SPECIAL ISSUE

Kenya Gazette Supplement No. 192 (Acts No. 15)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

ACTS, 2023

NAIROBI, 19th October, 2023

CONTENT

Act—

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

THE DIGITAL HEALTH ACT

No. 15 of 2023

Date of Assent: 19th October, 2023

Date of Commencement: 2nd November, 2023

ARRANGEMENT OF SECTIONS

Section

THE DIGITAL HEALTH ACT, 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

ENACTED by Parliament of Kenya as follows—

PART I— PRELIMINARY

Short title.

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

Interpretation.

2. 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, 2019; No. 24 of 2019.

"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, 2019; No. 24 of 2019.

"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 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 determine 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, 2017; No. 21 of 2017.

"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, 2017; No. 21 of 2017.

"health care services" has the meaning assigned to it under the Health Act, 2017; No. 21 of 2017.

"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, 2017; No. 21 of 2017.

"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, 2019; No. 24 of 2019.

"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 videoconferencing, 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.

Objects of the Act.

3. 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 life cycle;

(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.

Guiding principles.

4. 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

Establishment of the Digital Health Agency.

5. (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.

Functions of the Agency.

6. 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 for 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.

Powers of the Agency.

7. (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, 2015: No. 33 of 2015.

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.

Board of Directors.

8. (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.

Conduct of business and affairs of the Board.

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

Committees of the Board.

10. (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.

Chief Executive Officer.

11. (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.

Qualification for appointment as Chief Executive Officer.

12. (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 re-appointment for one further term of three years.

Corporation Secretary.

13. (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; and

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

Staff.

14. 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

Establishment of an integrated health information system.

15. (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.

Components of the System.

16. 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.

Objectives of the system.

17. 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 use;

(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.

Technical aspect of the system.

18. (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

Classification of health data.

19. 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.

Governing principles.

20. (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.

Establishment of health data governance framework.

21. (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.

Health data custodian.

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

Health data use.

23. (1) The Cabinet Secretary shall ensure that Health data 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

Security, privacy and disclosure of data in the system.

24. (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 life cycle stages.

(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, 2019. No. 29 of 2019.

(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.

Retention and disposal of data in system.

25. (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.

Establishment of health data banks.

26. (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 data banks;

(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, 2017.

No. 21 of 2017.

(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).

Use of sensitive personal data.

27. 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.

Responsibilities of health data bank controller.

28. 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.

Request for information by authorized person.

29. 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.

Disclosure of sensitive personal data of deceased persons.

30. (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.

Consent.

31. (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; and Cap. 242.

(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, 2019; No. 24 of 2019.

(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.

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

32. 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.

Duty to protect sensitive personal data.

33. (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.

Disposal of health information.

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

Breach of health data.

35. (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, 2019. No. 24 of 2019.

Health Data Portability.

36. (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 in enabling access and portability of personal health records. No. 24 of 2019.

Refusal to grant access to sensitive personal data.

37. 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 in circumstances in which confidentiality was expected; or

(e) access may result in the release of another person's personal health data.

Precautions on release of sensitive personal health data.

38. (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 as 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.

Right to rectification or erasure.

39. 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

e-Health as a mode of health service delivery.

40. (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.

Provision of e-Health services.

41. (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.

Principles and objectives of e-Health.

42. (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.

E-health services.

43. (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.

Reporting.

44. 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

E-waste management.

45. (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

Development of guidelines on health tourism.

46. (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, health 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 the 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.

Disclosure of sensitive personal data to organizations outside Kenya.

47. Personal health information may only be shared to any person outside Kenya for the purposes of health tourism.

PART IX—FINANCIAL PROVISIONS

Funds of the Agency.

48. (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.

Financial year.

49. The financial year of the Agency shall be the period of twelve months ending on the thirtieth day of June in each year.

Annual estimates.

50. (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).

Accounts and audit.

51. (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, 2012 and the Public Audit Act, 2015. No. 18 of 2012. No. 34 of 2015.

Annual report.

52. (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.

Bank account.

53. 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.

Investment of Funds.

54. (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

Protection from personal liability.

55. 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.

Conflict of interest.

56. (1) The Chairperson or a member of the Board, 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.

Confidentiality.

57. (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.

Duty to cooperate.

58. 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.

Offences.

59. (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.

Regulations.

60. 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.

Compliance to the Data Protection Act, 2019.

61. Any person processing personal data under this Act shall comply with the Data Protection Act, 2019.

Transitional provision.

62. 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

Meetings.

1. 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.

Election of vice-chairperson.

2. At the first meeting, the Board elects a vice-chairperson amongst their number who shall be a person of opposite gender.

Time and place of meetings.

3. A meeting of the Board shall be held on such date and at such time and place as the Board may determine.

Special meetings.

4. The chairperson shall, on the written application of one-third of the members, convene a special meeting of the Board.

Quorum.

5. The quorum for the conduct of business at a meeting of the Board shall be the chairperson and any four members.

Voting.

6. The Chairperson shall preside at 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 thereat, have all the powers of the chairperson.

Decisions of the Board.

7. 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.

Vacancy.

8. Subject to paragraph 5, no proceedings of the Board shall be invalid by reason only of a vacancy among the members thereof.

Signification of instruments and decisions of the Board.

9. 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.