African Population and
Health Research Center

DATA PROTECTION AND PRIVACY POLICY

Date of Approval:	November 2021
Effective Date:	November 2021
Review Date:	November 2025
Next review:	November 2028

Table of Contents

1. Definition of Terms

- **Consent** - means any manifestation of express, unequivocal (unambiguous), free, specific, and informed indication of the data subject's wishes by a statement or by clear affirmative action, signifying agreement to the processing of personal data relating to the data subject. Consent is the legal basis for processing personal data.

- **Data controllers** - natural or legal persons, public authorities, agencies, or other bodies which, alone or jointly with others, determine the purpose and means of the processing of personal data. Data controllers have the overall say and control over the reason (the why) and purposes (the how) behind data collection and the means and methods of any data processing.

- **Data processors** - natural or legal persons, public authority, agency, or other body, which processes personal data on behalf of the data controller.

- **Data protection impact assessment** - an assessment of the impact of the envisaged processing operations on the protection of personal data.

- **Data subject** - an identifiable natural person who is the subject of personal data.

- **Encryption** - the process of converting the content of any readable data using technical means into coded form.

- **Identifiable natural person** - a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more specific factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

- **Personal data** - any information relating to an identified or identifiable natural person. e.g., names, GPS locations, International Mobile Equipment Identity (IMEI) numbers, etc.

- **Personal data breach** - breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

- **Anonymisation**- processing of personal data in such a manner that the personal data can no longer be linked to a specific data subject without the use of additional information. Such additional information is kept separately and is subject to technical and organizational measures to ensure that personal data is not linked to an identified or identifiable natural person.
- **Pseudonymisation** is the processing of personal data in such a manner that the personally identifiable information (PIIs) in the dataset is(are) replaced by an artificial identifier or alias, known as pseudonyms. Pseudonyms may include fake or fictitious names in the case of qualitative data, or for quantitative/tabular data, these could be unique IDs generated and assigned to individuals sequentially during data collection or analysis. This process is also called de-identification.

- **Sensitive personal data** - data that reveals a person's racial, ethnic, or regional origin, filiation, political opinions, religious or philosophical beliefs, union membership, sexual life, genetic data, or, more generally, data related to the person's health.

2. Introduction

The African Population and Health Research Center (APHRC) recognizes that handling personal data appropriately is critical and has adopted appropriate data systems, privacy, and security measures to ensure that it shall not knowingly violate the rights of data subjects through its processing and handling of data.

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

- The Constitution of Kenya (2010);
- The Kenya Data Protection Act, No. 24 of 2019 and the relevant Regulations;
- Senegal Law No. 2008-12 on the Protection of Personal Data and relevant Regulations;
- The 2016 International ethical guidelines for health-related research involving humans;
- The U.S. Department of Health and Human Services, regulations (45 CFR 46.116);
- National Guidelines for Ethical Conduct of Research Involving Human Subjects (2008);
- Kenya Access to Information Act No. 31
- The EU General Data Protection Regulation (GDPR) 2016/679;
- African Union Convention on Cyber Security and Personal Data; and
- The UN Guidelines for the Regulation of Computerized Personal Data Files.

This policy provides guidance on procedures to secure individuals' personal data, regulate the collection, usage, transfer, and disclosure of the said data..

Policy Statement

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

3. Application

This Policy applies to all APHRC representatives in Kenya and the West Africa Regional Office (staff, partners, contractors, fellows, and Board members).

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

The Policy applies to all personal data that APHRC holds relating to identifiable natural persons. The Policy applies to any processing of personal data carried out by APHRC within Kenya or Senegal or processing data of Kenyan or Senegalese residents, and any automated or non-automated processing where Kenyan or Senegalese law applies.

