

THE REPUBLIC OF KENYA

LAWS OF KENYA

THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT PROCEDURES) REGULATIONS, 2025

NO. 76 OF 2025

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

The Digital Health (Health Information Management Procedures) Regulations, 2025

Legal Notice 76 of 2025

Legislation as at 11 April 2025

By Kenya Law and Laws.Africa. Share widely and freely.

www.kenyalaw.org | info@kenyalaw.org

FRBR URI: /akn/ke/act/ln/2025/76/eng@2025-04-11

There is no copyright on the legislative content of this document.

This PDF copy is licensed under a Creative Commons Attribution NonCommercial ShareAlike 4.0 License (CC BY-NC-SA 4.0). This license enables reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms. CC BY-NC-SA includes the following elements:

- BY: credit must be given to the creator.
- NC: Only noncommercial uses of the work are permitted.
- SA: Adaptations must be shared under the same terms.

Share widely and freely.

The Digital Health (Health Information Management Procedures) Regulations, 2025 (Legal Notice 76 of 2025)

Contents

Part I – PRELIMINARY 1

1. Citation 1

2. Interpretation 1

Part II – MANAGEMENT OF HEALTH INFORMATION 3

4. Notification of registration 3

5. Data custodianship 3

6. Information Security Operations Centre 4

7. Capability of an Information Security Operations Centre 4

8. Health Sector Information Security Operations Centre 4

9. Health Facility Information Security Operations Centre 5

10. Record of health data processors 6

11. Notification of a health data breach 6

12. Security of sensitive personal data 6

13. Health data privacy 8

14. Restriction on access 8

15. Archiving of health data 8

16. Migration of health data 9

17. Access to health data from the system 9

18. Access to health data by a data subject 10

19. Health data sharing 10

20. Correction of health personal data 11

21. Use of sensitive health data 11

22. Disclosure of sensitive personal data of deceased persons 12

23. Sensitive personal data in emergencies 12

24. Disclosure of personal health data for market research 12

25. Consideration before disclosure 12

26. Obligations of a health data controller 12

Part III – PROCEDURE FOR LODGING, ADMISSION AND RESPONSE TO COMPLAINTS 13

27. Lodging of a complaint 13

28. Register of complaints 13

29. Admission of a complaint 13

30. Investigation of a complaint 13

31. Discontinuation of a complaint 14

32. Withdrawal of a complaint 14
33. Outcome of investigations 14
34. Appeals 14
35. Exemption of complaints related to personal data 14
Part IV – PROVISION OF E-HEALTH AND CERTIFICATION 15
36. Certification of digital health solutions 15
37. E-health 15
38. Application for certification 15
39. Considerations for certification 16
40. Testing 16
41. Validity of a certificate 17
42. Monitoring of compliance by the Agency 17
43. Ad hoc audit 17
44. Revocation of certification 18
45. Transitional and saving provisions 18
FIRST SCHEDULE (r. 11(1)(2)(a)) 18
SECOND SCHEDULE (r.21(2)(b), r.38(3)(h)) 28

DIGITAL HEALTH ACT

THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT PROCEDURES) REGULATIONS, 2025

LEGAL NOTICE 76 OF 2025

Commenced on 11 April 2025

Part I – PRELIMINARY

1. Citation

These Regulations may be cited as the Digital Health (Health Information Management Procedures) Regulations, 2025.

2. Interpretation

In these Regulations, unless the context otherwise requires—

"Act" means the Digital Health Act, 2023 (No. 15 of 2023);

"Agency" means the Digital Health Agency established under section 5 of the Act;

"archiving" means the transfer of health data to a less frequently used storage medium;

"authorized person" means a person who is expressly permitted by a health data controller or a data subject to access health data;

"certification" means attestation that fulfilment or compliance with the requirements specified by the Agency has been demonstrated in relation to an e-health application or technology;

"Certification Framework" means the structured approach for defining, documenting and certifying operations, requirements and compliance of a digital health solution with the System such that the System can perform its intended functions reliably, securely and in accordance with these Regulations;

"Chief Executive Officer" means the Chief Executive Officer of the Agency appointed under section 11 of the Act;

"Comprehensive Integrated Health Information System" means the Comprehensive Integrated Health Information System established under section 15 of the Act;

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

"data quality protocols" means the procedures used to ensure that data is accurate, consistent, reliable and fit for its intended use;

"data quality standards" means a criteria used to ensure that data is accurate, consistent, reliable and fit for its intended use;

"de-identified" 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;

“digital health solution” includes a digital health application, intervention, initiative, digital health technology infrastructure including telehealth systems, electronic health information systems and provision of education and training support for e-Health initiatives;

“digital health solution provider” means a person who provides a digital health solution to a health data controller or a health data processor for purposes of providing healthcare services;

“e-health application or technology” includes a digital health solution that provides healthcare services;

“emergency treatment” means the necessary immediate health care that must be administered to prevent death or worsening of a medical situation;

“health information management” means the policies, procedures and structures for processing of health data in the provision of healthcare services;

“healthcare provider” means a person who provides healthcare services and includes a healthcare professional;

“healthcare services” means the prevention, promotion, management or alleviation of disease, illness, injury, and other physical and mental impairments in individuals, delivered by health care professionals through the health care system’s routine health services, or its emergency 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 processor” means a person, public authority, agency or other body who is an authorised worker to process health data;

“health facility” means the whole or part of a public or private institution, building or place whether for profit or not that is operated to provide inpatient or outpatient treatment, diagnostic or therapeutic intervention, nursing, rehabilitative, palliative, convalescent, preventative or other health service;

“Health Facility Information Security Operations Centre” includes the capability that encompasses technology, tools and Information Security experts organized to protect, monitor, detect, analyse, respond and report on threats in the health facility;

“Health Sector Information Security Operations Centre” includes the capability that encompasses technology, tools and Information Security experts organized to protect, monitor, detect, analyse, respond and report on threats in the Health Sector

“Information Security Operations Centre” means the capability that encompasses technology, tools and a team of information security experts organized to protect, monitor, detect, analyse, respond and report on information security incidents and threats;

“legacy data” means information that is stored in formats, technologies or systems that are difficult to access or that have become outdated, obsolete or were developed before the adoption of national standards;

“office of the Data Protection Commissioner” means the office of the Data Protection Commissioner established under section 5 of the Data Protection Act (Cap. 411C);

“personally identifiable information” means information that may be used to uniquely identify, contact or locate an individual, or may be used with other sources to uniquely identify a person;

“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;

“System” means the comprehensive integrated health information system established under section 15 of the Act;

“third party” means a 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; and

“unauthorized access” means the illegitimate and unsanctioned entry, retrieval and processing of data within a system by an individual or an entity that has not been granted explicit permission and privileges by a health data controller.

