

PRIVACY POLICY

Applies To	The ACS Provider & Payer Portal ("Portal") and the ACS Member Application ("Member App") on iOS and Android, and all related ACS services
Effective Date	July 2026
Governing Law	Kenya Data Protection Act, 2019 and Data Protection (General) Regulations, 2021
Version	2.0

TABLE OF CONTENTS

1. Introduction
2. About Our Products — What They Do
3. What Is Personal Data?
4. ACS's Commitment to Data Protection
5. How Do We Protect Your Data?
6. Data Processing By Product & Function
 - A. ACS Provider & Payer Portal
 - B. ACS Member App
 - C. Claims Management & Payments
 - D. Biometric Verification
 - E. Call Centre & Customer Support
 - F. Marketing Communications
7. Where Is Your Data Processed?
8. Who Do We Share Data With?
9. Your Rights as a Data Subject
10. Children's and Dependents' Data
11. Data Retention
12. Contact, Data Protection Officer & Complaints
13. Updates to This Statement

1. INTRODUCTION

Afia Concept Solution Limited and its affiliates (together, and each of them as the context may require, "ACS", "we", "us", or "our") provide third-party administration (TPA) services for health insurance and healthcare financing schemes in Kenya. We enable insurers, employers, and other payers of healthcare (each a "Payer") to digitally administer their schemes, and enable members to access and manage their healthcare benefits through two distinct digital products:

- The ACS Provider & Payer Portal (the "Portal") — a web-based platform used by Payers, their contracted healthcare providers, and ACS administrators to set up and manage benefit policies, check member eligibility, process biometric verifications, manage pre-authorizations, adjudicate and track claims, and process payments.
- The ACS Member App, called My Afia Solution, (the "Member App") — a mobile application available on iOS and Android, used by scheme members to view their benefits and dependents, access the provider network, check their claims and pre-authorizations, and submit reimbursement claims.

This privacy policy applies to both products and all related services (together, the "Services"), and is intended for all individuals whose personal data is processed through the Services — including scheme members, their dependents, healthcare providers, Payer representatives, and ACS staff using the Portal on an administrative basis (together, "Users" or "you").

By using the Portal or Member App, or by having your information registered on either platform, you acknowledge that you have read and understood this policy. If you share personal data of another person with us (for example, a dependent covered under your scheme), you are responsible for informing them of this statement.

This statement does not cover the processing of your personal data by Payers, healthcare providers, or other third parties acting independently as data controllers. Please consult their respective privacy statements for that information.

2. ABOUT OUR PRODUCTS — WHAT THEY DO

2.1 ACS Provider & Payer Portal

The Portal is a secure, web-based benefits administration platform accessible to authorized users — including Payer administrators, contracted healthcare providers, and ACS operations staff. Through the Portal, users can:

- Policy setup: Configure and manage benefit schemes, policy terms, member limits, and exclusions on behalf of Payers
- Eligibility checks: Verify in real time whether a member is active and entitled to specific benefits at the point of care
- Biometric verification: Authenticate a member's identity using biometric data (such as fingerprint recognition) at participating provider facilities to prevent fraud and ensure benefit access by entitled members only
- Pre-authorization: Submit, review, and approve or decline pre-authorization requests for planned procedures, investigations, and specialist referrals
- Claims management: Submit provider claims, review claim documentation, adjudicate claims against benefit rules, and track claim status through to payment
- Payments: Process and record payments to healthcare providers in settlement of adjudicated claims

2.2 ACS Member App (My Afia Solution)

The Member App is a mobile application for individual scheme members. Through the App, members can:

- View their active benefits, cover limits, and remaining balances
- Manage and view dependent details covered under their scheme
- Access the network of contracted healthcare providers and locate facilities near them
- Check the status of their claims and pre-authorization requests
- Submit reimbursement claims directly, including uploading supporting documentation such as receipts and medical reports

3. WHAT IS PERSONAL DATA?

Personal data is any information that can be linked to an identified or identifiable natural person. Examples include your name, date of birth, national ID or passport number, telephone number, email address, physical address, membership or policy number, and photographs.

