate

The Data Commissioner may, on issuance of a notice to show cause, vary terms and conditions of the certificate of registration or cancel the registration where—

(a) any information given by the applicant is false or misleading; or

(b) the holder of the registration certificate, without lawful excuse, fails to comply with any requirement of this Act.

23. Compliance and audit

The Data Commissioner may carry out periodical audits of the processes and systems of the data controllers or data processors to ensure compliance with this Act.

24. Designation of the Data Protection Officer

(1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where—

(a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;

(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or

(c) the core activities of the data controller or the data processor consist of processing of sensitive categories of personal data.

(2) A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

(3) A group of entities may appoint a single data protection officer provided that such officer is accessible by each entity.

(4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

(5) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

(6) A data controller or data processor shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

(7) A data protection officer shall—

(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;

(b) ensure on behalf of the data controller or data processor that this Act is complied with;

(c) facilitate capacity building of staff involved in data processing operations;

(d) provide advice on data protection impact assessment; and

(e) co-operate with the Data Commissioner and any other authority on matters relating to data protection.

Part IV – PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

25. Principles of data protection

Every data controller or data processor shall ensure that personal data is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

26. Rights of a data subject

A data subject has a right—

(a) to be informed of the use to which their personal data is to be put;

(b) to access their personal data in custody of data controller or data processor;

(c) to object to the processing of all or part of their personal data;

(d) to correction of false or misleading data; and

(e) to deletion of false or misleading data about them.

27. Exercise of rights of data subjects

A right conferred on a data subject may be exercised—

(a) where the data subject is a minor, by a person who has parental authority or by a guardian;

(b) where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or

(c) in any other case, by a person duly authorised by the data subject.

28. Collection of personal data

(1) A data controller or data processor shall collect personal data directly from the data subject.

(2) Despite subsection (1), personal data may be collected indirectly where—

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection from another source;

(d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;

(e) the collection from another source would not prejudice the interests of the data subject;

(f) collection of data from another source is necessary—

(i) for the prevention, detection, investigation, prosecution and punishment of crime;

(ii) for the enforcement of a law which imposes a pecuniary penalty; or

(iii) for the protection of the interests of the data subject or another person.

(3) A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

29. Duty to notify

A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of—

(a) the rights of data subject specified under section 26;

(b) the fact that personal data is being collected;

(c) the purpose for which the personal data is being collected;

(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;

(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;

(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and

(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

30. Lawful processing of personal data

(1) A data controller or data processor shall not process personal data, unless—

(a) the data subject consents to the processing for one or more specified purposes; or

(b) the processing is necessary—

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data subject or another natural person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

(2) Further processing of personal data shall be in accordance with the purpose of collection.

(3) A data controller who contravenes the provisions of subsection (1) commits an offence.

31. Data protection impact assessment

(1) Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment shall include the following—

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects;

(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

(3) The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.

(4) For the purposes of this section, a "data protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data.

(5) The data impact assessment reports shall be submitted sixty days prior to the processing of data.

(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section.

32. Conditions of consent

(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) The withdrawal of consent under subsection (2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, 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 personal data that is not necessary for the performance of that contract.

33. Processing of personal data relating to a child

(1) Every data controller or data processor shall not process personal data relating to a child unless—

(a) consent is given by the child's parent or guardian; and

(b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under subsection (2) shall be determined on the basis of—

(a) available technology;

(b) volume of personal data processed;

(c) proportion of such personal data likely to be that of a child;

(d) possibility of harm to a child arising out of processing of personal data; and

(e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under subsection (1).

34. Restrictions on processing

(1) A data controller or data processor shall, at the request of a data subject, restrict the processing of personal data where—

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

(b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;

(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(d) data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

(2) Where processing of personal data is restricted under this section—

(a) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) The data controller or data processor shall implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is observed.

35. Automated individual decision making

(1) Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

(2) subsection (1) shall not apply where the decision is—

(a) necessary for entering into, or performing, a contract between the data subject and a data controller;

(b) authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) based on the data subject's consent.

(3) Where a data controller or data processor takes a decision, which produces legal effects or significantly affects the data subject based solely on automated processing—

(a) the data controller or data processor must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and

(b) the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to—

(i) reconsider the decision; or

(ii) take a new decision that is not based solely on automated processing.

(4) A data controller or data processor, upon receipt of a request under subsection (3), shall within a reasonable period of time—

(a) consider the request, including any information provided by the data subject that is relevant to it;

(b) comply with the request; and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request; and

(ii) the outcome of complying with the request.

(5) The Cabinet Secretary may by Regulations make such further provision to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of decisions based solely on automated processing.

36. Objecting to processing

A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim.

37. Commercial use of data

(1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person—

(a) has sought and obtained express consent from a data subject; or

(b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

(3) The Cabinet Secretary, in consultation with the Data Commissioner, may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

38. Right to data portability

(1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under subsection (1), to another data controller or data processor without any hindrance.

(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.

(4) Where data controller or data processor declines to comply with a request under subsection (3), the Data Commissioner may make a determination on the technical capacity of the data controller or data processor.

(5) The right under this section shall not apply in circumstances where—

(a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or

(b) it may adversely affect the rights and freedoms of others.

(6) A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of thirty days.

(7) Where the portability request is complex or numerous, the period under subsection (6) may be extended for a further period as may be determined in consultation with the Data Commissioner.

39. Limitation to retention of personal data

(1) A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is—

(a) required or authorised by law;

(b) reasonably necessary for a lawful purpose;

(c) authorised or consented by the data subject; or

(d) for historical, statistical, journalistic literature and art or research purposes.

(2) A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under subsection (1) in a manner as may be specified at the expiry of the retention period.

40. Right of rectification and erasure

(1) A data subject may request a data controller or data processor—

(a) to rectify without undue delay personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or

(b) to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(2) Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested—

(a) the rectification of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; or

(b) the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(3) Where a data controller or data processor is required to rectify or erase personal data under subsection (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.

41. Data protection by design or by default

(1) Every data controller or data processor shall implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner; and

(b) to integrate necessary safeguards for that purpose into the processing.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.

(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration—

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage;

(d) its accessibility; and

(e) the cost of processing data and the technologies and tools used.

(4) To give effect to this section, the data controller or data processor shall consider measures such as—

(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) to establish and maintain appropriate safeguards against the identified risks;

(c) to the pseudonymisation and encryption of personal data;

(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) to verify that the safeguards are effectively implemented; and

(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.

42. Particulars of determining organisational measures

(1) In determining the appropriate measures referred to in section 41, in particular, where the processing involves the transmission of data over an information and communication network, a data controller shall have regard to—

(a) the state of technological development available;

(b) the cost of implementing any of the security measures;

(c) the special risks that exist in the processing of the data; and

(d) the nature of the data being processed.

(2) Where a data controller is using the services of a data processor—

(a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of organisational measures for the purpose of complying with section 41(1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

(3) Where a data processor processes personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing.

(4) A data controller or data processor shall take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor, complies with the relevant security measures.

43. Notification and communication of breach

(1) Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall—

(a) notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and

(b) subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

(2) Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.

(3) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.

(4) The data controller may delay or restrict communication referred to under subsection (1)(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

(5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including—

(a) description of the nature of the data breach;

(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;

(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and

(e) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.

(6) The communication of a breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.

(7) Where and to the extent that it is not possible to provide all the information mentioned in subsection (5) at the same time, the information may be provided in phases without undue delay.

(8) The data controller shall record the following information in relation to a personal data breach—

(a) the facts relating to the breach;

(b) its effects; and

(c) the remedial action taken.

Part V – GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

44. Processing of sensitive personal data

No category of sensitive personal data shall be processed unless section 25 applies to that processing.