3. Purpose of the Regulations

The purpose of these Regulations is to—

(a) ensure safe management of health information; and

(b) provide for e-health through e-health applications and technologies.

Part II – MANAGEMENT OF HEALTH INFORMATION

4. Notification of registration

(1) A health data controller or health data processor shall upon registration with the Office of the Data Protection Commissioner, notify the Agency in writing of such registration indicating the category of health data held by the health data controller or health data processor within seven days from the date of registration as a data controller or data processor.

(2) Upon receipt of the notice under subregulation (1), the Agency shall enter the details of the health data controller and health data processor in the register of health data controllers and health data processors.

5. Data custodianship

(1) The Agency shall as the custodian for all health data in Kenya—

(a) maintain a register of all health data controllers and health data processors;

(b) maintain a record of health data held by the health data controllers and health data processors;

(c) ensure that health data controllers submit health data to the Agency in the applicable format;

(d) maintain the National Health Data Bank;

(e) provide access to the relevant health data to authorized health data controllers and health data processors in the applicable manner;

(f) retain health data held in the System for a minimum of twenty years or as specified in the Act;

(g) implement security measures in the management of the System including firewalls, encryption and access controls to protect health data from unauthorized access, modification or disclosure;

(h) maintain a public portal for health data controllers and health data processors to access templates and standard operating procedures on the management of health data; and

(i) maintain a public portal for select aggregate health data published in the set formats for easy consumption by the relevant stakeholders including the members of public.

(2) The Agency shall utilize the existing relevant government and third party databases in the performance of its functions for purposes of enhancing access and utilization of healthcare services.

6. Information Security Operations Centre

The Agency shall coordinate the collection and analysis of information security threats through the Health Sector Information Security Operations Centre and the Health Facility Information Security Operations Centres and report to the Cabinet Secretary.

7. Capability of an Information Security Operations Centre

The Information Security Operations Centre under regulation 6, shall have the following capabilities—

(a) real time event monitoring, analysis, log collection and aggregation;

(b) alert system;

(c) information security specialists organized to prevent, detect, analyse and respond to threats;

(d) asset inventory;

(e) vulnerability management;

(f) network detection and response;

(g) end point detection and response;

(h) intrusion detection;

(i) malware analysis and testing;

(j) threat prevention, monitoring and detection;

(k) incidence response and management; and

(l) threat intelligence platform.

8. Health Sector Information Security Operations Centre

(1) A Health Sector Information Security Operations Centre shall be the health sector focal point for monitoring, detecting, preventing, responding, investigating and attribution of information security threats in the health sector.

(2) The Health Sector Information Security Operations Centre shall—

(a) monitor, detect, prevent, respond and investigate information security threats, that are specific to the health sector;

(b) have visibility of threats and incidents that occur in the health facility information security operations centre;

(c) have the requisite capability to monitor, detect, prevent, respond and investigate information security threats within the health sector;

(d) receive real-time information on information security threats and incidents from the health facility information operation centre;

(e) promote threat and information sharing;

(f) network detection and response;

(g) promote incidence response coordination;

(h) utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities;

(i) develop and implement information security policies and procedures;

(j) provide information security awareness training;

(k) monitoring logging and threat intelligence;

(l) perform information security and vulnerability assessments;

(m) deploy endpoint detection and response solutions to monitor and detect information security threats;

(n) undertake information security administration by configuring and maintaining security tools;

(o) define and implement of role-based user rights;

(p) execute and maintain audit trails for activities in the system;

(q) implement digital and physical security measures to the system;

(r) ensure secure and encrypted backups and restoration procedures;

(s) conduct system asset inventory; and

(t) convene information security meeting, colloquium, webinar, workshops, or other consultative platforms for Information security Operations Centres in order to—

(i) facilitate consultations, co-ordination and collaboration in the implementation of relevant policies and laws;

(ii) make recommendations to the Cabinet Secretary aimed at improving Information security in the health sector;

(iii) promote data and information sharing including sharing of experiences, best practices, on emerging issues on Information security; and

(iv) create awareness on information security.

(3) A Health Sector Information Security Operations Centre may create sub national information security hubs to assist it in discharging the functions specified under subregulation (2).

9. Health Facility Information Security Operations Centre

(1) A Health Facility Information Security Operations Centre shall be responsible for monitoring, detecting, preventing, responding and investigating of information security threats, in a health facility.

(2) Despite the generality of subregulation (1), a Health Facility Information Security Operations Centre shall—

(a) provide real-time information on cyber threats and incidents to the Health Sector Information Security Operations Centre;

(b) have the requisite capability to detect, monitor, prohibit, prevent, respond and investigate cyber threats, computer and cybercrimes in the concerned organization;

(c) be responsible for incidence detection, analysis and response in the health facility;

(d) report to the Health Sector Information Security Operations Centre all information security incidents detected in the health facility;

(e) undertake capacity building programs, research and development activities on information security threats and incidents in the health facility; and

(f) utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities.

10. Record of health data processors

A health data controller shall maintain a record of health data processors that it has engaged and provide role-based access to the health data processors in the System.

11. Notification of a health data breach

(1) A data subject, health data controller, health data processor or a third party may report any health data breach to the Chief Executive Officer in Form HMIS 1 set out in the First Schedule.