SENSITIVE PERSONAL DATA

Health information — including diagnoses, treatment records, procedure details, prescriptions, and medical history — is classified as sensitive personal data under Section 2 and Section 46 of the Kenya Data Protection Act, 2019. Biometric data, including fingerprint records used for member verification through the Portal, is also classified as sensitive personal data and is processed with additional safeguards and a specific legal basis. ACS treats both categories with a heightened standard of care beyond what is required for ordinary personal data.

Personal data we process may relate to you as a member or provider, or to any dependent covered under your scheme, where you have registered them through the Member App or they have been enrolled by your Payer. Where we do not need to identify you specifically — for example for service analytics or scheme-level reporting — we use anonymized or pseudonymized data, so that the information cannot be traced back to an individual.

4. ACS'S COMMITMENT TO DATA PROTECTION

We recognize that processing personal data — and particularly health and biometric data — in the context of healthcare benefit administration carries significant responsibilities. ACS is committed to handling your personal data lawfully, securely, and with respect for your right to privacy as guaranteed under Article 31 of the Constitution of Kenya, 2010.

ACS complies with the Kenya Data Protection Act, 2019 ("KDPA") and the Data Protection (General) Regulations, 2021, and is registered as a data controller and data processor with the Office of the Data Protection Commissioner ("ODPC") as required under the Act. We also align our internal practices with internationally recognized best practice, including relevant principles drawn from the EU General Data Protection Regulation (GDPR), where they raise the standard of protection for our Users.

4.1 Our Data Protection Principles

In accordance with Section 25 of the Data Protection Act, we ensure that personal data is:

Principle	What It Means in Practice
Lawful, fair & transparent	We process your data with a valid legal basis, treat you fairly, and tell you how we use your information through this statement
Purpose limitation	Data is collected for specified, explicit, and legitimate purposes and not used in a manner incompatible with those purposes
Data minimization	We collect only the data that is adequate and relevant to what is strictly necessary for the purpose
Accuracy	We take reasonable steps to ensure data is accurate and, where necessary, kept up to date
Storage limitation	We retain data only as long as is necessary for the stated purpose or as required by law (see Section 11)
Integrity & confidentiality	We apply appropriate technical and organizational security measures to protect data against unauthorized access, loss, or destruction

ACS enters into written data processing agreements with every third-party processor it engages, ensuring that any organization processing personal data on our behalf is bound by obligations equivalent to those imposed on ACS by the Data Protection Laws.

5. HOW DO WE PROTECT YOUR DATA?

Your personal data — especially health and biometric data — is treated with the strictest confidentiality and is accessed only by authorized persons with a legitimate need. We apply the following technical and organizational measures:

- End-to-end encryption of personal data in transit between the Member App or Portal and our servers, using industry-standard TLS protocols
- Encryption of sensitive data at rest, particularly health records, biometric data, and payment information
- Role-based access controls on the Portal, ensuring that only authorized staff — such as ACS claims assessors, care managers, and scheme administrators — can access member data relevant to their function
- Multi-factor authentication for Portal users to prevent unauthorized account access
- Secure biometric data storage, with fingerprint templates stored in encrypted, access-restricted environments separate from other member data
- Pseudonymization of data used for analytics, scheme reporting, and service improvement, so that analysis can be conducted without exposing individually identifiable information
- Contractual confidentiality obligations incorporated into every ACS employment contract and every third-party processor agreement
- Regular staff training on data protection, including mandatory certification for staff who access sensitive health and claims data
- System access logging and audit trails to detect and investigate unauthorized access or anomalous activity

6. DATA PROCESSING BY PRODUCT & FUNCTION

This section explains what personal data we process, why, on what legal basis, and in what capacity (controller or processor), for each key function of our two products.

A. ACS Provider & Payer Portal

(i) Policy Setup & Benefit Configuration

When a Payer onboards a scheme onto the Portal, ACS configures benefit policies, member groups, cover limits, and scheme rules. This involves processing member lists — including names, national ID numbers, membership numbers, dates of birth, genders, employer details, and dependent information — provided to ACS by the Payer.