The Center may obtain, hold, and process the personal data of data subjects in order to implement and manage all services and without which, the Center might not be able to provide its services to these individuals or to its clients. This data includes;

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

The Policy applies to data in the Center’s possession, collected from individuals within or outside Kenya or Senegal as part of the following functional categories;

- **Personal data of employees/applicants:** The Center collects and processes personal and Special Category data of job applicants and employees as described in the Kenya Data Protection Act (Cap 411C), Senegal Law No. 2008-12 on the Protection of Personal Data and other relevant data protection laws. The Center's Information is transmitted between and among internal units and divisions for necessary operational purposes.
- **Personal data of current/prospective fellows:** The Center will collect personal and Special

Category of Data for prospective or enrolled fellows into its programs including the CARTA fellowship program, in order to implement and manage all services and processes relating to its fellows, without which, the Center may be unable to provide its services to these individuals or others.

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

Guiding principles

APHRC will adhere to the principles for processing personal data as set out in various Kenyan, Senegal and relevant data protection laws in the countries it implements projects and relate to data subjects and data from other APHRC stakeholders. These principles include:

- **Privacy:** APHRC recognizes the right of a data subject to have control over how his or her personal data is collected, used, and/or disclosed. The Center will only process data provided by a data subject willingly and, or with a legal basis as required by the law.

- **Confidentiality:** The Center will take reasonable measures to ensure that data in its possession is kept safe and only accessed by authorized individuals.

- **Integrity:** The Center will maintain accurate records and where required, take necessary steps in providing the assurance of data accuracy and consistency of data in its possession.

- **Autonomy:** The Center recognizes and protects the rights of data subjects to make informed decisions about when to have their data collected and for what it may be used for. The Center will put in place measures that enable data subjects to exercise these rights.

- **Beneficence and maleficence:** The Center will process its data in a responsible way and will not knowingly process data in a way that causes harm to data subjects.

- **Justice:** APHRC will process all data that is in its possession lawfully, fairly, and in a transparent manner. In this regard, the Center will collect personal data for specified, explicit, and legitimate purposes.

4. Policy Implementation

Data systems

The Center will establish systems to ensure the security of personal data of any form in line with the ICT policy and as outlined in the Data Sharing Guidelines and Procedures and other relevant institutional guidelines or frameworks, such as the research governance framework and related documents. The systems may include those for data collection, analysis, storage and archival.

Oversight and compliance

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

In line with the Kenyan Data Protection Act (Cap 411C), APHRC will appoint a Data Protection Officer (DPO) who shall serve both Kenyan and the West Africa Regional Office in Senegal to coordinate the implementation of this policy across the Center's various functions. The DPO will liaise with staff in critical data-heavy positions in the Operations and Program Divisions to ensure compliance with this and other related policies.

5. Data handling at APHRC

Data safety and privacy

The Center will take technical and institutional measures against unauthorized or unlawful access, processing, accidental loss, destruction, or damage to secure all its data and data systems. As such, APHRC uses a wide range of security measures as outlined in its ICT Policy to safeguard personal data against unauthorized access and disclosure and will continually evaluate them to ensure they are effective. Staff will be regularly sensitised and capacitated on these provisions and their obligations to them, and appropriate anonymisation or de-identification techniques available from time to time.

Unless there is explicit consent from the data subjects for sharing personal data, only anonymised or de-identified data can be shared with third parties, upon approval by the relevant authorized persons in charge of the datasets to be shared.

Data access, sharing, and transfer

APHRC premises its data access and sharing practices on the principle that data is a public good and should be made available to all authorized users in a timely manner and in a user-friendly format. Any individual or organization using or seeking to access APHRC research data will be required to abide by the provisions of the Center's Data Sharing Procedures and Guidelines and other relevant institutional guidelines or frameworks, such as the research governance framework and related documents.

Storage limitations

APHRC will store personal data in line with the provisions of various laws and regulations guiding the storage of different types of data and as provided in Annex D.

Marketing and commercialization of data

The Center has no intention of selling personal data or deriving any financial benefit from handling personal data. With unambiguous consent or as otherwise permitted by the Kenya Data Protection Act

(Cap 411C), Senegal Law No. 2008-12 on the Protection of Personal Data and other relevant data protection laws, APHRC may use personal information for purposes relating to the marketing of our products and services, or those of our partners.