45. Permitted grounds for processing sensitive personal data

Without prejudice to section 44, sensitive personal data of a data subject may be processed where—

(a) the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that—

(i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and

(ii) the personal data is not disclosed outside that body without the consent of the data subject.

(b) the processing relates to personal data which is manifestly made public by the data subject; or

(c) processing is necessary for—

(i) the establishment, exercise or defence of a legal claim;

(ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or

(iii) protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

46. Personal data relating to health

(1) 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.

(2) The condition under subsection (1) is met if the processing—

(a) is necessary for reasons of public interest in the area of public health; or

(b) is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

47. Further categories of sensitive personal data

(1) The Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard—

(a) to the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;

(b) to the expectation of confidentiality attached to such category of personal data;

(c) to whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and

(d) to the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Data Commissioner may specify other categories of personal data, which may require additional safeguards or restrictions.

Part VI – TRANSFER OF PERSONAL DATA OUTSIDE KENYA

48. Conditions for transfer out of Kenya

A data controller or data processor may transfer personal data to another country only where—

(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;

(c) the transfer is necessary—

(i) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

49. Safeguards prior to transfer of personal data out of Kenya

(1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

(2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.

(3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

50. Processing through a data server or data centre in Kenya

The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.

Part VII – EXEMPTIONS

51. General exemptions

(1) Nothing in this Part shall exempt any data controller or data processor from complying with data protection principles relating to lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data.

(2) The processing of personal data is exempt from the provisions of this Act if—

(a) it relates to processing of personal data by an individual in the course of a purely personal or household activity;

(b) if it is necessary for national security or public interest; or

(c) disclosure is required by or under any written law or by an order of the court.

52. Journalism, literature and art

(1) The principles of processing personal data shall not apply where—

(a) processing is undertaken by a person for the publication of a literary or artistic material;

(b) data controller reasonably believes that publication would be in the public interest; and

(c) data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

(2) Subsection (1)(b) shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question.

(3) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature and Art.

53. Research, history and statistics

(1) The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes and the data controller or data processor shall ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

(2) The data controller or data processor shall take measures to establish appropriate safeguards against the records being used for any other purposes.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if—

(a) data is processed in compliance with the relevant conditions; and

(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Research, History and Statistics.

54. Exemptions by the Data Commissioner

The Data Commissioner may prescribe other instances where compliance with certain provisions of this Act may be exempted.

55. Data-sharing code

(1) The Data Commissioner may issue a data sharing code which shall contain—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation; and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) The data sharing code under subsection (1) shall specify on the lawful exchange of personal data between government departments or public sector agencies.

Part VIII – ENFORCEMENT PROVISIONS

56. Complaints to the Data Commissioner

(1) A data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner in accordance with this Act.

(2) A person who intends to lodge a complaint under this Act shall do so orally or in writing.

(3) Where a complaint made under subclause (1) is made orally, the Data Commissioner shall cause the complaint to be recorded in writing and the complaint shall be dealt with in accordance with such procedures as the Data Commissioner may prescribe.

(4) A complaint lodged under subclause (1) shall contain such particulars as the Data Commissioner may prescribe.

(5) A complaint made to the Data Commissioner shall be investigated and concluded within ninety days.

57. Investigation of complaints

(1) The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to—

(a) attend at a specified time and place for the purpose of being examined orally in relation to the complaint;

(b) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other enactment from disclosing; or

(c) furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(2) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(3) A person who, without reasonable excuse, fails or refuses to comply with a notice, or who furnishes to the Data Commissioner any information which the person knows to be false or misleading, commits an offence.

58. Enforcement notices

(1) Where the Data Commissioner is satisfied that a person has failed, or is failing, to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice on that person requiring that person to take such steps and within such period as may be specified in the notice.

(2) An enforcement notice served under subsection (1) shall—

(a) specify the provision of this Act which has been, is being or is likely to be, contravened;

(b) specify the measures that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise;

(c) specify a period which shall not be less than twenty-one days within which those measures shall be implemented; and

(d) state any right of appeal.

(3) Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

59. Power to seek assistance

For the purpose of gathering information or for any investigation under this Act, the Data Commissioner may seek the assistance of such person or authority as they deem fit and as is reasonably necessary to assist the Data Commissioner in the discharge of their functions.

60. Power of entry and search

The Data Commissioner, upon obtaining a warrant from a Court, may enter and search any premises for the purpose of discharging any function or exercising any power under this Act.

61. Obstruction of Data Commissioner

A person who, in relation to the exercise of a power conferred by section 9—

(a) obstructs or impedes the Data Commissioner in the exercise of their powers;

(b) fails to provide assistance or information requested by the Data Commissioner;

(c) refuses to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions;

(d) gives to the Data Commissioner any information which is false or misleading in any material aspect,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

62. Penalty notices

(1) If the Data Commissioner is satisfied that a person has failed or is failing as described in section 58, the Data Commissioner may issue a penalty notice requiring the person to pay to the Office of the Data Commissioner an amount specified in the notice.

(2) In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Data Commissioner shall, so far as relevant, have regard—

(a) to the nature, gravity and duration of the failure;

(b) to the intentional or negligent character of the failure;

(c) to any action taken by the data controller or data processor to mitigate the damage or distress suffered by data subjects;

(d) to the degree of responsibility of the data controller or data processor, taking into account technical and organisational measures;

(e) to any relevant previous failures by the data controller or data processor;

(f) to the degree of co-operation with the Data Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) to the categories of personal data affected by the failure;

(h) to the manner in which the infringement became known to the Data Commissioner, including whether, and if so to what extent, the data controller or data processor notified the Data Commissioner of the failure;

(i) to the extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;

(j) to adherence to approved codes of conduct or certification mechanisms;

(k) to any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) to whether the penalty would be effective, proportionate and dissuasive.

63. Administrative fines

In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

64. Right of appeal

A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court.

65. Compensation to a data subject

(1) A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor.

(2) Subject to subsection (1)—

(a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and

(b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the Act specifically directed at data processors; or

(ii) has acted outside, or contrary to, the data controller's lawful instructions.

(3) A data controller or data processor is not liable in the manner specified in subsection (2) if the data controller or data processor proves that they are not in any way responsible for the event giving rise to the damage.

(4) In this section, "damage" includes financial loss and damage not involving financial loss, including distress.

66. Preservation Order

The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.

Part IX – FINANCIAL PROVISIONS

67. Funds of the Office

The funds and assets of the Office shall consist of—

(a) monies allocated by the National Assembly for purposes of the Office;

(b) any grants, gifts, donations or other endowments given to the Office; and

(c) such funds as may vest in or accrue to the Office in the performance of its functions under this Act or any other written law.

68. Annual estimates

(1) At least three months before the commencement of each financial year, the Data Commissioner shall cause to be prepared estimates of the revenue and expenditure of the Office for that year.

(2) The annual estimates shall make provision for all the estimated expenditure of the Office for the financial year concerned and in particular shall provide for—

(a) the payment of salaries, allowances and other charges in respect of the staff of the Office;

(b) the payment of pensions, gratuities and other charges in respect of retirement benefits which are payable out of the finances of the Office;

(c) the acquisition, maintenance, repair and replacement of the equipment and other movable property of the Office;

(d) funding of training, research and development of activities of the Office;

(e) the creation of such reserve funds to meet future or contingent liabilities or in respect of such other matters as the Data Commissioner may deem fit; and

(f) any other expenditure for the purposes of this Act.

(3) The annual estimates shall be submitted to the Cabinet Secretary for tabling in the National Assembly.

69. Accounts and Audit

The annual accounts of the Office shall be prepared, audited and reported in accordance with the provisions of Articles 226 and 229 of the Constitution, the Public Finance Management Act (Cap. 412A), or any other law relating to audit of public entities.

70. Annual reports

(1) The Data Commissioner shall, within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year.

