EXHALE
Health Foundation

Data Protection Policy and Procedures

Policy reference EHF DP 07 | Version 1.0 | Policy owner: Executive Lead | Prepared 1 June 2026

Purpose and commitment

Exhale Health Foundation (EHF) will process personal data lawfully, fairly, transparently and securely. We will collect only what is needed for a defined purpose, keep it accurate, restrict access, retain it for a justified period and respect people's rights. This policy covers research, consultancy, recruitment, staffing, finance, events, websites, communications, and digital tools.

The policy will apply to trustees, staff, project workers, consultants, advisers, volunteers and service providers handling data for EHF. It will cover electronic and paper records, images, recordings, transcripts and information received from clients. We will follow the Nigeria Data Protection Act 2023, applicable NDPC directives and additional laws or contractual requirements that apply to the activity.

Definitions and accountability

Personal data will mean information about an identified or identifiable person, including indirect identifiers and combinations of details. **Sensitive personal data** will include health, genetic, biometric and other categories protected by applicable law. Replacing names with codes will not make information anonymous if re-identification remains possible. Public availability will not remove all data-protection duties.

A **controller** will decide why and how personal data is processed; a **processor** will act on a controller's documented instructions. EHF will assess its actual role for each activity and document it in the agreement. A contract label alone will not determine the legal role. Client processing and EHF's own staffing or administration may involve different responsibilities.

The Executive Lead will be accountable for implementation and will appoint a data-protection focal point. EHF will assess whether a formal Data Protection Officer, NDPC registration, audit or return is required and complete required measures within applicable deadlines. A formal DPO will have appropriate competence, independence and resources and will not hold incompatible responsibilities for deciding processing purposes or methods.

Project leads will maintain processing records, permissions and access arrangements. All personnel will complete relevant briefings and report suspected breaches immediately. An independent trustee route will be available for concerns involving leadership.

Planning and authorisation

Before collecting, receiving, or sharing data, the project lead will record the purpose, controller and processor roles, affected people, data categories, lawful basis, recipients, systems, transfers, retention, and the responsible person. Required ethics review, institutional permissions and data-access or processing agreements will be obtained before the relevant activity.

The lawful basis will be specific to the purpose, such as valid consent, contractual necessity, a legal obligation or another basis permitted by law. Sensitive data will also require an applicable

additional condition. Consent will not be used automatically where a person cannot freely refuse, or to disguise processing required by law. A client's permission will not replace a lawful basis or required ethics approval.

Privacy information will explain EHF's identity and contact details, purposes, legal basis, recipients and transfers, retention, rights and complaint routes. It will be accessible and supplied at the appropriate time. Recording, quotations, images and optional publicity will have separate permissions where appropriate. Declining publicity will not affect participation or services. Limits on withdrawing data after genuine anonymisation or aggregation will be explained honestly.

Children and people who may lack decision-making capacity will receive the additional safeguards required by law and the approved protocol, including appropriate permission and verification of authority. Gatekeeper approval will not substitute for individual consent or resolve all questions of capacity and best interests.

Data protection impact assessment

A documented assessment will be completed before processing likely to create high risks, including substantial sensitive data, vulnerable groups, novel technologies, systematic monitoring, intrusive linkage or profiling. It will describe the purpose, necessity, proportionality, risks to people and safeguards. The focal point or DPO and relevant technical or contextual experts will be involved; affected people's perspectives will be considered where appropriate.

Unresolved high risks will be escalated before processing, including consultation with the NDPC where legally required. Deadlines will not justify starting without the necessary protections. The assessment will be updated after material changes in purpose, technology, datasets or risk.

Collection access and security

- Teams will collect the minimum necessary data and avoid identifiers not needed for the task. Where feasible, teams will separate names and contact details from research responses, using coded identifiers and a separately protected key. Consent records will be kept separately from analysis files.
- Access will follow role and need. Advisers will receive only the information required for authorised tasks. Access will be reviewed after role changes and removed promptly when an engagement ends. Shared logins will not be used for confidential systems.
- Approved systems will use strong unique passwords, multi-factor authentication where available, supported software, security updates and appropriate malware protection. Personal or shared devices will require documented safeguards against unauthorised access and provision for secure removal of EHF information.
- Portable devices and removable media holding protected data will use appropriate encryption. Data will be encrypted during transfer and at rest where supported and proportionate to risk. Staff will not leave records or devices unattended in public places or insecure vehicles.
- Email recipients, attachments and sharing permissions will be checked before sending. Restricted material will use controlled-access links or encrypted transfer, with passwords supplied separately. We will not use public links or informal messaging groups for identifiable research or safeguarding material.

- Paper records will be locked away. Secure backups will be maintained where necessary, with documented access, recovery checks and deletion cycles. Backups will not become an uncontrolled permanent archive.
- Test and demonstration datasets will use genuinely anonymised or synthetic information where feasible. Teams will assess re-identification risks from small groups, location, quotations and linked public data before treating information as anonymous.

Suppliers sharing and international transfers

Before using a cloud platform, survey tool, transcription provider or other processor, EHF will assess security, hosting, sub-processors, confidentiality, retention, secondary use, deletion and breach-notification terms. A written agreement will specify permitted processing, safeguards, assistance with rights, return or deletion and relevant audit arrangements.

Staff will not enter protected material into an external system merely because it is convenient or popular. Public consumer AI services and unapproved personal accounts will not receive personal, sensitive, confidential or restricted information. Any proposed use of a restricted approved service will require a documented lawful basis, client permission, security review, contractual safeguards and risk assessment. Stricter project prohibitions will prevail.