(2) A health data controller of a digital health solution shall—

(a) in the case of a breach, notify the Chief Executive Officer of the breach within forty-eight hours of becoming aware of such breach, in Form HMIS 1 set out in the First Schedule; and

(b) within seventy-two hours of the notification of breach, notify the Chief Executive Officer of the—

(i) corrective measure taken;

(ii) mitigation action adopted; and

(iii) timelines for the rectification of the breach.

(3) A health data controller or a health data processor who fails to notify the Chief Executive Officer of a health data breach in accordance with subregulation (2), commits an offence and is liable, on conviction to the penalty specified under section 35(2) and (3) of the Act, where applicable.

12. Security of sensitive personal data

Sensitive personal data shall be secured in accordance with security measures in the System established by the Cabinet Secretary under section 24(5) of the Act, which shall—

(a) ensure that personalized authentication and log-in where—

(i) health data controllers shall log and monitor login attempts and password changes for suspicious activity;

(ii) authorised users shall have unique usernames and strong passwords meeting minimum length, complexity and non-dictionary requirements;

(iii) there is limitation of the number of failed logins;

(iv) user accounts shall adopt multi-factor authentication; and

(v) biometric authentication methods including fingerprint scanners or iris recognition may be used as an optional secondary authentication factor;

(b) adopt role-based system user rights where—

(i) health data controllers shall define clear user roles with specific access permissions to different data types and functionalities within the System;

(ii) the principle of least privilege shall be applied granting access only to the minimum data required for the role of each user;

(iii) health data controllers shall review access permissions and update them regularly to reflect changes in user roles and responsibilities;

(iv) superuser or administrator access is restricted to a limited number of authorized personnel and subject to controls;

(v) a user account assigned to a healthcare provider are linked to his or her identifier as a health data controller or health data processor issued by the System; and

(vi) the user accounts of clients are inked to their national identity documents,

(c) conduct audit trails within the System where—

(i) health data controllers shall log all user actions and data access within the System in a secure and tamper-proof manner including timestamps, user IDs and actions performed;

(ii) audit logs are retained for minimum of twenty years;

(iii) access to audit logs is restricted to authorized personnel for purposes of the security investigations and regulatory compliance; and

(iv) health data controllers shall review audit logs on a quarterly basis to identify potential security incidents or suspicious activity patterns;

(d) ensure digital and physical security of the System where—

(i) health data controllers shall implement secure network infrastructure with firewalls, intrusion detection systems and vulnerability assessments;

(ii) health data controllers shall regularly update software and firmware on all System components to address security vulnerabilities;

(iii) health data controllers shall encrypt data at rest and in transit using strong encryption algorithms;

(iv) health data controllers shall implement physical security measures for hardware and data storage devices including restricted access and security cameras;

(v) health data controllers shall conduct user training on data security practices and awareness of potential threats and phishing attacks;

(vi) health data controllers shall implement breach notification procedures to individuals in case of unauthorized data access in accordance with the Data Protection Act (Cap 411C);

(vii) health data controllers shall implement an Incident Response plan outlining procedure for identifying, reporting and mitigating security incidents; and

(viii) the Agency shall conduct and promote regular security audits and penetration tests to identify and address System vulnerabilities; and

(e) provide encrypted backup where—

(i) health data processors and health data controllers shall regularly backup all System data and store backups in a secure location with encryption at rest and in transit;

(ii) health data processors and health data controllers shall restrict backup data to authorized personnel for disaster recovery purposes; and

(iii) backup systems shall be subject to the same security measures as the System including encryption, access controls and audit logging.

13. Health data privacy

(1) The Agency shall ensure health data in the System is protected throughout the health data life-cycle.

(2) A person or entity shall not access health data unless authorized by the client or the health data controller to whom the data relates to.

14. Restriction on access

Where a health data controller is no longer allowed to access the health data, the health data controller shall—

(a) extract a copy of all their data in the applicable format and transmit the data to the Agency;

(b) notify the respective clients and health data processors who had access to the health data, of the discontinued access to health data;

(c) notify the Agency in writing within seven days from the date of the health data controller was denied access of their data; and

(d) permanently delete all copies of the data in the health data controller's possession.

15. Archiving of health data

(1) The Agency shall archive health data where—

(a) a data subject is dead and such death has been confirmed by a copy of a death certificate or a decree declaring the presumption of the death of the data subject; and

(b) a heath data record of the data subject has been inactive for a minimum of twenty years.

(2) The twenty-year period specified under section 25(1) of the Act for the retention and archival of health data held in the System shall commence from the date of the last update of a health data record of the data subject who is presumed to be living.

(3) A data subject shall receive an electronic notification on the twentieth year on the archiving of their health data and unless the data subject expressly requests for the halting of the process in writing, the health data shall be archived after seven days from the date of the notice to archive health data.

(4) Heath data of a deceased data subject shall, upon confirmation of the death of a data subject be archived after the lapse of a period of eight years from the date of confirmation of the death of that data subject.

(5) A health data controller who intends to stop dealing with health data shall ensure that the digital health solution that the health data controller has been utilizing shall archive all health data in the possession of that health data controller in the County Health Data Bank.

(6) All health data archived under this regulation shall retain the minimum data elements as specified in the Shared Health Record.

(7) The Agency shall, before health data is archived, remove all information that may be used to identify, contact or locate a data subject or which may be used with other sources to uniquely identify the data subject.

(8) The health data controller shall—

(a) maintain a record of the archiving process and data sets; and

(b) submit a copy of the record to the Agency.

(9) A person may access or recall archived health data by making a request to the Agency or respective County Government and that person shall access archived health data in the manner set out in the Kenya Health Data Governance Framework.

(10) The systems of archiving health data shall be subject to security measures as set out in the prevailing information security standards issued by the Board of the Information and Communication Technology Authority established under paragraph 6 (1) of the Information and Communications Technology Authority Order (L. N No. 183/2013) and other relevant laws.