(2) The Cabinet Secretary shall submit the annual report before the National Assembly within three months of receipt of the report under subsection (1).

(3) The annual report shall contain in respect of the year to which it relates—

(a) the financial statements and description of activities of the Office;

(b) such other statistical information as the Data Commissioner may consider appropriate relating to the Data Commissioner's functions;

(c) the impact of the exercise of any of Data Commissioner's mandate or function;

(d) any impediments to the achievements of the object and purpose of this Act or any written law; and

(e) any other information relating to its functions that the Data Commissioner may consider necessary.

Part X – PROVISIONS ON DELEGATED POWERS

71. Regulations

(1) The Cabinet Secretary may, make regulations generally for giving effect to this Act, and for prescribing anything required or necessary to be prescribed by or under this Act.

(2) Without prejudice to the generality of subsection (1), regulations made under that subsection may provide for—

(a) the requirements which are imposed on a data controller or data processor when processing personal data;

(b) mechanisms of conducting certification program;

(c) the contents which a notice or registration by a data controller or data processor should contain;

(d) information to be provided to a data subject and how such information shall be provided;

(e) the levying of fees and taking of charges;

(f) the measures to safeguard a data subject's rights, freedoms and legitimate interests;

(g) the processing of data through a data server or data centre in Kenya;

(h) issuing and approval of codes of practice and guidelines; or

(i) any other matter that the Cabinet Secretary may deem fit.

(3) For the purposes of Article 94(6) of the Constitution—

(a) the purpose and objective of the delegation under this section is to enable the Cabinet Secretary to make regulations for better carrying into effect the provisions of this Act;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and fulfilment of the objectives specified under this section.

(4) The principles and standards applicable to the delegated power referred to under this Act are those found in—

(a) the Statutory Instruments Act (Cap. 2A);

(b) the Interpretation and General Provisions Act (Cap. 2);

(c) the general rules of international law as specified under Article 2(5) of the Constitution; and

(d) any treaty and convention ratified by Kenya under Article 2(6) of the Constitution.

Part XI – MISCELLANEOUS PROVISIONS

72. Offences of unlawful disclosure of personal data

(1) A data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected commits an offence.

(2) A data processor who, without lawful excuse, discloses personal data processed by the data processor without the prior authority of the data controller commits an offence.

(3) Subject to subsection (4), a person who—

(a) obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or data processor by whom the data is kept; or

(b) discloses personal data to third party, commit an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor acting within the scope of such mandate.

(5) A person who offers to sell personal data where such personal data has been obtained in breach of subsection (1) commits an offence.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

73. General penalty

(1) A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.

(2) In addition to any penalty referred to in subsection (1), the Court may—

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence; or

(b) order or prohibit the doing of any act to stop a continuing contravention.

74. Codes, guidelines and certification

(1) The Data Commissioner may, for the purpose of this Act—

(a) issue guidelines or codes of practice for the data controllers, data processors and data protection officers;

(b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act;

(c) require certification or adherence to code of practice by a third party;

(d) develop sector specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social Protection and any other area as the Data Commissioner may determine.

(2) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.

75. [Spent]

FIRST SCHEDULE [s. 15]

OATH OF OFFICE

I, ..., make oath/solemnly affirm/declare that I will faithfully and honestly fulfil my duties as the Data Commissioner in conformity with the Data Protection Act and that I shall not, without the due authority in that behalf, disclose or make known any matter or thing which comes to my knowledge by reason of discharge of my duties.

.....

Magistrate/Judge

SECOND SCHEDULE [s. 75.]

CONSEQUENTIAL AMENDMENTS

Spent

THE REPUBLIC OF KENYA

LAWS OF KENYA

THE DIGITAL HEALTH ACT

NO. 15 OF 2023

Revised and published by the National Council for Law Reporting
with the authority of the Attorney-General as gazetted by the Government Printer

www.kenyalaw.org

Kenya

Digital Health Act

Act No. 15 of 2023

Legislation as at 24 November 2023

FRBR URI: /akn/ke/act/2023/15/eng@2023-11-24

Digital Health Act (Act No. 15 of 2023)
Contents

DIGITAL HEALTH ACT

NO. 15 OF 2023

Published in Kenya Gazette Vol. CXXV—No. 249 on 24 November 2023

Assented to on 19 October 2023

Commenced on 2 November 2023

AN ACT of Parliament to provide for the establishment of the Digital Health Agency; to provide a framework for provision of digital health services; to establish a comprehensive integrated digital health information system; and for connected purposes

Part I – PRELIMINARY

1. Short title

This Act may be cited as the Digital Health Act, 2023.

2. Interpretation

In this Act, unless the context otherwise requires—

"**Agency**" means the Digital Health Agency established under section 5;

"**anonymization**" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

"**Board**" means the Board of Directors of the Agency constituted under section 8;

"**Cabinet Secretary**" means the Cabinet Secretary for ministry responsible for matters relating to health;

"**client**" means an individual who uses, or has used, a health service, or in relation to whom health data has been created;

"**consent**" has the meaning assigned to it under the Data Protection Act (Cap. 411C);

"**County Executive Committee Member**" means the member of county executive committee appointed and designated to supervise health services;

"**data**" means information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

(d) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d);

"**data analysis**" means the process of inspecting, cleaning, transforming, consolidation and modelling of data with the goal of discovering useful information, extracting meaningful insights, suggesting conclusions and supporting decision making;

"**data bank**" means an organised collection of data designed to efficiently store and retrieve data that can be accessed, managed and updated electronically to allow users to easily search for and access the information they need, to derive insights, make informed decisions and improve performance;

"**data commissioner**" means the person appointed under section 6 of the Data Protection Act (Cap. 411C);

"**data controller**" means a natural or legal person, public authority, agency or other body which, alone jointly with others, determines the purpose and means of processing of personal data; or

"**data disposal**" means the process of destroying manual or electronic records or data completely without being used or accessed for an authorized purpose;

"**data governance**" means the overall management of the availability, usability, integrity and security of data used in an organization;

"**data integrity**" means the overall completeness, accuracy and consistency of data;

"**data life cycle**" means the stages through which data passes from its creation or acquisition to its eventual deletion or archival;

"**data management**" means the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets, and involves policy formulation and adherence to data management procedures such as reporting rates, harmonized and standard data collection tools;

"**data privacy**" means the aspect of information technology that deals with the ability an organization or individual has to detemine what data in a computer system can be shared with third parties for purposes of the keeping of information private and safe;

"**data processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"**data reporting**" means the process of collection, submission and organisation of data into informational summaries in order to monitor performance;

"**data retention**" means the continued storage of an organization's data for compliance with national policy guidelines and regulations;

"**data security**" means protection of electronic health data, and specifically the means used to protect the privacy of health information contained in electronic health data that supports professionals in holding that information in confidence;

"**data storage**" means the recording of information in a storage medium or holding information in digital format;

"**data subject**" means an identified or identifiable natural person who is the subject of personal data;

"**de-identification**" means removing or hiding personal information from records in such a way that the remaining information cannot be used to identify an individual;

"**data verification**" includes the authentication and validation of gathered data, data quality checks, audit of the health data using the data quality protocols;

"**digital health**" means the field of knowledge and practice that is associated with the development and use of digital technologies to improve health;

"**Director-General**" means the Director-General for health appointed under section 16 of the Health Act (Cap. 241);

"**disclosure**" means submission of relevant information to an authorized party;

"**e-Health**" means the combined use of electronic communication and information technology in the health sector including telemedicine;

"**e-Health ecosystem**" means the combined application of e-Health infrastructure, standards, technology, systems applications, investment, health workforce and governance that support patient-centred models of healthcare;

"**e-Health platform**" means an ecosystem of hardware, software and technology used to deliver e-Health services;

"**electronic health data**" means an electronic record of personal health related information about an individual and shall include—