6. Data Retention

Types of Data and Data Classifications

Data shall be classified into:

a) Formal records
b) Public data
c) Private data
d) Internal data
e) Confidential data
f) Restricted data

Retention Periods

Any data that is part of any of the categories listed in the Records Retention Schedule contained in Annex D, must be retained for the period of time indicated in the Records Retention Schedule. If an employee is unsure whether to retain a certain record, they should contact the Data Protection Officer.

APHRC shall, as per the period indicated in the Records Retention Schedule, consider the principle of storage limitation and balance this against APHRC's requirements to retain the data. Where data is disposable information, employees shall consider the principle of storage limitation when deciding whether to retain this data.

Storage, Backup and Disposal of Data

APHRC's data shall be stored in a safe, secure, and accessible manner. Any document and financial file that is essential to APHRC's operations during an emergency must be duplicated and/or backed up in line with APHRC's ICT backup process and procedures.

The Data Protection Officer, in consultation with department managers, is responsible for the continuous process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data shall be done by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be coordinated with the ICT department in Kenya or Senegal as applicable.

Where litigation is involved, the destruction of data shall stop immediately upon notification from the Legal department that the preservation of documents for contemplated litigation is required. Destruction may resume once the Legal Department lifts the requirement for preservation.

7. Data subject rights

APHRC recognizes that Data Subjects have a number of rights regarding our use of their personal data, some of which are subject to conditions as provided for in the applicable data protection laws.

All requests will be addressed to and dealt with by our Data Protection Officer.

Right of access

This right gives a data subject the right to request in prescribed form and obtain information on whether or not we process their personal data. The request may include what APHRC uses the data for, who APHRC shares it with, how long APHRC stores it and where APHRC has obtained it from. Individuals can also ask for a copy of their personal data. If APHRC processes the said personal data, the data subjects are entitled to make a request to access it. Once APHRC receives such requests, APHRC shall provide an enabling environment for proactive access of personal data or provision of copies of the personal data.

Right to rectification

A data subject may make a request to us in a prescribed format to rectify their personal data that is untrue, outdated, incomplete or misleading APHRC shall process the request and either rectify the personal data within the timelines set out in the relevant data protection laws or decline the request and provide written reasons for refusal within the timelines set out in the relevant data protection laws.

Right to erasure

Data subjects may ask APHRC in a prescribed format to erase or destroy their personal data if doing so is necessary to satisfy a legal obligation or if it is no longer necessary, or in cases where consent is withdrawn or there is an objection to the processing operation. APHRC has put in place mechanisms to respond to such requests within the timelines set out in the relevant data protection laws. The obligation for APHRC to erase personal data only applies in certain circumstances and shall not override processing that is necessary for reasons allowable by the relevant laws.

Right to object

A data subject may make a request to APHRC in a prescribed format not to process all or part of their personal data for a specified purpose or manner. APHRC shall address requests made in respect of direct marketing and related automated decision-making activities within the timelines set out in the relevant laws. APHRC may also decline the request and provide written reasons for declining the request which could include legitimate interests or defense of a legal claim.

Right to data portability

A data subject may make a request to APHRC in a prescribed format to receive their personal data in a structured, commonly used, machine-readable format, and to transmit this ported data to another data controller or processor, or to request the transfer to another data controller or processor where possible. APHRC commits to process the request for data portability within the timelines set out in the relevant laws. APHRC may also decline the request based on certain considerations such as potential for negation of the data subjects' rights guaranteed under the Data Protection Act (CAP 411C), Senegal Law No. 2008-12 on the Protection of Personal Data and other relevant data protection laws and provide written reasons

for refusal not later than 7 days after the decision to decline has been made by APHRC.