16. Migration of health data

(1) An institution that immediately before the coming into force of these Regulations was using a digital health solution for the management of health data shall, within twenty-four months upon the operationalization of the County Health Data Banks, transfer its legacy data to the County Health Data Banks.

(2) The Agency shall manage the migration of legacy data to the System in accordance with the applicable protocols and formats.

(3) A health data controller or health data processor who has control of legacy data shall, within one year from the coming into force of these Regulations —

(a) migrate the data to compliant systems or the National Data Health Bank; and

(b) store or archive the data as required under the Act and these Regulations.

(4) A health data controller or health data processor who fails to migrate legacy data as required under this regulation, commits an offence and shall on conviction be liable to the penalty specified under section 59(2) of the Act.

17. Access to health data from the system

(1) A person may request for health data in the System in Form HMIS 2 set out in the First Schedule.

(2) A request for access under subregulation (1) shall be granted where the requester complies with data sharing requirements as may be defined by the health data controller or the Agency.

(3) A request for health data containing personally identifiable information shall be accompanied by—

(a) the execution of a data sharing agreement between the health data controller and the person making the health data request; and

(b) consent by the data subject to whom the requested health data relates to and such consent shall be demonstrated by a data subject in writing and the data subject shall specify that they understand what they are doing.

(4) A request for health data in the System for research purposes shall be accompanied by—

(a) an approval issued by a duly registered Institutional Review Board established under section 3 of the National Commission for Science, Technology and Innovation Act (Cap. 511);

(b) a licence issued by National Commission for Science, Technology and Innovation established under section 3 of the Science, Technology and Innovation Act (Cap. 511); and

(c) an approval from the health data controller, where applicable—

(i) in the case of health data in the National Health Data Bank, the Cabinet Secretary; or

(ii) in the case of health data in the County Health Data Bank, the respective County Executive Committee Member.

(5) Upon receipt of the application under subregulation (4), Agency shall, within thirty days from the date of receipt of the request, consider the request for health data and may—

(a) grant access, if the request meets the requirements specified under this regulation; or

(b) deny access, where the request does not meet the necessary requirements and communicate the reasons for denial to the applicant within seven days from the date if the decision.

(6) A person whose request for health data under this regulation is denied, may make an application for review of denial to the Agency within seven days from the date of the decision.

(7) A person aggrieved by the decision of the Agency under subregulation (6), may appeal to the High Court.

18. Access to health data by a data subject

(1) A data subject may have access to health data from the patient portal.

(2) A data subject under subregulation (1) may in a secure manner, share the Shared Health Record or file an extract of their Shared Health Record through the patient portal in accordance with these Regulations.

(3) Where a data subject seeks healthcare outside Kenya, the Agency shall grant the data subject access to their health data and access shall include—

(a) setting an expiry date;

(b) creating an access code or password; and

(c) limiting the number of times that the access link may be accessed.

(4) On the completion of healthcare services sought outside Kenya, a client under this regulation shall, with the guidance of the referring healthcare provider, update their medical record to reflect the treatment sought or any other healthcare service received outside the country.

(5) A data subject shall take the necessary precautionary measures to prevent the access of their Shared Health Record by an unauthorized person.

(6) The Agency shall monitor and track the transfer of medical records, biological specimens, health images, human tissues and organs of a client outside Kenya through the System.

19. Health data sharing

(1) A person may make a request for health data in writing to the Agency.

(2) A request under subregulation (1) shall be accompanied by a statement on the purpose for which the data is requested.

(3) Upon receipt of the of the request under subregulation (1), the Agency shall undertake verification mechanisms to determine whether the request for data meets the requirements of this regulation.

(4) Where the Agency is satisfied with the verification under subregulation (3), the Agency shall communicate its decision to the applicant within forty-eight hours from the date of the decision.

(5) The Agency may—

(a) decline the request for health data; or

(b) approve the request for health data and—

(i) require the applicant to enter into the data sharing agreement with the data controller; and

(ii) grant the applicant access level to the system.

(6) Where health data is shared in accordance with this regulation, the health data shall—

(a) be used for the purpose for which the health data was requested;

(b) be used for a period specified in the authorization by the health data controller;

(c) be used in accordance with the data sharing agreement;

(d) not be shared with a third party.

(7) For avoidance of doubt, shared health data shall be used for the initial specific purpose approved by the Agency under this regulation and a fresh approval shall be sought for any further processing of the requested health data.

(8) The Agency shall carry out periodic audits to monitor compliance with access levels provided under this regulation and any recommendations that may have been provided by Agency.

(9) Subject to section 25 of the Data Protection Act (Cap. 411C), the Agency may, upon request in writing, provide, receive, exchange, transmit or share personal data collected by a data controller, data processor, third party or a data subject.

(10) The Agency shall, in providing, receiving, exchanging, transmitting or sharing personal data from one data controller or data processor to another, determine the—

(a) purpose for which the personal data is required;

(b) means of providing, receiving, exchanging or sharing personal data including access to, and integration to the information systems of the data controller, data processor or third party; and

(c) safeguards to be put in place to secure personal data from unlawful disclosure.

20. Correction of health personal data

(1) A data subject may in writing request the health data controller to correct inaccurate, outdated, incomplete or misleading health data.

(2) The request under subregulation (1) shall specify the health personal data that is to be corrected and how such information is inaccurate, out of date, incomplete or misleading.

(3) Upon receipt of the request under subregulation (1), a health data controller shall, correct the health data of the data subject, within seventy-two hours.

21. Use of sensitive health data

(1) A health data controller shall ensure that personal data used for purposes specified under section 27(f), (g), (h) and (i) of the Act is accessed in a de-identified form.

(2) A person may access health data in the System for purposes specified under section 27(f), (g), (h) and (i) of the Act by—

(a) making a request in writing to the Agency; and

(b) paying the fees specified in the Second Schedule.

(3) The Agency shall consider a request under subregulation (2) and communicate its decision to the applicant within fourteen days from the date of the request.