(a) information concerning the physical or mental health of the individual;

(b) information concerning any health service provided to the individual;

(c) information concerning the donation by the individual of any body part or any bodily substance;

(d) information derived from the testing or examination of a body part or bodily substance of the individual;

(e) information that is collected in the course of providing health services to the individual; or

(f) information relating to details of the health facility accessed by the individual;

"**encryption**" means the process of converting the content of any readable data using technical means into coded form;

"**enterprise class**" refers to applications that are designed to be robust and scalable across a large organization, and compatible with existing databases and tools, customizable for the needs of specific departments, powerful enough to scale up along with the needs of the business using it, secure from outside threats and data leaks;

"**enterprise service bus**" means an architectural pattern whereby a centralized software component performs integrations between applications; transformations of data models, handles connectivity, message routing, converts communication protocols and potentially manages the composition of multiple requests and may make these integrations and transformations available as a service interface for reuse by new applications;

"**e-waste**" means waste resulting from electrical and electronic equipment including components and sub-assemblies thereof;

"**guardian**" means a guardian recognised under any law for the time being in force;

"**health care professional**" includes any person who has obtained health professional qualifications and licensed by the relevant regulatory body;

"**health care provider**" has the meaning assigned to it under the Health Act (Cap. 241);

"**health care services**" has the meaning assigned to it under the Health Act (Cap. 241);

"**health data**" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for or provision of health services or data which associates the data subject to the provision of specific health services;

"**health data controller**" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of health data;

"**health data custodian**" means a person or organization that possesses legal custody over health data;

"**health data processor**" means a person, public authority, agency or other body who is an authorised worker to process health data;

"**health facility**" has the meaning assigned to it under the Health Act (Cap. 241);

"**health informatics**" means the practice of acquiring, studying and managing health data and applying medical concepts in conjunction with health information technology systems to help health professionals provide better healthcare;

"**health information bank**" means an electronic database under the custody and control of the Ministry of Health that contains personal health information and is designated by the Cabinet Secretary as a health information bank;

"**health information system**" means a health ecosystem designed to manage health and health related system data that provides the foundations for decision-making and includes a system that collects, collates, stores, manages, analyses, synthesises, transmit patient's or client's electronic health record and uses health and health related data for operational management or a system supporting healthcare policy decisions;

"**health records and information management**" means the practice of acquiring, analysing and protecting digital and traditional medical information vital to providing quality patient or client care;

"**health records and information manager**" means an officer trained in health records and information management and charged with the responsibility of managing health records and health information for the health services which include—

(a) creating and enforcing policies for effective data management;

(b) clinical coding and classifications;

(c) coding for health insurance firms;

(d) health information management;

(e) health administrative data and medical data analytics and research;

(f) appraisal of medical documentations and audits;

(g) advice on medical legal issues;

(h) advise on retrieval and disposal of Health and medical records;

(i) use of e-Health applications;

"**health related data information**" means the service delivery and administrative health data collected, analysed and synthesised for decision making in the health sector;

"**health system**" means an organization of people, institutions and resources that deliver health care services to meet the health needs of the population, in accordance with established policies;

"**health technology**" means the application of organized knowledge and skills in the form of devices, medicine, vaccines, procedures and systems developed to solve a health problem and improve the quality of life;

"**health tourism**" means a situation where a patient travels across international borders to receive medical treatment;

"**individual**" means data subject;

"**integrated e-Health information system**" means a health information system that collects health and health related data that addresses the needs of all users for decision making;

"**Kenya Health Enterprise Architecture**" means a blueprint that guides the design, development and evolution of the comprehensive integrated health information system to align investments, in technology, information and processes that are cost-effective, sustainable, and aligned with the Kenya health sector strategic goals;

"**medical equipment data**" means data relating to a medical equipment and contains manufacturer-provided information and client-created inventory information about such equipment and may include exhaust digital data and individual data that may be classified as sensitive data under the Data Protection Act (Cap. 411C);

"**m-Health**" means the delivery of medical services using mobile technologies;

"**personal data**" means any information relating to an identified or identifiable natural person;

"**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**personal health data**" means any information relating to the state of physical or mental health of an identified or identifiable person and includes records on the past, present or future state of that person's health;

"**personal health information**" means data related to the state of physical or mental health of an individual and includes information provided by the client, records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the individual to the provision of specific health services;

"**personally identifiable information**" means information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person;

"**private health services**" means provision of health services by a health facility that is not owned by the national or county governments and includes health care services provided by individuals, faith-based organizations, non-governmental organizations and private for profit health institutions;

"**processing**" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means including—

(a) collection, recording, organisation or structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

"**pseudo-anonymization**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"**public health services**" means health services owned and offered by the national and county governments;

"**referral**" means the process by which a given health facility transfers a client service, specimen and client parameters to another facility to assume responsibility for consultation, review or further management;

"**research for health**" includes research which seeks to contribute to the extension of knowledge in any health related field, such as that concerned with the biological, clinical, psychological or social processes in human beings improved methods for the provision of health services; human pathology; the causes of disease; the effects of the environment on the human body; the development or new application of pharmaceuticals, medicines and other preventative, therapeutic or curative agents; or the development of new applications of health technology;

"**system**" means the comprehensive integrated health information system established under section 15;

"**system integration**" refers to the merging or combining of two or more components or configuration items into a higher level system element and ensuring that the logical and physical interfaces are satisfied and that the integrated system satisfies its intended purpose;

"**system interoperability**" refers to the capability to communicate, execute programs or transfer data among various functional units such that the user needs little or no knowledge of the unique characteristics of those units;

"**telehealth**" means the use of electronic information and telecommunications technologies including video conferencing, the internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications, to support long-distance clinical health care, patient and professional health-related education, public health and health administration;

"**telemedicine**" refers to the provision of health care services and sharing of medical knowledge over distance using telecommunications and includes consultative, diagnostic, and treatment services; and

"**third party**" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. Objects of the Act

The objects of this Act are to—

(a) establish the Digital Health Agency;

(b) establish and maintain a comprehensive integrated health information system;

(c) promote innovation and the safe, efficient and effective use of technology for healthcare, including for continuity of care, emergency and disaster preparedness and disease surveillance;

(d) establish a regulatory framework for the e-Health ecosystem data lifecycle;

(e) provide for privacy, confidentiality, and security of health data;

(f) develop standards for the provision of m-Health, telemedicine, and e-learning;

(g) establish a regulatory framework for e-waste management; and

(h) provide for the safe and secure transfer of personal, identifiable health data and client's medical records to and from health facilities within and outside Kenya.

4. Guiding principles

In implementing the Act, all persons shall be guided by the following principles—

(a) health data is a strategic national asset;

(b) safeguard of the privacy, confidentiality and security of health data for information sharing and use;

(c) digital health shall facilitate data sharing and use for informed decision-making at all levels; and

(d) the digital health ecosystem shall serve the health sector and facilitate in a progressive and equitable manner, the highest attainable standard of health.

Part II – ESTABLISHMENT OF THE DIGITAL HEALTH AGENCY

5. Establishment of the Digital Health Agency

(1) There is established an Agency to be known as the Digital Health Agency.

(2) The Agency shall be a body corporate with perpetual succession and a common seal and shall, in its corporate name, be capable of—

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging and disposing of movable and immovable property;

(c) receiving, investing, borrowing money; and

(d) doing or performing such other things or acts necessary for the proper performance of its functions under this Act.