Rights in relation to automated individual decision-making, including profiling

When APHRC processes personal data using automated means without human involvement, APHRC shall inform data subjects of the fact of the processing being based on automated decision-making, explain the logic involved. APHRC has put in place measures and procedures to ensure that automatic decision making shall not be prone to errors or discriminatory effects and to ensure that data subjects are granted the opportunity to obtain human intervention and express their views on the automatic decision making. This gives individuals the right to object to decisions being made about them solely by automated means (without any human involvement) and to profiling (where automated processing is used to evaluate certain things about the individual).

Overall, when APHRC is unable to comply with a request, the firm shall clearly inform data subjects about the reasons why.

8. Consent

APHRC is committed to offering the data subjects real choice and control in data processing. For this reason, APHRC shall ensure that the consent of a data subject is freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them and can be withdrawn their consent at any time.

APHRC will ensure there is active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.

APHRC will ensure that the method used to obtain consent shall meet the following requirements:

i. our identity either as a data processor or data controller or both.

ii. the purpose of each of the processing operations for which consent is sought.

iii. the type of personal data that is collected and used.

iv. information about the use of personal data for automated decision-making, where relevant.

v. the possible risks of data transfers due to the absence of an adequacy decision or appropriate safeguards.

vi. whether personal data shall be shared with third parties.

vii. the right to withdraw consent.

viii. the implications of providing, withholding, and withdrawing consent.

ix. where the information relates to a child, a parent has been given full information on the consent and the parent takes an affirmative action to signify consent.

In case of sensitive personal data, APHRC shall obtain the written consent of data subjects unless an alternative legitimate basis for processing exists, or the processing is carried out in the course of legitimate activities, or the information is manifestly made in public, or is necessary.

APHRC shall take steps to ensure that consent that is obtained is given freely, and is specific, unambiguous and granular in the sense of being specific to the processing operation.

Where a data subject withdraws consent, APHRC shall restrict the aspect of the processing of which the consent is withdrawn. The restricted processing can only proceed with the consent of the data subject.

9. CCTV and surveillance systems

Lawful Grounds for CCTV Surveillance

APHRC uses CCTV under its premises for the following legitimate purposes:

a) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
b) for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;
c) to support law enforcement bodies in the prevention, detection and prosecution of crime;
d) to assist in day-to-day management, including ensuring the health and safety of staff and others; and
e) to assist in the effective resolution of disputes which arise during disciplinary or grievance proceedings.

Operation of CCTV

Where CCTV cameras are placed in the workplace, APHRC will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their images may be recorded.

CCTV cameras will monitor the exterior of the building and both the main entrance and secondary exits. The cameras operate 24 hours a day and the data is continuously recorded.

Surveillance systems will not be used to record sound, only image monitoring will only be done by authorised personnel. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

APHRC will ensure live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health, safety and security. APHRC will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include human resource staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated and secure offices.

Given the large amount of data generated by surveillance systems, APHRC may store video footage using a cloud computing system. APHRC will take all reasonable steps to ensure that any cloud service provider maintains the security of the information, in accordance with industry standards.

APHRC may engage data processors to process data on its behalf. APHRC will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Use of additional surveillance systems

Before introducing any new surveillance system, including placing a new CCTV camera in any workplace location, APHRC will carry out a Data Protection Impact Assessment (DPIA) based on the tools and procedures provided in Kenya Data Protection Act (Cap 411C), the Senegal Law No. 2008-12 on the Protection of Personal Data and other respective data protection laws.

A DPIA will assist APHRC in establishing whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

No surveillance cameras will be placed in areas where there is an expectation of privacy unless, in exceptional circumstances, where it is deemed necessary for security or legal reasons.

Covert monitoring

APHRC will not engage in covert monitoring or surveillance unless, in highly exceptional circumstances, where it is deemed necessary for security or legal reasons and, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, APHRC reasonably believe there is no less intrusive way to obtain information.

In the unlikely event that covert monitoring is justified, it will only be carried out with the express authorization of the Executive Director. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring. Covert monitoring will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorized activity.

Requests for disclosure

APHRC may share data with law enforcement agencies and organizations based on an identified legal basis or upon seeking the consent of the data subject where the data shared is sensitive personal data.

