LEGAL NOTICE NO. …………………

THE DIGITAL HEALTH ACT

(No. 15 of 2023)

THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

ARRANGEMENT OF REGULATIONS

Regulation

PART III —DISCLOSURE OF PERSONAL DATA

PART IV —COMPLAINTS MANAGEMENT

THE DIGITAL HEALTH ACT

(No. 15 of 2023)

IN EXERCISE of the powers conferred by section 60(a) of the Digital Health Act, 2023, the Cabinet Secretary for Health in consultation with the Board of the Digital Health Agency and the County Governments, makes the following Regulations—

THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

PART I —PRELIMINARY

Citation.

1. These Regulations may be cited as the Digital Health (Health Information Management) Regulations, 2024.

Interpretation.

2. In these Regulations, unless the context otherwise requires—

No. 15 of 2023.

"Act" means the Digital Health Act, 2023;

"Agency" means the Digital Health Agency established under section 5(1) of the Act;

"aggregate data" means health data or information consolidated and stored in a single, central system for ease of access including service statistics or clinical data;

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

"authorized access" means the legitimate and sanctioned entry, retrieval and processing of data within a system by an individual or an entity that has been granted explicit permission and privileges by a health data controller based on the roles and responsibilities of that individual or entity and the applicable policies governing the system of the health data controller;

"Board" means the Board of Directors of the Digital Health Agency established under section 8 of the Act;

"Cabinet Secretary" means the Cabinet Secretary for the time being 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;

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

"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 personal data;

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

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

"health data" means data related to the state of physical or mental health of a 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 processor" means a person, public authority, agency or other body who is an authorised worker to process health data;

"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 healthcare professionals through the healthcare system's routine health services, or its emergency health services;

"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; and

"System" means the Comprehensive Integrated Health Information System established under section 15(1) of the Act.

Object of the Regulations.

3. The object of these Regulations is to give effect to the provisions of the Act by ensuring the safe management of health information.

PART II— MANAGEMENT OF HEALTH INFORMATION

The Kenya Health Data Governance Framework.

4. (1) The Kenya Health Data Governance Framework established pursuant to section 21(1) of the Act shall be the reference document for the management of health data and shall govern the collection, access, sharing and use of health data.

(2) The Agency shall ensure that health data controllers and health data processors comply with the provisions of the Kenya Health Data Governance Framework in the management of health data.

Data custodianship.

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

(a) maintain a registry of all health data controllers;
(b) maintain an inventory of health data held by the health data controllers;
(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.

Security of health data.

6.(1) There shall be an Information Security Operations Centre within the Agency which shall be responsible for—

(a) real time monitoring and managing security and network of the system including event and alerts management;

(b) developing and implementing security and network policies and procedures;
(c) providing security awareness training;
(d) analysing logs, network traffic monitoring and incident management;
(e) detecting and responding to security and network incidents;
(f) performing information security and vulnerability assessments
(g) endpoint administration by managing security settings on endpoints and security policies;
(h) security and network system administration by configuring and maintaining security tools;
(i) definition and implementation of role-based user rights;
(j) execute and maintain audit trails for activities in the system
(k) implement digital and physical security measures to the system;
(l) ensure secure and encrypted backups and restoration procedures;
(m) system asset inventory; and
(n) perform such other function as may be prescribed by any other law or as necessary for the promotion of objects of the Agency.

Notification of health data breaches.

7. (1) A health data controller shall maintain an inventory of health data processors that it has engaged and provide role-based access to the health data processors in the System.

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

(a) in the case of a breach, notify the—

(i) Agency within twenty-four hours of becoming aware of such breach using Form 1 set out in the First Schedule; and
(ii) Office of the Data Protection Commissioner in the manner set out in section 43(1)(a) of the Data Protection Act;

(b) within forty-eight hours of the notification of breach, notify the Agency of the—

(i) corrective measure taken;
(ii) the mitigation action adopted; and
(iii) the timelines for the rectification of the breach.

(3) A health data controller of a digital health solution who fails to comply with the provisions of this regulation commits an offence and shall, on conviction, be liable to the penalty specified under section 35(2) and (2) of the Act as may be applicable.