(4) A person who uses sensitive personal data contrary to these Regulations, commits an offence and shall on conviction be liable to the penalty specified under section 35 of the Act.

(5) In making a determination under subregulation (3), the Agency shall be guided by the provisions of the Fair Administrative Action Act (Cap. 7).

22. Disclosure of sensitive personal data of deceased persons

(1) A person may request a health data controller for disclosure of sensitive personal data of a deceased person.

(2) A health data controller may grant a request under subregulation (1), where the sensitive personal data of the deceased is requested for the purpose of—

(a) identifying a person;

(b) informing the next of kin in the circumstances; or

(c) investigating a cause of death.

(3) A person aggrieved by a decision of the heath data controller under this regulation may within seven days from the date of the decision of the heath data controller appeal to the Agency.

(4) A person aggrieved by the decision of the Agency under this regulation may appeal to the High court.

23. Sensitive personal data in emergencies

A request for access to personal sensitive data for purposes of emergency treatment shall be granted—

(a) through a multi-factor authentication process governed by the policy of the health data controller of the digital health solution; and

(b) where the health data controller keeps an auditable log of the access granted.

24. Disclosure of personal health data for market research

A health data controller who discloses personal health data for market research purposes, commits an offence and shall, on conviction, be liable to the penalty specified under section 59 (2) of the Act.

25. Consideration before disclosure

A health data controller shall, before disclosing personal health data—

(a) verify the identity of the requester of the data by—

(i) requiring official identification documents;

(ii) verifying the credentials of the requester electronically; or

(iii) conducting other appropriate identification checks;

(b) ensure confidentiality of the data and access control by taking reasonable steps to ensure that the intended recipient receives the requested data where—

(i) in the case of a minor, the data shall be received by a parent or guardian;

(ii) in the case of a person with disabilities, the data shall be received by the person authorized to act as the guardian or administrator of the person with disability; and

(iii) in any other case, personal data shall be received by a person explicitly authorized by the client in writing or by a court order.

26. Obligations of a health data controller

A health data controller shall—

(a) develop a health data-sharing plan;

(b) store health data in a format that allows sharing;

(c) share health data in accordance with these Regulations and the Act; and

(d) maintain a log of all health data requests.

Part III – PROCEDURE FOR LODGING, ADMISSION AND RESPONSE TO COMPLAINTS

27. Lodging of a complaint

(1) A data subject or any person aggrieved on any decision under the Act and these Regulations may lodge a complaint with the Agency.

(2) A complaint under subregulation (1) may be lodged in Form HMIS 3 set out in the First Schedule.

(3) A complaint under subregulation (1) may be lodged through mail or electronic means, including email, web posting or a complaint management information system.

(4) A complaint under subregulation (1) may be lodged by—

(a) a complainant; or

(b) a person acting on behalf of the complainant.

(5) The Agency shall acknowledge receipt of the complaint within seven days of receipt of the complaint under subregulation (1).

(6) The Agency shall consider the complaint under subregulation (1), within thirty days from the date of the lodging of the complaint.

(7) The complaint under subregulation (1) shall be lodged free of charge.

28. Register of complaints

(1) The Agency shall keep and maintain an up to date register of complaints.

(2) An entry into the register of complaints shall state the particulars of the complainant and the complaint filed with the Agency.

(3) The Agency shall protect the identity of the complainant where the request to protect the identity is sought by the complainant.

29. Admission of a complaint

Upon receipt of a complaint under this part, the Agency shall—

(a) admit the complaint; or

(b) decline to admit the complaint where the complaint does not raise any issues under the Act and these Regulations and communicate to the complainant within seven days giving reasons for declining to admit the complaint.

30. Investigation of a complaint

(1) Where the Agency admits a complaint, the Agency shall conduct an investigation and may—

(a) issue summons requiring the attendance of any person at a specified date, time and place for examination.

(b) require any person to produce any document or information from a person or institution;

(c) administer an oath or affirmation on any person during the proceedings;

(d) examine any person in relation to a complaint; and

(e) upon obtaining warrants from the court, enter into any establishment or premises and conduct a search and may seize any material relevant to the investigation.

(2) Upon completion of the investigation, the Agency shall prepare an investigation report.

(3) In conducting investigations under this regulation, the Agency shall comply with the provisions of the Fair Administrative Action Act (Cap. 7J).

31. Discontinuation of a complaint

(1) The Agency may discontinue a complaint where the complainant refuses or fails, neglects to communicate with the Agency without a justifiable cause.

(2) The Agency shall provide reasons for discontinuation on any of the grounds specified under subregulation (1) and shall, in writing, notify the complainant and respondent within fourteen days from the date the decision to discontinue a complaint is made.

(3) Where a complaint has been discontinued pursuant to these Regulations, a complainant may re-institute a complaint upon providing grounds for the restitution of the complaint to the Agency.

32. Withdrawal of a complaint

(1) A complainant may at any stage during consideration of a complaint withdraw a complaint but before a determination is made.

(2) A withdrawn complaint under subregulation (1) may be re-lodged, within six months from the date of withdrawal of such complaint.

(3) A complaint re-lodged under this regulation shall be processed in accordance with the provisions of this Part.

33. Outcome of investigations

(1) The Agency shall upon the conclusion of the investigation, make a determination based on the findings of the investigations.

(2) A determination under subregulation (1) shall be in writing and shall state—

(a) nature of the complaint;

(b) summary of the facts and evidence adduced;

(c) decision of the Agency and reasons for the decision; and

(d) any remedy to which the complaint is entitled.

(3) The Agency shall within seven days from the date of such determination, communicate the decision under subregulation (2) to the parties, in writing.

34. Appeals

A person aggrieved by a decision of the Agency under this part, may within fourteen days from the date of the decision of the Agency, appeal to the High Court.

35. Exemption of complaints related to personal data

A data subject who is aggrieved by a decision of any person under the Data Protection Act, shall lodge a complaint with the Data Commissioner in accordance section 56 of the Data Protection Act (Cap. 411C).