No images from APHRC CCTV cameras will be disclosed to any other third party, without consent being given by the data subject. Data will not be released unless there is satisfactory evidence that it is required for legal proceedings or under a court order that has been produced.

In other appropriate circumstances, APHRC may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime. APHRC will maintain a record of all disclosures of CCTV footage. No images from CCTV will be posted online or disclosed to the media.

10. Roles and responsibilities

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

adhere to it.

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

The Board of Directors

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

Executive leadership team

- Oversee the implementation of the Policy by developing appropriate programs and guidelines, establishing systems and processes to protect personal data in the Center's possession.
- Ensure that APHRC representatives are sensitized on the Policy and compliance procedures.
- Exercise appropriate oversight to ensure that the Center adequately assesses data protection risks and implements risk mitigation procedures and processes.
- Monitor trends in data protection and institute appropriate measures.

Data Protection Committee

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures;
- Providing guidance, training, monitoring and updating in relation to this policy; and
- Advising on and monitoring APHRC's compliance with data protection laws which regulate personal data and on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

Data Synergy and Evaluations Team

- Develop databases/software used to safely capture, manage, store data collected from research studies at the Center.
- Ensure compliance with the Center ICT policy in the development of data management, processing, and storage tools and platforms

- Liaise with the DPO to ensure the safety of personal research data.
- Oversee the Center's data-sharing systems and processes, ensuring compliance with laws and regulations governing ethical use of human subjects' data.
- Advise the Center on all matters related to data systems for collection and processing of research data.

Data Protection Officer

- Advise the Center and APHRC representatives on data processing requirements provided under the Data Protection Act (Cap 411C), Senegal Law No. 2008-12 on the Protection of Personal Data or any other relevant data protection law.
- Ensure on behalf of the Center that the relevant data protection laws are complied with.
- Facilitate capacity building and sensitization of staff involved in data processing operations.
- Cooperate with and seek the guidance of the Kenya Data Protection Commissioner and the Senegal Personal Data Protection Commission on any matters relating to data protection.
- Record all data breaches and notify the Kenyan Data Protection Commissioner within 72 hours, where it is established that the breach may result in real harm to affected data subject(s).
- Conduct a data protection impact assessment as required by the relevant data protection laws.

Internal Auditor

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

Legal and Grants Officers

- Review and advise on any changes in the law in Kenya and/or Senegal relating to data protection.
- Draft and review contracts with partners and third parties to ensure compliance with the data protection policy.
- Ensure contracts with partners embody Data Protection principles as envisaged in the relevant data protection laws.

ICT Manager

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

All APHRC staff in Kenya and Senegal

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

9. Non-Compliance

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

10. Related Policies

- Human Resource Policy and Manual
- Safeguarding Policy
- ICT Policy
- Data Protection Notice in accordance with the EU General Data Protection Regulation (GDPR)
- The APHRC Guidelines on Data Access and Sharing
- APHRC Research Handbook

11. Monitoring and review

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

12. Policy revision

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

ANNEX A

APHRC DATA SUBJECT CONSENT FORM

A. Introduction

The African Population and Health Research Center (APHRC) is the continent's premier research and policy organization, exploring population, health, and well-being questions. APHRC has for the last two decades run numerous research projects and generated evidence that has shaped policy and practice across African countries.

B. Privacy at APHRC

APHRC respects the privacy of its employees and third parties who interact with its operational processes in its offices in Kenya and Senegal and other respective jurisdictions. In this consent form, APHRC outlines the categories of personal data it collects from a data subject and how it processes the personal data collected.

C. Data Processing at APHRC

APHRC processes a data subject's personal data by collecting their biographical information, photographs and video recordings that are taken while performing its assignments including personal data previously provided under appropriate legal conditions, based on existing legitimate interests.

D. Transfer of your personal data

APHRC will not share a data subject's personal data with any third party unless they are APHRC partners, such as other research institutions and donors (who may be data processors or sub-processors), solely for research, promotion and advocacy aimed at improving APHRC's fundraising portfolio and donor management, or because of other legal obligations or authorizations. As a safeguard measure, APHRC will pseudonymize the personal data by default and ensure regular deletion of personal data that is no longer required.