(4) The Agency shall revoke the certification of a digital health solution that fails to comply with the provisions of this regulation.

(5) All healthcare providers and health facilities shall use a digital health solution that has been certified by the Agency in accordance with the Digital Health (Use of e-health Applications and Technologies), 2024.

(6) For the purpose of section 35 of the Act, a health data breach occurs where a 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.

(7) A health data subject, health data controller, data processor or any other third party may in writing report any health data breach to the Agency in Form 1 set out in the First Schedule.

Inventory of health data

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

Security of sensitive personal data.

9.(1) The Cabinet Secretary, in consultation with the Agency, shall implement security measures for the protection of sensitive personal data as contemplated under section 24(5) of the Act and shall—

(a) ensure 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 shall be restricted to a limited number of authorized personnel and subject to controls;
(v) a user account assigned to a healthcare provider shall be 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 shall be linked 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 shall be retained for minimum of twenty years;
(iii) access to audit logs shall be 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;

(vii) health data controllers shall implement an Incident Response plan outlining procedures 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 an 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.

Health data privacy.

10. (1) The Agency shall implement and maintain privacy standards throughout the data life-cycle.

(2) No person or entity shall access health data unless authorized by the client or the health data controller to whom the data relates to.

(3) 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 after the deletion of their data; and

(d) permanently delete all copies of the data in their possession.

Archiving of health information.

11. (1) The Agency shall archive health information in the circumstances determined by it including —

(a) where the 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) where the record has been inactive for a minimum of twenty years.

(2) The twenty-year period provided 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 the health 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 data shall be archived seven days from the date of the notification of archival.

(4) The data of the deceased data subject shall, on 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 death 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 determined by the Agency 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, the relevant laws, international standards and best practices.

Migration of data.

12. (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 using the applicable protocols and formats.

(3) A health data controller or health data processor with legacy data under their control 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 by the Act and these Regulations.

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

Health data sharing.

13. (1) Shared health data shall—

(a) be used for the purposes described in the request by the data requester and for a specified period as stipulated in the authorization by the health data controller or the Data Sharing Agreement; and
(b) not be transferred to individuals outside the duly recognized working group of the data requester.

(2) Health data may be shared in a format that may be developed by the Agency or other formats that meet the following essential minimum requirements:

(a) a clear statement of the purpose and objectives of the data sharing arrangement;
(b) specification of the categories of data to be shared;
(c) defined roles, responsibilities, rights, and obligations of all parties involved;
(d) provisions for data protection, including confidentiality and security measures; and
(e) mechanisms to ensure compliance with the Act and other relevant laws.

(3) The health data controller shall handle any subsequent processing and use of data not included in the initial authorization on a case-by-case basis.

(4) A health data controller shall, for purposes of this regulation, develop and implement a data sharing plan in accordance with the Kenya Health Data Governance Framework.

(5) The Agency shall determine and monitor, on its own initiative or upon request by a health data controller, the access levels to the System.

Access to health data from the System.

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

(2) A person may request for health data not containing personally identifiable information.

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

(4) 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 client to whom the requested health data relates to.

(5) 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;
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; and

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

(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 County Executive Committee Member.

(5) The Agency shall, within thirty days from the date of receipt of the request, consider the request for health data and shall—

(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.

(6) A person whose request is granted shall notify the Agency or the health data controller whether the health data requested shall be used for a purpose not included in the initial authorization to the Agency or the health data controller.

(7) A person whose request is denied may make an application for review of the denial of the access request to the Complaints Committee within fourteen days from the date of the decision of the Agency.

(8) The Complaints Committee shall consider the complaint within thirty days from the date of lodging of the complaint.

Correction of health personal data.

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

(2) The request under sub regulation (1) shall specify —

(a) health personal data that is to be amended indicating how such information is inaccurate, out of date, incomplete or misleading; and
(b) remedy sought by the client.

(3) The health data controller shall, within seventy-two hours from the date of the receipt of the request under sub regulation (1), correct the health data of the client.

Secondary use of health data.

16. (1) Health data containing sensitive personal health data may be used for public health purposes specified under section 27(f), (g), (h) and (i) of the Act and shall be accessed in de-identified form.