6. Functions of the Agency

The Agency shall—

(a) develop, operationalise and maintain the Comprehensive Integrated Health Information System to manage the core digital systems and the infrastructure required for its seamless health information exchange;

(b) establish registries, in consultation with other statutory authorities, at appropriate levels to create single source of truth in respect of clients, health facilities, healthcare providers, health products and technologies;

(c) promote adoption of best practices and standards for digital health that facilitate data exchange;

(d) establish a system of shareable and portable personal health records, based on best practices and standards;

(e) ensure health data portability;

(f) facilitate collection and analysis of data to inform policy and research in the health sector;

(g) promote the development of enterprise-class health application systems;

(h) strengthen existing health information systems by ensuring their conformity with the prescribed standards and integration with the comprehensive integrated health information system;

(i) develop and implement the infrastructure for health data exchange of health information in a secured manner;

(j) maintain, in collaboration with the counties and other statutory authorities, the technological infrastructure necessary for the core digital health services;

(k) support the development and implementation of standards for enhanced interoperability;

(l) undertake resource mobilization implementation of health digitization in the country;

(m) certify digital health solutions based on best practices and standards;

(n) advise the Cabinet Secretary on matters related to digital health; and

(o) perform any other function for the better carrying out of functions under this Act.

7. Powers of the Agency

(1) The Board shall be responsible for the management and administration of the Agency.

(2) Without prejudice to the generality of the foregoing, the Agency shall have power to—

(a) manage, control and administer the assets of the Agency in such manner and for such purpose as best promotes the objects for which the Agency is established in accordance with the Public Procurement and Assets Disposal Act (Cap. 412C):

Provided that the Agency shall not charge or dispose of any immovable property without the prior approval of the National Assembly;

(b) enter into association with such other bodies or organizations, within or outside Kenya, as it may consider desirable or appropriate and in furtherance of the purpose for which the Agency is established; and

(c) invest the funds of the Agency not immediately required for its purposes in the manner provided in this Act.

8. Board of Directors

(1) There shall be a Board of Directors of the Agency which shall consist of—

(a) a non-executive chairperson who shall be appointed by the President;

(b) the Principal Secretary responsible for Health or a representative designated in writing;

(c) the Principal Secretary responsible for the National Treasury or a representative designated in writing;

(d) the Principal Secretary responsible for Information, Communication and Technology or a representative designated in writing;

(e) the Data Commissioner or a representative designated in writing;

(f) one person representing the private sector appointed by the Cabinet Secretary;

(g) three persons, not being Governors, nominated by the Council of County Governors with knowledge and experience in matters of digital health; and

(h) the Chief Executive Officer, who shall be an *ex-officio* member of the Board.

(2) The Chairperson of the Board and the members appointed under subsection (1) (f) and (g) shall serve for a term of three years and shall be eligible for re-appointment for one further term of three years.

(3) In appointing persons as members of the Board under subsection (1)(f) and (g), the Cabinet Secretary shall ensure that the appointments afford equal opportunity to men and women, youth, persons with disabilities, minorities and marginalized groups and ensure regional balance.

(4) A person appointed to the Board under sub-section (1)(a), (f) and (g) shall cease to be a member of the Board if the person-

(a) resigns in writing addressed to the Cabinet Secretary;

(b) is adjudged bankrupt;

(c) is absent from three consecutive meetings without the permission of the Chairperson;

(d) is convicted of a criminal offence and sentenced to imprisonment for a term exceeding six months; or

(e) is unable to perform the functions of his office by reason of mental or physical infirmity.

(5) Despite subsection (4), the Chairperson or the member of the Board may be removed for-

(a) incompetence or neglect of duty;

(b) gross misconduct whether in the performance of the members' functions or otherwise; or

(c) violation of the Constitution or any other written law.

(6) The Agency shall pay to the directors such remuneration, fees or allowances for expenses as may be determined by the Cabinet Secretary on the advice of the Salaries and Remuneration Commission.

(7) The Board may co-opt any other person with necessary expertise as it may deem necessary to assist the Board in discharging its duties and responsibilities.

9. Conduct of business and affairs of the Board

Except as provided in the Schedule, the Board shall regulate its own procedure.

10. Committees of the Board

(1) The Board may, from time to time, establish such committees as it considers necessary for the better carrying out of its functions under this Act.

(2) The Board may co-opt into the membership of a committee established under sub-section (1) such other person whose knowledge and skills are found necessary for the functions of the Agency.

11. Chief Executive Officer

(1) The Board shall, through an open, transparent and competitive recruitment process, appoint a suitably qualified person to be the Chief Executive Officer of the Agency.

(2) Subject to this Act, the Chief Executive Officer shall be appointed on such terms and conditions of service as shall be determined by the Board in the instrument of appointment or otherwise in writing from time to time in consultation with the Salaries and Remuneration Commission.

12. Qualification for appointment as Chief Executive Officer

(1) A person shall be qualified for appointment as the Chief Executive Officer of the Agency if that person—

(a) has a minimum of a master's degree from a university recognized in Kenya;

(b) has at least ten years' knowledge and experience in health information science, data science, data governance, health informatics, digital health or any other relevant field;

(c) has served in a management level for a period of at least five years;

(d) has not been convicted of an offence and is not serving a term of imprisonment; and

(e) meets the requirements of Chapter Six of the Constitution.

(2) The Chief Executive Officer shall, subject to the directions of the Board, be responsible for the day to day management of the affairs and staff of the Board.

(3) The Chief Executive Officer shall be the accounting officer of the Agency.

(4) The Chief Executive Officer shall hold office for a period of three years and shall be eligible for reappointment for one further term of three years.

13. Corporation Secretary

(1) There shall be a Corporation Secretary who shall be competitively recruited and appointed by the Board on such terms as the Board may, on the advice of the Salaries and Remuneration Commission, determine.

(2) A person qualifies for appointment as the Corporation Secretary of the Agency if the person—

(a) holds a bachelor's degree in law from a university recognized in Kenya;

(b) is an Advocate of the High Court of Kenya;

(c) has at least five years' experience as a corporation secretary or a similar governance role;

(d) is a member in good standing of the Institute of Certified Secretaries of Kenya; and

(e) meets the requirements of Chapter Six of the Constitution.

(3) The Corporation Secretary shall be the Secretary to the Board and shall—

(a) in consultation with the Chairperson of the Board, issue notices for meetings of the Board;

(b) keep in custody, the records of the deliberations, decisions, and resolutions of the Board;

(c) transmit decisions and resolutions of the Board to the Chief Executive Officer for execution, implementation and other relevant action;

(d) provide guidance to the Board on their duties and responsibilities on matters relating to governance;

(e) perform such other duties as the Board may direct.

14. Staff

The Board may appoint such staff as may be necessary for the proper discharge of the functions of the Agency under this Act, upon such terms and conditions of service as the Board may determine upon the advice of the Salaries and Remuneration Commission.

Part III – THE ESTABLISHMENT AND ADMINISTRATION OF THE COMPREHENSIVE INTEGRATED HEALTH INFORMATION SYSTEM

15. Establishment of a comprehensive integrated health information system

(1) There is established a system to be known as the comprehensive integrated health information system which shall be administered by the Agency.

(2) The Agency shall, in consultation with the Cabinet Secretary, establish a framework for administration and management of the system and shall ensure the maintenance of the integrity and security of the system.

(3) The system shall operate as a point of collection, collation, analysis, reporting, storage, usage, sharing, retrieval or archival of data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

16. Components of the System

The system shall comprise of—

(a) an Information and Communication Technology environment which consists of the underlying infrastructure, enterprise service bus, standards, data banks, data exchange, governance, actors and applications, internet enabled environment, and other related components;

(b) data collection, collation, analysis, reporting, storage, usage, sharing, retrieval, or archival;

(c) applications, infrastructure and tools, and best practices that enable access to and analysis of information to improve and optimise decisions and performance;

(d) data quality assurance and audit; and

(e) shared or common resources, including the national health data dictionary, client registry, facility registry, health worker registry, the Kenya Health Enterprise Architecture, product catalogue, interoperability layer, logistics management information services, shared health records, health management information services, and finance and insurance services.