APHRC may transfer a data subject's personal data out of Kenya, Senegal or any other applicable jurisdiction for purposes of sharing it with donors. APHRC has put in place appropriate safeguards and security measures regarding the transfer.

E. Automatic decision making

APHRC may undertake automated decision-making or profiling based on the personal data that APHRC collects from data subjects. This will be done in accordance with the Kenya Data Protection Act (Cap 411C), Senegal Law No. 2008-12 on the Protection of Personal Data and other respective data protection laws.

F. Objection to the use of data

A data subject has the right at any time to object to the processing of all or part of their personal data. APHRC will cease processing of the data subject's personal data unless APHRC can demonstrate compelling legitimate grounds for processing that outweigh its interests, rights and freedoms, or if the processing is for asserting, pursuing or defending legal claims.

G. Withdrawal of consent

Data subjects can withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of APHRC's processing based on the consent provided before the withdrawal.

H. Consent

Based on the information above, APHRC requests your consent to collect and process your personal data and sensitive personal data.

Please sign below to allow APHRC to process your personal data.

If you have any questions regarding the processing of your personal data at APHRC, please reach out to us via email address at dpo@aphrc.org or [APHRC to insert other recommended means that a data subject can contact them]

Name Date, and sign.

I consent I do not consent.

ANNEX B

APHRC DATA SUBJECT ACCESS REQUEST FORM

Preliminary

The Kenya Data Protection Act (Cap 411C), Senegal Law No. 2008-12 on the Protection of Personal Data and other respective data protection laws grant a data subject the right to access their personal data held by APHRC including the right to obtain confirmation that APHRC processes your personal data, receives certain information about the processing of the data subject's personal data, and obtain a copy of the personal data APHRC processes.

The data subject can submit this request form through any of the following means:

1. Physical delivery to our offices in Dakar Senegal or Nairobi, Kenya (where applicable) at [Insert APHRC physical office location]
2. Email delivery via dpo@aphrc.org
3. APHRC microdata portal via datarequest@aphrc.org

The Center shall respond to requests within one month of receipt of a fully completed form and proof of identity.

I. Requester Name (Data Subject) and Contact Information

Please provide the data subject's information in the space provided below. [If you are making this request on the data subject's behalf, provide your name and contact information in Section III.]

APHRC will only use the information the data subject provides on this form to identify the data subject and the personal data they are requesting access to and to respond to the request.

First and last name:	
Any other names that the data subject has been known by (including nicknames):	
Home address:	
Date of birth:	
Telephone number:	

Email address:	
If the data subject is a current or former employee of APHRC, please provide your employee identification number and your approximate dates of employment:	
Please provide other unique identifiers or related information to help us locate your personal data (for example, National ID number).	

II. Proof of Data Subject's Identity

APHRC requires proof of the data subject's identity before it responds to their access request. To help APHRC establish the data subject's identity, he/she is required to provide identification that clearly shows their name and date of birth. APHRC accepts a photocopy or a scanned image of one of the following documents as proof of identity: passport, national identification card, or birth certificate.

In case of a change of the data subject's name, please provide the relevant documents as evidence of the change.

If the data subject does not have any of these forms of identification available, please contact the data protection officer via dpo@aphrc.org for advice on other acceptable forms of identification.

APHRC may request additional information from the data subject to help confirm their identity and their right to access, and to provide them with the personal data it holds about the data subject.]

III. Requests made on a Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name:	
Postal address:	
Date of birth:	

Telephone number:	
Email address:	
Relationship with the Data Subject	

APHRC requires a copy of either of the following documents as proof of the legal authority to act on the data subject's behalf: a written consent signed by the data subject, a certified copy of a power of attorney, or any other evidence of parental responsibility.

APHRC may request additional information from you to help confirm the data subject's identity.

APHRC will notify the data subject of its inability to process the request with reasons to support that decision.