ACS's role	Data processor acting on behalf of the Payer, who is the data controller
Legal basis	Performance of the contract between you and the Payer, and between the Payer and ACS
Who to contact	For questions about this processing, contact your Payer unless ACS has been appointed to handle member queries, in which case contact us via Section 12

(ii) Eligibility Checks

When a member presents at a contracted healthcare provider, the provider uses the Portal to verify in real time whether the member is active and entitled to cover for the requested service. This involves processing the member's name, membership number, national ID, date of birth, scheme details, benefit balances, and active dependent list.

ACS's role	Data processor on behalf of the Payer; controller for the eligibility response presented to the provider
Legal basis	Performance of the contract between you and the Payer; legitimate interest of the Payer and ACS in preventing fraud and ensuring benefits reach entitled members only

(iii) Pre-Authorization Management

Healthcare providers submit pre-authorization requests through the Portal for planned procedures, specialist referrals, and high-cost investigations. ACS's clinical and operations team reviews the request, applies benefit and clinical criteria, and approves or declines accordingly. This process involves the member's identity data, diagnosis codes (ICD-10), procedure codes, clinical notes, referral letters, and relevant medical history submitted by the provider.

ACS's role	Data processor on behalf of the Payer for pre-auth decisions on Payer-branded schemes; controller for ACS-administered schemes where ACS makes the clinical determination
Legal basis	Performance of the contract between you and the Payer; and, for urgent or emergency pre-authorisations, the protection of your vital interests where immediate clinical action is required

HEALTH DATA IN PRE-AUTHORISATION

Clinical documentation submitted in support of a pre-authorization request — including diagnoses, procedure details, and medical history — is sensitive personal data under the KDPA. Access to this data on the Portal is restricted to ACS clinical staff (including Care Managers and Claims Assessors) and relevant Payer personnel with a legitimate need. It is not accessible to provider staff beyond what they submitted.

B. ACS Member App

(i) Member Registration & Account

To create a Member App account and access your benefits, ACS processes the following data, which may be pre-populated from enrollment data provided by your Payer, or entered by you during registration:

- Full name, date of birth, gender, and photograph (where applicable)
- National ID or passport number, and mobile phone number
- Policy or membership number, scheme name, and employer (where applicable)
- Email address (for account access and correspondence)

ACS's role	Controller of account and profile data held within the Member App; processor on behalf of the Payer for scheme-specific data
Legal basis	Performance of the contract with you to access and manage your healthcare benefits

(ii) Benefits, Dependents & Provider Network

Through the Member App, you can view your active benefits, cover limits, remaining balances, and the dependents enrolled under your scheme. You can also browse the network of contracted healthcare providers. This requires ACS to display your scheme's configured benefits and the provider directory, which includes provider names, locations, contact details, and specialties. No additional personal data is collected for these browsing functions beyond your authenticated account details.

(iii) Claims & Pre-Authorization Status

The Member App allows you to track the status of claims and pre-authorization requests associated with your membership. You can view the date, provider, service category, amount billed, amount approved, and current status (e.g. submitted, under review, approved, paid, declined). The underlying clinical detail of a claim is viewable only by you as the member (and your Payer), not by other users.

(iv) Reimbursement Claim Submission

Where you have paid for a healthcare service out-of-pocket and wish to claim reimbursement through your scheme, the Member App allows you to submit a reimbursement claim directly. This involves uploading:

- The name of the healthcare provider visited, date of service, and type of service
- The total amount paid, along with supporting receipts, invoices, or payment proof

- A prescription, referral letter, or medical report (where required by your scheme for the type of service claimed)

ACS processes this documentation to assess, adjudicate, and settle your reimbursement claim in accordance with your scheme's benefit rules. Medical and clinical documentation uploaded as part of a reimbursement claim is sensitive personal data and is handled accordingly.