17. Objectives of the system

The main objectives of the system shall be to-

(a) facilitate people-centred quality health service delivery;

(b) facilitate data collection and reporting at all levels;

(c) enable secure health data sharing to ensure timely and informed interfacility health service delivery;

(d) facilitate data processing and use for informed decision-making at all levels, including-

(i) at individual patient level;

(ii) for public health purposes; and

(iii) for resource allocation and management in the health sector;

(e) safeguard the privacy, confidentiality, and security of health data for information sharing; and

(f) serve the health sector and facilitate in a progressive and equitable manner realisation of universal health coverage, to achieve the highest attainable standard of health;

(g) ensure standardisation of health data management; and

(h) facilitate the tracking and tracing of health products and technologies in the country.

18. Technical aspect of the system

(1) The Agency shall adopt relevant internationally accepted standards, procedures, technical details, best practices, and formalities for effective implementation of the system.

(2) The processes and technical aspects of the system shall be guided by the following principles—

(a) confidentiality, security and privacy;

(b) scalability and interoperability;

(c) accuracy, responsiveness and reliability;

(d) efficiency and effectiveness;

(e) redundancy;

(f) transparency;

(g) simplicity and accessibility; and

(h) consistency in use.

Part IV – HEALTH DATA GOVERNANCE

19. Classification of health data

For the purposes of this Act, health data shall be classified into the following categories-

(a) sensitive personal level health data;

(b) de-identified, pseudo-anonymized or anonymized individual-level health data;

(c) administrative data;

(d) aggregate health data;

(e) medical equipment data; and

(f) research for health data.

20. Governing principles.

(1) Health data shall be governed by the following principles-

(a) improvement of client health, safeguard of individuals and communities against harm and violations;

(b) data security throughout the entire data life-cycle;

(c) equity and accountability;

(d) privacy and confidentiality; and

(e) accuracy and reliability.

21. Establishment of health data governance framework

(1) The Cabinet Secretary shall, in consultation with the Director-General, establish a health data governance framework.

(2) Without prejudice to the generality of subsection (1) the Cabinet Secretary shall—

(a) develop guidelines to promote effective use of legacy data including data migration;

(b) establish standards for integration, interoperability and exchange of health data;

(c) ensure regular update and availability of the national health data dictionary for utilization within the system;

(d) establish standards for and conduct routine data quality checks in the system;

(e) ensure the security and accountability of data for the system while promoting appropriate data use and sharing;

(f) provide guidance on the integration and interoperability of all health information systems into the system per set standards; and

(g) require all health data controllers and processors to report designated health data in accordance with ministry of health in the approved and prescribed formats and platforms.

22. Health data custodian

The Agency shall be the custodian for all health data in Kenya.

23. Health data use

(1) The Cabinet Secretary shall ensure that Health data use is used for public good.

(2) The Agency shall provide health data to the Cabinet Secretary for relevant action.

Part V – CONFIDENTIALITY, PRIVACY AND SECURITY OF DATA

24. Security, privacy and disclosure of data in the system

(1) The Cabinet Secretary shall be responsible for the confidentiality, privacy and security of all sensitive personal data held in the system.

(2) Sensitive personal data held in the system shall not be disclosed to a third party unless—

(a) the data subject is unable to give informed consent for the disclosure and such consent is given by a person authorised by the data subject in writing to grant consent;

(b) the disclosure has been authorised by the implementation of written law or the enforcement of a court order;

(c) a health service without informed consent as authorised by written law or court order is being provided;

(d) the data subject is being treated in an emergency situation;

(e) failure to treat the data subject, or a group of people which includes the data subject, would result in a serious risk to public health; or

(f) a delay in providing a health service to the data subject may result in death or irreversible damage to the health of the data subject and the data subject has not expressly, by implication or by conduct refused that service.

(3) The Cabinet Secretary shall be responsible for the privacy of the data held in the system during all the data.

(4) Where the data held in the system data is intended to be used for research and planning, the Cabinet Secretary shall be the data controller for the purposes of section 53 of the Data Protection Act (Cap. 411C).

(5) The Cabinet Secretary shall establish the security measures in the system to protect sensitive personal data including—

(a) personalised authentication and log-in credentials;

(b) role based user rights;

(c) audit trails for all activities within the system;

(d) digital and physical security of the system; and

(e) an encrypted backup that is subject to the security measures herein.

25. Retention and disposal of data in system

(1) Data held in the system shall be maintained for a minimum period of twenty years.

(2) Data held in the system may be maintained for a period exceeding that specified in subsection (1) where—

(a) it is required or authorised by law;

(b) it is authorised by the data subject; or

(c) it is reasonably necessary for a lawful purpose;

(d) for historical, statistical or research purposes.

(3) Where the period for the maintenance of the data held in the system is not extended under subsection (2), the data shall be secured by de-identification, anonymization, pseudo-anonymization or archiving, or establishing such technical and organisational security measures as the Cabinet Secretary may determine to be necessary.

26. Establishment of health data banks

(1) The Cabinet Secretary shall—

(a) establish a national health data bank and designate county health data banks;

(b) store the health data submitted to the system in the national health data bank; and

(c) establish seamless integration and interoperability of the national health data bank with other relevant databases.

(2) The County Executive Committee Member shall—

(a) establish county health databanks;

(b) store the health data submitted to the system in the county health data bank; and

(c) establish seamless integration and interoperability of the county health data bank with other relevant databases and data banks.

(3) The health information databases and data banks referred to in subsections (1) and (2) shall be established at the different levels of healthcare delivery specified under section 25 of the Health Act (Cap. 241).

(4) A data controller shall transmit health data containing sensitive personal data to the national health information data bank and county health information data bank in a secure and encrypted form.

(5) A data controller shall maintain records of the health data containing sensitive personal data transmitted to the national health information data bank and county health information data bank under subsection(4).

27. Use of sensitive personal data

The health data that is contained in a health data bank shall be applied to—

(a) identify a person who needs or is receiving a health service;

(b) provide health services to, or facilitate the care of or treatment of, a person;

(c) identify a health service provider who is providing a health service;

(d) identify a person offering health insurance;

(e) assess and address public health needs;

(f) conduct disease surveillance, research and innovation;

(g) engage in health system planning, management, evaluation or improvement, including health service development, management, delivery, monitoring and evaluation including surveys;

(h) assess the safety and effectiveness of health services; and

(i) continuous enhancement of the system.

28. Responsibilities of health data bank controller

The responsibility of the data controller of a health data bank shall be to—

(a) take reasonable measures to ensure that no agent or the data controller or processor collects, uses, discloses, retains or disposes of sensitive personal data unless it is in accordance with the law; and

(b) remain responsible for any sensitive personal data that is collected, used, disclosed, retained or disposed of by the data controller's or processor's agents, regardless of whether or not the collection, use, disclosure, retention or disposal was carried out in accordance with this Act or other law.

29. Request for information by authorized person

A person authorised by the data controller to enter sensitive personal data into the system shall ensure compliance with section 24(2) of this Act.

30. Disclosure of sensitive personal data deceased persons

(1) A data controller may disclose sensitive personal data about a person who is deceased, or is reasonably suspected to be deceased when—

(a) identifying the person;

(b) informing a person to whom it is reasonable to inform in the circumstances of; or

(c) investigating the cause of death.

(2) A request under subsection (1) shall be made as provided under the relevant law.

31. Consent

(1) A healthcare provider shall ensure that he or she has obtained consent to process sensitive personal data.

(2) Subsection (1) shall not apply where a health service is being provided—

(a) for public health in accordance with the Public Health Act (Cap. 242); and

(b) in compliance with any other statutory requirements.