Part IV – PROVISION OF E-HEALTH AND CERTIFICATION

36. Certification of digital health solutions

(1) Pursuant to section 6(m), the Agency shall certify a digital health solution including e-health and telemedicine platforms in accordance with the Certification Framework.

(2) The Agency shall, in relation to certification of digital health solutions—

(a) manage the certification process;

(b) ensure that health data controllers and digital health solutions comply with the Certification Framework;

(c) ensure that the Certification Framework is aligned to digital health standards and guidelines developed and published by the Cabinet Secretary; and

(d) disseminate the Certification Framework including the digital standards and guidelines.

(3) The Agency may, in collaboration with the relevant institutions, set up and certify laboratory-based testing environments for the purposes of assessing the conformity of digital health solutions with the Certification Framework.

37. E-health

(1) A healthcare provider or a health facility shall not use a digital health solution in the provision of healthcare services, unless the digital health solution has been certified by the Agency.

(2) A health data controller or a health data processor shall not use or access the Comprehensive Integrated Health Information System unless it is certified by the Agency and shall—

(a) use a digital health solution certified by the Agency for service delivery; and

(b) adhere to the digital and physical security requirements in the Certification Framework.

(3) The Agency shall—

(a) certify all e-health and telemedicine platforms in accordance with the Certification Framework; and

(b) give user access to the System to a health data controller of a certified digital health solution.

38. Application for certification

(1) A digital health solution provider shall apply for the certification of a digital health solution to the Agency in the Form HMIS 4 set out in the First Schedule.

(2) A digital health solution provider shall, prior to applying for certification under subregulation (1), undertake self-attestation on the digital health solution and prepare a self-attestation report.

(3) An application under subregulation (1) shall be accompanied by—

(a) a self-attestation report;

(b) certificates of incorporation the applicant;

(c) particulars of the health data controller;

(d) a system manual and requirements specification of the digital health solution;

(e) evidence of registration with the Office of the Data Protection Commissioner as a data controller and data processor;

(f) the Data Protection Impact Assessment Report of the digital health solution prepared in accordance with the Data Protection Act (Cap. 411C);

(g) the security, privacy and confidentiality policy of the digital health solution provider;

(h) proof of payment of the certification fees set out in the Second Schedule;

(i) the system back-up and recovery policy of the applicant; and

(j) the Cyber Security Assessment Report of the digital health solution.

39. Considerations for certification

The Agency shall certify digital health solutions based on the following—

(a) functionality as set out in the Certification Framework including the system and data quality;

(b) compliance with reporting and alerts as required by the prevailing policies and guidelines in the health sector;

(c) compliance with the Information Security, Privacy and Confidentiality standards provided in the Kenya Health Data Governance Framework established under section 21(1) of the Act; and

(d) capacity to perform information exchange and interoperability in accordance with the Interoperability Framework developed by the Cabinet Secretary pursuant to section 21(2)(b) of the Act.

40. Testing

(1) The Agency shall schedule and test the digital health solution submitted to the Agency for certification.

(2) Upon completion of testing under subregulation (1), the Agency shall prepare a testing report and notify the digital health solution provider of the results of the testing within five days from the date of the adoption of the testing report by the Board.

(3) The Agency may specify in the testing report prepared under subregulation (2) the non-compliance issues that the digital health provider may be required to comply with.

(4) A digital health solution provider may, after receiving the testing report take corrective action as required under subregulation (3) and submit evidence of the corrective actions taken to comply with the requirements given by the Agency under subregulation (3).

(5) Where the Agency is satisfied that the corrective action taken by the digital health solution provider addresses the compliance action specified in the testing report the Agency shall issue a certificate of compliance for the digital health solution.

(6) Where the Agency determines that the corrective action does not address non-compliance issues, the Agency shall not certify the digital health solution.

(7) Where a digital health solution provider is dissatisfied by the decision of the Agency in relation to the certification process, a digital health solution provider may apply to the Agency for a review of the decision.

(8) The Agency shall consider the application for review under subregulation (7), within fourteen days from the date of the application.

(9) Where the Agency is satisfied with the outcome of the testing under this regulation, the Agency may—

(a) issue a certificate of compliance for the digital health solution; and

(b) notify the digital health solution provider within thirty days from the date of the completion of the testing.

(10) A person aggrieved by the decision of the Agency under subregulation (8), may seek a remedy from the High Court.

41. Validity of a certificate

(1) A certificate of compliance issued under regulation 40, shall be valid for two years from the date of issuance.

(2) A digital health solution provider shall, upon the expiry of the period under subregulation (1), apply for re-certification in the manner set out in these Regulations.

42. Monitoring of compliance by the Agency

(1) The Agency shall monitor compliance with the Certification Framework by digital solution providers or health data controllers and, in particular, shall—

(a) review the data quality assessments submitted by health data controllers to ensure compliance with the digital health standards and guidelines; and

(b) schedule and conduct annual audits and checks, using the tools and procedures in the Data Quality Assessment Standards, to assess adherence and compliance to Data Quality Protocols by the System and the certified digital health solutions.

(2) A digital health solution provider or health data controller shall comply with a change in the digital health standards and guidelines within six months from date of the change.

(3) The Cabinet Secretary shall, in consultation with the Agency, continuously revise and update Data Quality Protocols.

43. *Ad hoc* audit

(1) A digital health solution provider or health data controller shall comply with the Certification Framework for purposes of maintaining the certification of the digital health solution and shall, in particular—

(a) perform the necessary updates and bug fixes;

(b) ensure that the certified digital health solution documents any change logs;

(c) ensure that data generated through the certified digital health solution is accurate, timely, complete, consistent, valid and in conformity to the needs of the health sector;

(d) perform regular data quality assessments of their systems using standards, protocols and tools defined by the Agency and maintain records of the assessments for review by the Agency;

(e) notify the Agency in the event of system changes affecting security, functionality, reporting or interoperability of the digital health solution upon which the Agency shall conduct a fresh audit of the digital health solution; and

(f) notify the Agency, in the event of system breaches, on the nature of the breach and the solution implemented to resolve the breach.