Data sharing will have a defined purpose, minimum dataset, identified recipients and legal basis. Cross-border transfers will meet applicable Nigerian requirements, including an appropriate adequacy assessment or other lawful safeguard where required. A provider's reputation, a privacy-policy link or general consent will not automatically establish compliance. UK or EU requirements will be assessed where their territorial scope or a contract makes them relevant.

Rights requests and complaints

Requests may be made through exhalehealthfoundation@gmail.com or a published project contact. Staff will send them immediately to the focal point and record the receipt date. EHF will normally acknowledge a request within two working days and verify identity proportionately, without routinely demanding unnecessary identity documents.

The focal point will identify the relevant records and applicable right, including access, correction, erasure, objection, restriction or portability where the law provides it. Requests will be addressed without undue delay; the internal target will be 14 calendar days, subject to any shorter legal deadline. A lawful extension or refusal will be explained with reasons, timing and complaint options. Fees and exceptions will require a legal basis.

Where EHF acts as a processor, it will promptly notify the controller and assist under the agreement, rather than independently change client records without authority. People will be told how to contact the NDPC or another relevant regulator. Raising a complaint or exercising a right will not lead to retaliation.

Personal data breach procedure

A breach may include theft, loss, accidental disclosure, unauthorised access, alteration, destruction, a wrongly addressed email, an exposed link or protected data entered into an

unapproved tool. Anyone who suspects a breach will report immediately to the focal point and project lead, using a direct telephone route if email may not be seen promptly. They will not wait for complete information.

Contain and preserve. The response lead will secure accounts and links, prevent further disclosure, recover information where feasible and preserve evidence and event times. Staff will not delete evidence or make uncontrolled copies. Appropriate IT or legal support will be obtained where needed.

Assess risk. The lead will record what happened, affected people and data, recipients, likely harm, recovery, protective actions and outstanding uncertainties. They will document the time of awareness and any contractual deadline. EHF will escalate safeguarding risks through the relevant procedure.

Notify appropriately. As a processor, EHF will notify the controller without undue delay and within any shorter contractual period. As a controller, EHF will notify the NDPC within 72 hours of awareness of a breach likely to result in a risk to individuals' rights and freedoms, as required by the Act. Delay will be explained and information supplied in phases where permitted. A high-risk breach will be communicated to affected people promptly as required, with useful protective advice.

Coordinate without delay. Legal notifications will not wait for a completed investigation, internal meeting or client response. EHF will also report relevant incidents affecting clients' work immediately through an approved secure channel. Initial notifications will minimise identifying information while providing what is necessary.

Review and close. EHF will record the reporting decision and its reasons, complete corrective actions and review similar risks. All breaches and near misses will be logged, including those not requiring regulator notification. Lessons will inform training, system and supplier decisions. Staff will not alert a suspected perpetrator in a way that undermines protection or a lawful investigation.

Retention, deletion and handover

Each project will have a retention schedule approved before collection and reflected in notices and agreements. Legal requirements, ethics approvals, and justified client conditions will take precedence over EHF's default settings. Retention will not be indefinite merely because storage is inexpensive.

EHF will retain records for six months after an unsuccessful recruitment exercise closes; six years after a staff engagement ends for necessary core personnel records; and seven years after the relevant financial year or contract closes for financial and audit records. Research data will normally be retained for five years after project closure where justified and permitted. Identifiable contact lists and linkage keys will be deleted earlier when no longer needed. Raw recordings will normally be deleted within 90 days of transcript verification and agreed quality checks unless a documented protocol or lawful requirement justifies a different period. These will be organisational defaults, not claims of identical statutory periods.

Safeguarding and legal cases will have case-specific retention decisions, with specialist advice where necessary. Legal holds will suspend deletion of affected records. At closure, teams will

securely transfer authorised outputs, revoke access, remove unnecessary copies and record what remains, why and until when. Disposal will include secure shredding, digital deletion and sanitisation before equipment reuse. Backup deletion cycles will be documented and deleted records will not be restored for routine use.

Practical records and review

The focal point will maintain a processing register, retention schedule, supplier and transfer assessments, rights-request log, breach register and training records. The focal point will separate restricted case material from ordinary governance files. Access will be checked at least quarterly during active projects and after significant staff changes.

The Executive Lead will review implementation annually, including any NDPC registration, DPO, audit and return requirements. The policy will be revised after material legal changes, serious incidents or substantial new processing. EHF will not claim NDPC certification or registration without evidence.

Required record fields will include processing purpose and legal basis; data and affected people; roles and access; safeguards and permissions; hosting and transfer arrangements; retention and deletion dates; reviewer and approval. Incident records will include event and awareness times, risk assessment, notifications, action owners and closure evidence.

Legal and operational references

Nigeria Data Protection Act 2023 and NDPC resources

Nigeria Data Protection Act General Application and Implementation Directive 2025

NDPC official information and complaint routes

Approval and implementation

This policy will take effect on the approval date recorded below. The Board of Trustees, or a trustee with documented delegated authority, will approve the policy and record the operational appointments. An implicated person will not approve or oversee a case concerning themselves.

Approved by: Dr Kelly Elimian **Position**: President/Executive Director

Signature:  **Approval and effective date**: 1st July 2026

Operational focal point: Dr Florence Amiewalan **Direct contact:** +2348035090922

Independent trustee or alternate: Prof. Nosa Eghafona **Direct contact:** +2348034468560

Next review due: 1st June 2027 **Adoption record reference**: Board resolution dated 1st July 2026

Before implementation, the Executive Lead will confirm named contacts and access permissions, brief the people covered by this policy, establish the required records and communicate relevant reporting routes. No activity requiring prior safeguards or approval will begin until those controls are in place. Staff will acknowledge the policy at induction and after material revisions.