(3) When processing personal data, a healthcare provider shall—

(a) ensure confidentiality of the information of the client;

(b) provide prompt and accurate data necessary for treatment of the patient;

(c) comply with the duty to notify the data subject in accordance with the Data Protection Act (Cap. 411C);

(4) A data subject who has issued a consent to the use or disclosure of personal data may withdraw their consent at any time by notifying the health care provider.

32. Processing of personal data relating to a minor or a person without capacity

Where a data subject is a minor or for any other reason does not have the capacity to issue informed written consent, the parent, an appointed guardian or next friend of the patient shall, for purposes of section 31 (1), act on behalf of, and in the best interest of, the patient in accordance with the law.

33. Duty to protect sensitive personal data

(1) A data controller shall protect sensitive personal data and adopt reasonable administrative, technical and physical safeguards to ensure the privacy, confidentiality, security, accuracy and integrity of the data.

(2) A data controller shall establish controls that govern persons who may use sensitive personal data and such data shall not be used unless—

(a) the identity of the person seeking to use the information is verified;

(b) the data processor is authorized to use it; and

(c) the proposed use is authorised under this Act.

34. Disposal of health information

The Cabinet Secretary shall develop regulations for the disposal of sensitive personal data.

35. Breach of health data

(1) A person commits an offence if, in relation to health data, the person—

(a) tampers with the data;

(b) abuses a privilege;

(c) discloses inauthentic access to the data;

(d) improperly disposes of unnecessary but sensitive data;

(e) loses data;

(f) steals data; or

(g) shares sensitive personal data to an unauthorised party.

(2) A person who commits an offence under subsection (1) shall be liable, on conviction, to a fine not exceeding one million shillings or to imprisonment for a term not exceeding fifteen years, or to both.

(3) Where a person commits an offence under subsection (1) with respect to sensitive personal data, that person shall be liable, on conviction, to the penalties under section 73 of the Data Protection Act (Cap. 411C).

36. Health Data Portability

(1) Subject to this Act, a person has a right, on request, to examine and receive a copy of his or her personal health information maintained by a data controller.

(2) A request under subsection (1) shall be made in writing to the relevant health facility or health information bank.

(3) The health data controller shall comply with the provisions of section 38 of the Data Protection Act (Cap. 411C) in enabling access and portability of personal health records.

37. Refusal to grant access to sensitive personal data

A person in charge of a health data bank may refuse to grant access to a third party, all or part of a person's sensitive data or health information if it is reasonable to believe that—

(a) access is restricted by a court process, order or judgement;

(b) another law prohibits disclosure;

(c) the information was collected or created in the course of an inspection, investigation or similar procedure not yet concluded;

(d) access may lead to the identification of a person who provided information in the record to the custodian confidentiality was expected; or

(e) access may result in the release of another person's personal health data.

38. Precautions on release of sensitive personal health data

(1) A health data bank and health data controller, before releasing any personal health data to any person, shall—

(a) be satisfied as to the identity of the person making the request; and

(b) take reasonable steps to ensure that any personal health information intended for a person is received only by that person or—

(i) where the data subject is a minor, by a person who has parental authority or by a guardian;

(ii) where the data subject has a mental or other disability, by a person duly authorised to act their guardian or administrator; or

(iii) in any other case, by a person duly authorised by the data subject or by a court order.

(2) A health data controller shall not disclose, for the purpose of market research, personal health information that is contained in a health data information bank.

39. Right to rectification or erasure

A health data bank or a health provider may, upon request by the data subject—

(a) rectify, without undue delay, personal data in its possession or under its control that is inaccurate, outdated, incomplete or misleading; or

(b) erase or destroy, without undue delay, personal data that the health data bank or health provider is no longer authorised to retain, or personal data which is irrelevant, excessive or obtained unlawfully.

Part VI – E-HEALTH SERVICE DELIVERY

40. E-Health as a mode of health service delivery

(1) E-Health shall be a recognized model of health service delivery.

(2) E-Health Services shall be complementary to existing healthcare service delivery modalities.

41. Provision of e-Health services

(1) The e-Health service shall be provided through—

(a) telemedicine;

(b) electronic health records;

(c) m-health;

(d) e-learning;

(e) telehealth; and

(f) any other recognized e-health service.

(2) An entity providing e-health services shall be—

(a) a healthcare provider holding a valid licence issued by a relevant regulatory body;

(b) a healthcare provider holding a valid licence from an equivalent regulatory authority outside Kenya but shall be recognized by the local regulatory authority;

(c) a health facility licenced to offer e-health services by the relevant regulatory body; or

(d) for foreign facilities, be licenced by an equivalent regulatory authority recognized in Kenya.

(3) The Cabinet Secretary shall develop standards and guidelines for the e-Health platform.

42. Principles and objectives of e-health

(1) The e-Health service shall be an integral part of health service delivery to benefit people in a manner that is ethical, safe, secure, reliable, equitable and sustainable.

(2) The objectives of e-Health shall be to—

(a) promote patient-centred health care services;

(b) ensure equitable access to quality health care services using Information and Communication Technology;

(c) promote the integration of e-health into the healthcare system;

(d) facilitate the integration of e-health solutions; and

(e) promote the use of e-health solutions.

43. E-health services

(1) In the provision of e-health services to a client, a healthcare provider shall—

(a) provide the client with all the information for the management of his or her health;

(b) ensure the client can access their own health records where necessary;

(c) ensure the client's data is managed as prescribed in the law;

(d) ensure the highest possible quality of care is delivered;

(e) ensure that the agents of the e-health service provider adhere to the provisions of this Act;

(f) ensure the platform used is interoperable with the system;

(g) ensure that when e-health service delivery involves a minor, the consent of the parent or an appointed guardian is obtained; and

(h) ensure that when e-health service delivery involves a mentally ill person, the consent of an appointed guardian or next friend of the patient is obtained.

(2) The use of e-health service platforms to share the information of a patient including images and lab results for consultation and training shall adhere to the standards prescribed by law.

44. Reporting

In the delivery of e-health services, it shall be the responsibility of the e-health service provider to meet their reporting obligations in accordance with the provisions of this Act.

Part VII – E-WASTE MANAGEMENT

45. E-waste management

(1) The Cabinet Secretary shall—

(a) in consultation with county governments and relevant lead agencies, develop guidelines for the safe handling and disposal of all health sector related e-waste material; and

(b) in consultation with relevant stakeholders, develop an e-waste management system for the health sector.

(2) The e-waste management system referred to in subsection (1) above, shall—

(a) comprise an appropriate mechanism for segregation of e-waste at source, collection, transportation, and processing;

(b) promote reuse and lifetime extension;

(c) promote activities aimed at resource recovery and recycling of e-waste materials into useful products;

(d) embrace the best available technologies and practices in e-waste management; and

(e) promote sustainable models for e-waste management through public-private partnerships.

Part VIII – HEALTH TOURISM

46. Development of guidelines on health tourism

(1) The Cabinet Secretary shall take all necessary measures to safeguard the transfer of a client's medical records to and from facilities outside Kenya.

(2) A data controller, who being a custodian of, and who transfers outside Kenya, biological specimens, heal the images, human tissues and organs of a Kenyan citizen shall ensure confidentiality of personal health information:

Provided that where such transfer is for purposes of health research or post-mortem, the Data controller shall—

(a) provide a report to the Director-General for Health stating the findings;

(b) not share the health information without notifying the Cabinet Secretary; and

(c) seek guidance from ithe Cabinet Secretary in the manner the health information shall be stored, processed and destroyed.

(3) The Cabinet Secretary shall in consultation with the County Governments, and relevant lead agencies, develop guidelines on health tourism.

47. Disclosure of sensitive personal data to organizations outside Kenya.

Personal health information may only be shared to any person outside Kenya for the purposes of health tourism.