(2) The Agency shall, during the validity period of the certificate of compliance, undertake *ad hoc* audits including site visits to—

(a) assess compliance with certification requirements; and

(b) verify corrective actions in the event of non-conformity with the certification requirements.

44. Revocation of certification

(1) The Agency shall revoke the certification of a digital health solution where—

(a) the digital health solution provider or health data controller fails to adhere to the conditions set out in the certificate issued under regulation 40(9);

(b) a major system security breach has occurred on health data; or

(c) a digital health solution provider fails to notify the Chief Executive Officer of a data breach in accordance with regulation 11.

(2) Where a digital health solution provider is dissatisfied by the decision of the Agency under subregulation (1), the digital health solution provider may apply to the Agency for a review of the decision.

(3) The Agency shall consider the application for review under subregulation (2), within fourteen days from the date of the application.

(4) A person aggrieved by the decision of the Agency under subregulation (3), may seek a remedy from the High Court.

(5) In making the revocation under subregulation (1), the Agency shall comply with the provisions of the Fair Administrative Actions Act (Cap. 7J).

45. Transitional and saving provisions

(1) A digital health solution provider who, subject to subregulation (2) and (3), immediately before the commencement of these Regulations was providing a digital health solution shall continue to provide that digital health solution.

(2) A digital health solution provider referred to under subregulation (1) shall make an application in the Form HMIS 4 set out in the First Schedule within six months of the coming into force of these Regulations for the certification of a digital health solution to the Agency in accordance with regulation 38.

(3) Where the Board rejects an application for certification of a digital health solution, the digital health solution provider shall cease to provide that digital health solution from the date of the rejection of the application.

FIRST SCHEDULE (r. 11(1)(2)(a))

FORM HMIS 1

NOTIFICATION OF BREACH

.DETAILS OF THE HEALTH DATA CONTROLLER.
☐ FULL NAME:
☐ ID/PASSPORT NO.

☐ SEX:
☐ ORGANIZATION NAME:
☐ POSITION IN THE ORGANIZATION
☐ EMAIL ADDRESS:
☐ COUNTY:
☐ TEL NO.
DETAILS OF DATA PROTECTION OFFICER
☐ FULL NAME:
☐ ID/PASSPORT NO.:
☐ SEX:
☐ EMAIL ADDRESS:
DIGITAL HEALTH SOLUTION DETAILS
☐ SOLUTION NAME:
☐ DHS CERTIFICATION OF COMPLIANCE NO.:
☐ DESCRIPTION OF THE DHS:
DESCRIPTION OF THE BREACH
☐ DATE THE BREACH OCCURRED (Provide your best estimate if the exact date is not known):

☐ WAS THE BREACH REPORTED WITHIN 48hrs. OF DISCOVERY? (If No, please specify why)YES ☐ NO

☐ If No, please specify why

☐ DATE THE BREACH WAS DISCOVERED:

☐ PRIMARY CAUSE OF THE BREACH

☐ MALICIOUS ☐ CRIMINAL ATTACK

☐ SYSTEM FAULT ☐ HUMAN ERROR

☐ OTHER

If Other, please specify

☐ DESCRIPTION OF HOW THE BREACH OCCURRED:

DATA BREACH

☐ WAS THERE A DATA BREACH?

☐ YES ☐ NO

☐ TYPE OF INFORMATION INVOLVED IN THE DATA BREACH:

☐ CATEGORIES AFFECTED:

☐ PATIENT DATA ☐ HUMAN RESOURCE DATA

☐ ADMINISTRATIVE DATA ☐ DE-IDENTIFIED DATA

☐ AGGREGATE HEALTH DATA

☐ EXACT NUMBER OF DATA SUBJECTS WHOSE PERSONAL DATA WAS INVOLVED IN THE DATA BREACH:
☐ EFFECT OF THE BREACH

REMEDIAL ACTIONS
☐ A DETAILED DESCRIPTION OF ANY ACTION INCLUDING REMEDIAL ACTION TAKEN TO ASSIST DATA SUBJECTS WHOSE PERSONAL DATA WAS INVOLVED IN THE DATA BREACH:
☐ DETAILED PRESCRIPTION OF ANY ACTIONS YOU HAVE TAKEN OR INTEND TO TAKE TO PREVENT RE-OCCURRENCE:
☐ SPECIFY THE STEPS YOUR ORGANIZATION RECOMMENDS THAT INDIVIDUALS TAKE TO REDUCE THE RISK THAT THEY EXPERIENCE SERIOUS IMPACTS AS A RESULT OF THIS DATA BREACH:
OTHER ENTITIES AFFECTED: (IF THE SYSTEM BREACH DESCRIBED ABOVE WAS ALSO A BREACH OF ANOTHER ORGANIZATION, PROVIDE THEIR IDENTITY AND CONTACT DETAILS)
ANY OTHER RELEVANT INFORMATION
DECLARATION
I hereby attest that the information provided, including the attached documents, is true and accurate to the best of my knowledge. I authorize the DHA to validate and verify for legitimate purposes.
Signature:..... Date:.....