IV. Information Requested

To help APHRC process the data subject's request quickly and efficiently, please provide as much detail as possible about the personal data of the data subject requesting access. Please include the time frames, dates, names, types of documents, file numbers, or any other information below to help the Center locate your personal data.

APHRC will contact the data subject for additional information if the scope of the request is unclear or does not provide sufficient information for APHRC to conduct a search. APHRC will begin processing the data subject's access request as soon as APHRC has verified their identity and has all the information needed to locate their personal data.

If the information the data subject requests reveals personal data about a third party, APHRC will either seek that individual's consent or redact their personal data before responding to the request.

If APHRC is unable to provide the data subject with access to their personal data because disclosure would violate the rights and freedoms of third parties, APHRC will notify the data subject of this decision.

V. Signature and Acknowledgment

I, _____, confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that:

i. APHRC shall confirm my identity and may need to contact me again for further information.
ii. My request will not be valid until APHRC receives all of the required information to process the request.
iii. I am entitled to one free copy of the personal data I have requested and acknowledge that for any further copies I request, APHRC may charge a reasonable fee based on administrative costs; and
iv. I assume full responsibility for any use of the data provided by APHRC, whether such use is intended or unintended, lawful or unlawful. APHRC will not be liable in any way for the consequences of any use of the data by myself as the data subject.

If you would like to receive a copy of the personal data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

____ Hard copy.

____ Electronic copy.

_____

Signature

_____

Date

VI. Authorized Person Signature (where applicable)

I, _____, confirm that I am authorized to act on behalf of the data subject. I understand that APHRC shall confirm my identity and my legal authority to act on behalf of the data subject's behalf and may need to request additional information for verification purposes. I assume full responsibility for any use of the data provided by APHRC, whether such use is intended or unintended, lawful or unlawful. APHRC will not be liable in any way for the consequences of any use of the data by myself as the authorized person.

_____

Signature

_____

Date

ANNEX C

LETTER NOTIFYING OF A PERSONAL DATA BREACH TO AFFECTED DATA SUBJECTS

[APHRC LETTERHEAD]

Dear (DATA SUBJECT),

RE: NOTIFICATION OF A PERSONAL DATA BREACH

We regret to inform you of a breach of security that has resulted in the loss of/unauthorized disclosure of/unauthorized access to/alteration of/destruction of/corruption of your personal data.

The breach was discovered on [DATE] and is likely to have taken place on [DATE].

As a result of our preliminary investigation of the breach, we have concluded that:

- The breach affects the following types of information:
    i. ***List all the types of information/personal data that may have been impacted e.g., financial, health, special category/sensitive data, criminal offence data].***
- The information has been accidentally or unlawfully destroyed, corrupted, lost, altered, disclosed without authorization, accessed ***(edit as necessary***) by [name or description of organization or an unauthorized person].
- The breach occurred under the following circumstances and for the following reasons:
    i. ***[circumstances]***
    ii. ***[reasons]***

We have taken the following steps to mitigate any adverse effects of the breach:

i. ***[measures]***

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

i. [***measures]***

Kindly note that investigations are ongoing, and we shall provide further information as the case may be or where necessary.

For Kenyan data subjects, we informed the Office of the Kenyan Data Protection Commissioner of the breach on [DATE]

You can obtain more information about the breach from any of the following contact points:

i. [dpo@aphrc.org; and
ii. APHRC'S ***[insert contact details].***

We apologize for any inconvenience this breach may cause you.