Part IX – FINANCIAL PROVISIONS

48. Funds of the Agency

(1) The funds of the Agency shall consist of—

(a) monies appropriated by the National Assembly for the purposes of the Agency;

(b) such monies or assets as may accrue to the Agency in the course of the exercise of its powers or in the performance of its functions under this Act;

(c) such levy fees for services rendered by the Agency;

(d) monies from any other source provided, donated, lent or given as a grant to the Agency; and

(e) any other funds designated for or accruing to the Agency by virtue of the operation of law.

(2) There shall be paid out of the funds of the Agency, all expenditure incurred, administrative expenses or for such other purposes as may be necessary for the discharge of the functions of the Agency in the exercise of its powers or the performance of its functions under this Act.

49. Financial year

The financial year of the Agency shall be the period of twelve months ending on the thirtieth day of June in each year.

50. Annual estimates

(1) Before the commencement of each financial year, the Chief Executive Officer shall cause to be prepared estimates of the revenue and expenditure of the Agency for that year.

(2) The annual estimates shall make provision for all the estimated expenditure of the Agency for the financial year concerned and in particular shall provide for—

(a) payment of salaries, allowances, gratuities, pensions and other charges in respect of the members of the Board and Agency;

(b) maintenance of buildings and grounds of the Agency; and

(c) funding of training, research and development of activities in relation to the organization and functioning of the Agency.

(3) The annual estimates shall be approved by the Board before the commencement of the financial year to which they relate, and shall be submitted by the Chief Executive Officer for tabling in the National Assembly.

(4) The annual estimates, once approved by the Board, shall not be amended before being tabled in the National Assembly.

(5) No expenditure shall be incurred for the purposes of the Agency except in accordance with the annual estimates approved under subsection (3).

51. Accounts and Audit

(1) The Board shall cause to be kept all proper audit books and records of accounts of the income, expenditure, assets and liabilities of the Agency.

(2) The accounts of the Agency shall be audited and reported upon in accordance with the Public Finance Management Act (Cap. 412A) and the Public Audit Act (Cap. 412B).

52. Annual report

(1) At the end of each financial year, the Chief Executive Officer shall prepare an annual report on the activities of Agency.

(2) The annual report shall be submitted for tabling in the National Assembly not later than one month after the submission of the Auditor-General's report.

(3) The annual report shall contain—

(a) the financial statements of the Agency;

(b) a description of the activities and outcomes of functioning of the Agency; and

(c) any other information that the Agency may consider relevant.

53. Bank account

The Chief Executive Officer may, in accordance with the law relating to the management of public finance, open bank accounts on behalf of the Agency with the approval of the Board and the National Treasury and shall, as the accounting officer, be responsible for the proper management of the finances of the Agency.

54. Investment of Funds

(1) All monies in the Agency which are not immediately required to be applied for the purposes of this Act shall be invested—

(a) in such investment in a reputable bank on the advice of the Central Bank of Kenya, being an investment in which trust funds, or part thereof, are authorized by law to be invested; and

(b) in government securities as may be approved by the National Treasury.

(2) All investments made under this section shall be held in the name of the Agency.

Part X – MISCELLANEOUS PROVISIONS

55. Protection from personal liability

No matter or thing done by the Chairperson, a Board member, or any officer, employee or agent of the Agency shall, if the matter or thing is done in good faith and for the purposes of executing any provisions of this Act, render the Chairperson, Board member, or any officer, employee or agent of the Agency or any person acting under the direction of those persons personally liable for any action, claim or demand arising from the same.

56. Conflict of interest

(1) The Chairperson or a member of the Board, conflict of who has a direct or indirect personal interest in a matter being considered or to be considered by the Board, shall as soon as reasonably practicable after the relevant facts concerning the matter have come to their knowledge, disclose the nature of such interest.

(2) A disclosure of interest made under subsection (1) shall be recorded in the minutes of the meeting and the chairperson or member shall not take part in the consideration or discussion on or vote during any deliberations on the matter.

(3) A person who fails to make the requisite disclosure under this section commits an offence.

(4) A member of the Board shall recuse themselves from proceedings before the Board in which they have apparent or perceived conflict of interest.

57. Confidentiality

(1) A member of the Board or staff of the Agency may not without the consent in writing given by, or on behalf of, the Board, publish or disclose to any person other than in the course of the person's duties, the contents of any document, communication or information which relates to, and which has come to the person's knowledge in the course of the person's duties under this Act.

(2) The limitation on disclosure referred to under subsection (1) shall not be construed to prevent the disclosure of criminal activity by a member of the Board or staff of the Agency.

58. Duty to cooperate

A person responsible for a matter in question before the Board shall co-operate with the Board and shall in particular—

(a) respond to any inquiry made by the Board;

(b) furnish the Board with a report in respect of the question raised; and

(c) provide any other information that the Board may require in the performance of its functions under the Constitution, this Act or in any other written law.

59. Offences

(1) A person who—

(a) obstructs, hinders or threatens a member, an officer, employee or agent of the Board acting under this Act;

(b) disregards an order of the Board;

(c) submits false or misleading information to the Board; or

(d) makes a false representation to, or knowingly misleads a member, an officer, employee or agent of Board acting under this Act,

commits an offence and is liable, on conviction, to a fine of not less than one million shillings or to imprisonment for a term of not less than two years, or to both.

(2) Any person who violates or fails to comply with any provision of this Act for which no other penalty is provided, commits an offence, and is liable on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding two years, or to both.

60. Regulations

The Cabinet Secretary may, in consultation with the Agency and the county governments, develop regulations providing for—

(a) health information management policies and procedures;

(b) the use of e-Health applications and technologies, medical devices and innovations;

(c) data quality and data protection audits; and

(d) the establishment and implementation of the data exchange component as per the Kenya Health Enterprise Architecture.

61. Compliance to the Data Protection Act (Cap. 411C)

Any person processing personal data under this Act shall comply with the Data Protection Act (Cap. 411C).

62. Transitional provision

A person, who being a data controller or data processor of health data or who has been handling health information before the commencement of this Act, shall, within six months of the commencement of this Act, comply with the requirements of this Act.

SCHEDULE [s. 9]

CONDUCT OF BUSINESS AND AFFAIRS OF THE BOARD

1. Meetings

   The Board shall meet as often as may be necessary for the dispatch of its business but there shall be at least four meetings of the Board in any financial year.

2. Election of vice-chairperson

   At the first meeting, the Board elects chairperson amongst their number who shall be a person of opposite gender.

3. Time and place of meetings

   A meeting of the Board shall be held on such date time and place of and at such time and place as the Board may determine.

4. Special meetings

   The chairperson shall, on the written application of one-third of the members, convene a special meeting of the Board.

5. Quorum.

   The quorum for the conduct of business at a meeting of the Board shall be the chairperson and any four members.

6. Voting

   The Chairperson shall preside every meeting of the Board at which the chairperson shall be present and in the absence of the chairperson at a meeting, the vice chairperson shall preside and in the absence of both the chairperson and the vice-chairperson, the members present shall elect one of their number who has, with respect to that meeting and the business transacted there at, have all the powers of the chairperson.

7. Decisions of the Board

   Unless a unanimous decision is reached, a decision on any matter before the Board shall be by concurrence of a majority of all the members present and voting at the meeting.

8. Vacancy

   Subject to paragraph 5, no proceedings of the Board shall be invalid by reason only of a vacancy among the members thereof.

9. Signification of instruments and decisions of the Board

   Unless otherwise provided by or under any law, all instruments made by and decisions of the Board shall be signified under the hand of the Chairperson.

Transform Health Kenya is a multi-stakeholder coalition advocating for an enabling environment that ensures **equitable, inclusive and sustainable digital health transformation** for all.

ADVOCATE

Influencing policies and laws that protect data and promote digital health for all.

COLLABORATE

Bringing together diverse partners to drive collective action and strengthen health systems.

TRANSFORM

Supporting responsible use of data and technology to achieve UHC in the digital age.