(2) A health data controller shall—

(a) ensure that data used for public health purposes shall be accessed by authorized persons; and
(b) in consultation with the Agency, facilitate access to data for secondary use in the manner determined by the Cabinet Secretary.

(3) The Agency shall—

(a) grant rights for secondary use of data in accordance with the guidance issued by the Cabinet Secretary;
(b) in consultation with the Cabinet Secretary, implement the secondary use of data as provided under section 27 of the Act; and
(c) enforce the compliance with section 27 of the Act by the health data controllers, health data processors and third parties.

(4) A health data controller or a third party shall access health data in the System for public health purposes 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 applicable fees set out in the Second Schedule.

(5) The Agency shall consider a request under sub-regulation (4) and communicate its decision within fourteen days from the date of the request.

Access to health data by a data subject.

17. (1) A data subject shall access their Shared Health Record from the patient portal.

(2) A data subject under sub regulation (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) The Agency shall grant access to a client under sub regulation (1) with limitations on the validity of the link by—

(a) setting an expiry date;
(b) creating an access code or password; or
(c) limiting the number of times that the link may be accessed.

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

(5) On the completion of healthcare services sought outside Kenya, a client under this regulation shall, on 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.

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

PART III—DISCLOSURE OF HEALTH PERSONAL DATA

Sensitive personal data of deceased persons.

18. (1) A request for disclosure of sensitive personal data of a deceased person shall be made in writing to a health data controller in possession of such sensitive personal data .

(2) The health data controller shall grant a request under sub regulation (1) where the data is requested for purposes of—

(a) identifying a person;
(b) informing a person to whom it is reasonable to inform in the circumstances; or
(c) investigating a cause of death.

(3) Where a request under sub regulation (1) is denied, the requester may make an application for review of the denial to the Agency.

Sensitive personal data in emergencies.

Cap. 241.

19. A request for access to personal sensitive data shall, for purposes of emergency treatment as defined under the Health Act, 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.

Disclosure of personal health data for market research.

Cap. 411C.

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

Request for sensitive personal data in the System.

Cap. 411C.

21. (1) A third party may, subject to the provisions of section 24(2) of the Act, make a request, in writing, to a health data controller to access sensitive personal data in accordance the Act and these Regulations.

(2) A third party shall make an application under sub regulation (1) an in an identity verification Form specifying the reason for the request for information.

(3) A health data controller shall ensure that the system is able to log and that the logs are accessible.

(4) All requests to access sensitive personal data shall be logged and the log made available to the relevant health data controllers in the health data banks.

(5) The health data controller shall consider the request and respond to the third party within fourteen days from the date of the request.

(6) Where the health data controller fails to respond to the request within fourteen days, the third party may make a request in writing to the Agency.

(7) The Agency shall consider a request under sub regulation (4) and shall communicate its decision to the third party within fourteen days from the date of receipt of the request.

(8) A person who accesses personal health data contrary to the provisions of section 27 of the Act commits an offence and shall, on conviction, be liable to the penalty specified under section 35 of the Act.

(9) The third party may, where a request is denied at any level, lodge a complaint with the Complaints Committee which shall consider the request within ten days from the date of the appeal.

(10) A person dissatisfied by the decision of the Committee, may within fourteen days apply for review of the decision by the Complaints Committee.

Processing of sensitive personal data in the System.

22. A health data controller shall, before releasing personal health data, —

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

requiring official identification documents;

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

(ii) 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, the data shall be received by a person explicitly authorized by the client in writing or by a court order.

PART IV- COMPLAINTS MANAGEMENT

Lodging of complaints.

23. (1) A person may, in writing to the Complaints Committee appointed by the Board, lodge a complaint on matters in relation to the requirements of the Act and these Regulations including—

(a) data breaches;
(b) unauthorized sharing, access and use of data;
(c) the certification process;
(d) access to data or denial of access to data;
(e) non-compliant digital health solutions or health data controllers;
(f) denial of services within the System; and
(g) obligations on the use of the System.

(2) A complaint may be lodged at such place or in such manner as the Agency may determine including —

(a) at the offices of the Agency through the designated officer of the Agency; or
(b) through a virtual complaints desk.