Yours sincerely,

[dpo@aphrc.org]

For and on behalf of the African Population and Health Research Center (APHRC)

ANNEX D: RECORDS RETENTION SCHEDULE

Nature of Personal Data	Retention Period in Kenya	Retention Period in Senegal
Employees personal data	5 years after the termination of employment	6 months, subject to compliance with the provisions relating to the retention period of accounting documents (invoices), which is 10 years.
Biometric time-keeping data	N/A	To be deleted as soon as the employee leaves.
Data relating to human resource management	5 years after the termination of employment	10 years after the employee's departure.
Video surveillance(CCTV) data	N/A	A maximum of 3 months. The maximum duration of 3 months does not apply when the system allows automatic deletion of recordings within a shorter period.
Tax Records	5 years from the date of assessment, save for cases where they are necessary for a judicial proceeding commenced before the end of the five years, the entity shall retain the document until all proceedings have been completed.	Invoices, books and records must be kept for at least 10 years
Research data and statistical data	Retained for periods longer than when the research was concluded for an unspecified period as long as a statistical or research purpose exists.	N/A
Magnetic badges for visitor control, and premises security with anonymous badge distribution if there is a possibility of re-identification.	N/A	A maximum of 6 months and if the badge does not allow re-identification of the visitor, the 6-month period does not apply.
Input and output registers	N/A	A maximum of 6 months.
Vehicle geolocation system for fleet management, route control, and accident prevention.	N/A	A maximum of 2 years.
Customer data if any at APHRC	N/A	To be retained throughout the business relationship. They must be kept subsequently, for ten (10) years, for accounting or tax proof purposes.
Commercial prospecting and promotional offers campaign data	N/A	To be kept for the duration of said campaign. Beyond this period, the data must be deleted or archived.
Processing of bank customer data for combating money laundering and the financing of terrorism.	N/A	10 years from the end of the relationship with the customer.
Insurance customer data for combating money laundering and the financing of terrorism.	N/A	10 years from the end of the relationship with the customer.
Life subscription and memberships: Insurance proposal, special conditions, insurance certificate,	N/A	Up to 5 years after settlement and/or closure.

contract, quote, investment evaluation, medical file data.		

NOTES:

i. N/A means the data protection and other relevant laws in the respective countries do not expressly provide for the retention period.

ii. For personal data storage that is not expressly provided by law in Kenya, section 39(1) of the Data Protection Act (CAP 411C) requires APHRC to store that data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless it is reasonably necessary for a lawful purpose, or the data subject has given consent to retain the data for a longer period.

SCHEDULE:

EXAMPLES OF INCIDENTS OF BREACH

Possible ways in which a data breach may occur:

1. **Human Error**
   i. loss of laptop, phone, data storage devices or paper records
   ii. sending personal data to a wrong email, phone number or physical address or disclosing data to a wrong recipient
   iii. improper disposal of personal data (e.g., hard disk, storage media or paper documents containing personal data are sold or discarded before data is properly deleted.

2. **Malicious Activities**
   i. **Denial of Service**: an attack that consumes the resources on a system or network, preventing normal use of resources for legitimate purposes
   ii. **Malicious Code:** programs such as viruses, worms, logic bombs, Trojan Horses that are surreptitiously inserted into the system to destroy data, run destructive or intrusive programs, or otherwise compromise the security and/or integrity of the victim environment
   iii. **Unauthorized Access:** Gaining or escalating privileges on any computer, network, storage medium, system, program, file, user area or another private repository without the express permission of the owner.
   iv. **Attempted Unauthorised Access**: The precursor to unauthorized access, this incident typically manifests as repeated failed login attempts. As an example, brute force attempts can show tens or hundreds of failed logins per second.
   v. **Inappropriate Usage**: Employee activity on a system that violates any of the established business or security policies.
   vi. **System Compromise / Defacement:** Escalated privileges on a system that leverages to access, modify, or otherwise compromise the integrity of residing data, processes, content or function of a system or website.
   vii. **Data Compromise**: A malicious or unauthorized third party that accesses, manipulates or appropriates personal data, including sensitive or confidential data.
   viii. **Social Engineering**: Technical and non-technical methods for acquiring information or access to an environment. Examples include fake emails containing malicious links or code (also known as phishing), phone calls from individuals pretending to be employees or members, or physical access attempts by individuals who are not authorized to be in a facility.
   ix. **Computer System Error**s: Unforeseen circumstances such as flooding.
   x. **Blagging:** offences where information is obtained by deceiving the organization that holds it.