FORM HMIS 2 (r.17(1))

HEALTH DATA REQUEST FORM

DETAILS OF THE REQUESTER

☐ FULL NAME:
☐ ID/PASSPORT NO.
☐ SEX:
☐ INSTITUTIONAL AFFILIATION:
☐ PROOF OF REGISTRATION WITH THE ODPC AS A DATA CONTROLLER/PROCESSOR (For PII data):
☐ EMAIL ADDRESS:
☐ TEL NO.
REQUEST DETAILS
☐ PURPOSE OF THE REQUEST (Detailed description)
☐ PROGRAM/POLICY ☐ RESEARCH
☐ DESCRIPTION OF THE DATA BEING REQUESTED
☐ SENSITIVE PERSONAL DATA ☐ DE-IDENTIFIED DATA ☐ AGGREGATE HEALTH DATA
☐ DESCRIPTION OF HOW THE DATA WILL BE PROCESSED Give a detailed description of the following; o *The purpose of processing* o *How the data will be processed* o *How long the data will be used* o *How the data will be stored* o *How the data will be managed and deleted after use* o *Number of people with access to the data shared*

RECIPIENT DETAILS
☐ FULL NAME:
☐ ID/PASSPORT NO.
☐ SEX:

☐ INSTITUTIONAL AFFILIATION:
☐ PROOF OF REGISTRATION WITH THE ODPC AS A DATA CONTROLLER (For PII data):
☐ EMAIL ADDRESS:
☐ TEL NO.
REQUISITE DOCUMENTS (Attach the following documents)
☐ IRB Approvals (ERC & NACOSTI) – For research requests
☐ Documents showing lawful purpose – For Program and Policy requests
DECLARATION
I hereby attest that; o The data received shall not be used for any other purpose besides what is described above. o The data received shall not be shared unless with prior authorization. Signature of requestor…… Date of Request Submission……
APPROVAL OF DATA REQUEST

Date of Request Approval…… Signature of Approving Health Data Controller……

FORM HMIS 3 (r.27(2))

COMPLAINT FORM

TYPE OF COMPLAINT
☐ Collection of sensitive personal data without consent by the client; ☐ Data breaches; ☐ Unauthorized sharing, access, and use of data; ☐ The certification process; ☐ Access to data or denial of access to data; ☐ Non-compliance of digital health solutions; ☐ Non-compliance of health data controllers; ☐ Denial of services within the system; ☐ Obligations on the use of the system; ☐ Any other
COMPLAINANT'S DETAILS
☐ FULL NAME:
☐ ID/PASSPORT NO.
☐ EMAIL ADDRESS:
☐ TEL NO.:
☐ PREFERRED MODE OF COMMUNICATION BY THE COMPLAINANT:
RESPONDENT'S DETAILS

☐ FULL NAME:
☐ ID/PASSPORT NO.:
☐ EMAIL ADDRESS:
☐ PHYSICAL ADDRESS:
☐ TEL NO.:
NATURE OF THE COMPLAINT
☐ DATE OF OCCURRENCE OF ALLEGED INFRINGEMENT:
☐ DETAILS OF THE COMPLAINT:
☐ PARTICULARS OF OTHER PERSONS IMPACTED BY THE ALLEGED INFRINGEMENT:

☐ ANY ACTUAL OR POTENTIAL HARM OR URGENCY TO BE TAKEN NOTE OF:
SUPPORTING DOCUMENTS
☐ Pre-certification Audit Report (for certification process complaints)
☐ Any other documents in support of the complaint
DECLARATION
I hereby attest that the information provided, including the attached documents, is true and accurate to the best of my knowledge. I authorize the DHA to validate and verify for legitimate purposes.

Signature:..... Date: .....

FORM HMIS 4 (r. 38(1), r.45(2))

APPLICATION FOR DIGITAL HEALTH SOLUTION CERTIFICATION FORM

APPLICANT'S DETAILS
☐ FULL NAME:
☐ SEX
☐ ID/PASSPORT NO.:
☐ ORGANIZATION NAME:
☐ POSITION IN THE ORGANIZATION:
☐ EMAIL ADDRESS:
☐ TEL NO.:
☐ CITIZENSHIP: ☐ KENYAN ☐ RESIDENT ☐ FOREIGN NATIONAL
ORGANIZATIONAL DETAILS
☐ ORGANIZATION NAME:
☐ PHYSICAL ADDRESS:
☐ EMAIL ADDRESS:
☐ PHONE NO.:

☐ CERTIFICATE OF BUSINESS/REGISTRATION NO.:
APPLICATION DETAILS
☐ TYPE OF APPLICATION (Tick appropriately) ☐ New Application ☐ Re-application
☐ NAME OF THE DIGITAL HEALTH SOLUTION:
☐ DESCRIPTION OF THE DHS:
☐ PROPOSED USAGE: ☐ HEALTH FACILITY-WIDE ☐ COMPONENT

COMPONENT (Tick appropriately) ☐ LABORATORY ☐ OUTPATIENT MANAGEMENT ☐ PHARMACY ☐ FINANCE	
☐ CHRONIC DISEASE MANAGEMENT ☐ PREVENTION AND PROMOTION	
☐ SURVEILLANCE & REPORTING ☐ OTHER	
IF OTHER SPECIFY:	
REQUISITE DOCUMENTS (Attach the following documents)	
☐ Certificate of Incorporation	
☐ Tax Compliance Certificate	

☐ Evidence of Registration with the ODPC	
☐ Data Protection Impact Assessment Report	
☐ System Manual & Requirements Specification	
☐ Self-attestation Report	
☐ Security, Privacy and Confidentiality Policy	
☐ System Backup and recovery policy	
☐ Cybersecurity Assessment Report	
☐ Proof of payment of the prescribed fee	
DECLARATION	
I hereby attest that the information provided, including the attached documents, is true and accurate to the best of my knowledge. I authorize the DHA to validate and verify for legitimate purposes.	
Signature: ..... Date:	

SECOND SCHEDULE (r.21(2)(b), r.38(3)(h))

FEES

	Component	Fees
1	Data use	1. Middle level colleges and undergraduate – KES. 500 2. Post-graduate— (a) Masters—KES. 5,000 (b) PhD— KES. 20,000 3. Independent researcher - KES. 30,000 4. Research institutions-1% of the total research budget

2	Support for the System by the implementers of health projects	1% of the total budget allocated to monitoring and evaluation
3	Certification	A Digital Health Solution Vendor Application fees – KES. 20,000 Testing of the PoC, Hospital-wide HMIS – KES. 500,000 Mhealth solution – KES. 50,000 Telemedicine – KES. 250,000 Testing of an Outpatient ONLY HMIS – KES. 100,000 Innovators Students and innovator system testing up to a maximum of KES.10,000