(3) The complaint may be lodged using Form 3 set out in the First Schedule or in such other form as the Agency may from time to time determine.

Form of the complaint.

24. (1) The complaint form shall provide the—

(a) name and contact details of the complainant;
(b) particulars of the person complained against;
(c) substance of the complaint in sufficient detail to enable the Agency to act on the complaint; and
(d) documentary evidence of the complaint, where applicable.

(2) Despite sub regulation (1), a complaint may be made anonymously, or treated in such a manner as to protect the identity of, or particulars of, the

complainant where necessary, as may be directed by the Board of the Agency.

(3) Where the complaint is made orally or the complainant cannot read or write, the complaint shall be reduced into writing by the designated officer of the Agency.

Complaints Register.

25. (1) The Agency shall keep a register of complaints in which all complaints shall, upon receipt, be entered.

(2) The Complaints Register shall contain the information determined by the Board including the—

(a) name of the complainant;
(b) contact details of the complainant;
(c) name of the person or entity complained against;
(d) date of receipt of the complaint;
(e) summary of the complaint including the interventions made to resolve the complaint; and
(f) status on the handling of the complaint.

Processing of complaints.

26. (1) The Complaints Committee shall acknowledge a complaint lodged within seven days from the date of receipt of the complaint.

(2) The Complaints Committee shall review the complaint and communicate its decision and the appropriate action to be taken in relation to the complaint within thirty days from the date of receipt of the complaint.

(3) The Agency shall, in processing and reviewing a complaint, have due regard to the principles of natural justice and, in particular, the principles of fair administrative action specified in Article 47 of the Constitution and the Fair Administrative Action Act.

(4) The Agency shall maintain a ticketing system for purposes of tracking the progress of a complaint and providing feedback to the complainant on the resolution of the complaint.

Cap. 7L.

(5) A complainant may, in writing, give notice to the Agency for withdrawal of a complaint pending before the Agency at any stage during its consideration by the Agency —

(a) before a determination is made; and
(b) subject to the approval by the Complaints Committee.

(6) A person dissatisfied with the decision of the Complaints Committee may apply in writing to the Board for a review of the decision of the Complaints Committee within seven days from the date of the decision.

(7) The Board shall consider an application under subregulation (6) and shall make a decision on the appropriate action to be taken in relation to the complaint within thirty days from the date of the application.

(8) A person shall not file any legal proceedings in a Court of law unless the complaints handling procedure provided for under these Regulations has been exhausted.

Exemption of complaints related to personal data.

Cap. 411C.

27. A complaint in relation to sensitive personal data shall be processed in accordance with the provisions of section 56 of the Data Protection Act.

FIRST SCHEDULE

FORM 1 ((r. 7(2)(a)(ii), (r.7(7))

REPUBLIC OF KENYA
DIGITAL HEALTH ACT, NO. 15 OF 2023
THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

NOTIFICATION OF BREACHES
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 24hrs. 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 DATA**

- **EXACT NUMBER OF DATA SUBJECTS WHOSE PERSONAL DATA WAS INVOLVED IN THE DATA 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 2 ((r. 14(1))

REPUBLIC OF KENYA
DIGITAL HEALTH ACT, NO. 15 OF 2023
THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

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 DATA**
• **DESCRIPTION OF HOW THE DATA WILL BE PROCESSED**   **Give a detailed description of the following;**   ○ ***The purpose of processing***   ○ ***How the data will be processed***   ○ ***How long the data will be used***   ○ ***How the data will be stored***   ○ ***How the data will be managed and deleted after use***   ○ ***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 3 ((r. 23(3))

REPUBLIC OF KENYA
DIGITAL HEALTH ACT, NO. 15 OF 2023
THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

COMPLAINTS 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: ....

SECOND SCHEDULE

((r. 16(4)(b)

REPUBLIC OF KENYA
DIGITAL HEALTH ACT, NO. 15 OF 2023
THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024

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 of the institution
2	Support for the System by the implementers of health projects	1% of the total budget allocated to monitoring and evaluation

DR. DEBORAH M. BARASA,
Cabinet Secretary for Health.