ACS's role	Processor on behalf of the Payer for claims adjudication; controller for the processing involved in receiving, reviewing, and responding to the submission through our platform
Legal basis	Performance of the contract between you and your Payer; and, for health data specifically, the necessity of processing for reasons of preventive or occupational medicine, assessment of working capacity, or provision of health care services, as provided under Section 46(d) of the KDPA

C. Claims Management & Payments

Beyond individual claim submissions through the Member App, ACS manages a full end-to-end claims lifecycle through the Portal. This includes receiving provider claims (submitted directly by facilities), reviewing supporting documentation, adjudicating claims against benefit rules and policy terms, and processing payments to providers. Data processed in this function includes:

- Member identity and benefit data (verified via the Portal at the point of care)
- Provider identity and banking or mobile money payment details
- Itemized bill of services rendered, including procedure codes, medication lists, and billed amounts
- Clinical documentation: diagnoses (ICD-10 codes), medical notes, investigation results, and treatment records submitted by the provider in support of the claim
- Payment reference data: payment amounts, dates, recipient accounts, and settlement confirmation

ACS's role	Processor on behalf of the Payer for Payer-branded schemes; controller and processor jointly with the Payer for ACS-administered schemes
Legal basis	Performance of the contract between you and the Payer, and between ACS and the Payer and provider; legal obligation (Insurance regulatory and financial reporting requirements)

D. Biometric Verification

Where required by your Payer or scheme, the Portal supports biometric verification — using your fingerprint — to confirm your identity at the point of care at participating provider facilities. This is used to prevent fraud and ensure that healthcare benefits are accessed only by the enrolled member or their covered dependents.

- Your fingerprint template is collected and enrolled during your first visit to a participating provider facility
- On subsequent visits, your fingerprint is scanned and matched against the stored template to verify your identity before benefit access is granted
- Fingerprint templates are stored in encrypted, access-restricted environments, separate from other personal and health data

- Biometric data is never shared with any party other than ACS and the Payer under whose scheme you are enrolled, and only for the purpose of identity verification and fraud prevention

Legal basis	Your explicit consent, obtained at the point of enrolment; and, where processing is required by the Payer's scheme rules as a condition of cover, the performance of your contract with the Payer
--------------------	---

EXTRA PROTECTION FOR BIOMETRIC DATA

Biometric data is among the most sensitive categories of personal data recognised under Kenyan law. ACS applies additional controls to biometric templates including encryption at rest, strict access limitation, and regular security audits. Biometric data is retained only for as long as your scheme is active and for a reasonable period thereafter to facilitate scheme re-enrolment, after which it is securely and permanently deleted.

E. Call Centre & Customer Support

When you contact ACS through our call centre, the Member App's in-app support function, or by email, we process the personal data necessary to verify your identity, understand and resolve your query, and keep a record of the interaction for quality assurance, training, audit, and dispute resolution purposes. This may include health-related or claims-related information you share in the course of describing your query.

Telephone calls to our call centre may be recorded. Where a call is recorded, you will be informed of this at the start of the call. Call recordings are retained for a limited period for the purposes above, after which they are securely deleted.

Legal basis	Performance of contract; legitimate interest of ACS in maintaining service quality, resolving disputes, training clinical and non-clinical staff, and fulfilling regulatory requirements
--------------------	--

F. Marketing Communications

With your consent, or where you are an existing member and the communication relates to a similar service, we may use your name, email address, and mobile number to share information about new ACS products, scheme benefits, wellness programs, or to invite your feedback on your experience with the Portal or Member App.

You may opt out of marketing communications at any time — at no cost — using the notification settings in the Member App, the unsubscribe link in any email, or by contacting us using the details in Section 12. Opting out of marketing does not affect your ability to receive essential service notifications about your cover, claims, or account activity.

Legal basis	Your consent, or ACS's legitimate interest in communicating with existing members about related services (with an absolute right to opt out at any time)
--------------------	--

7. WHERE IS YOUR DATA PROCESSED?

ACS hosts its core systems — including the Portal and the Member App back-end infrastructure — on servers located in Kenya, in alignment with the data localization principle that personal data relating to Kenyan residents should, as far as practicable, be stored and processed within Kenya.

Where we engage cloud service providers, technology partners, or other processors located outside Kenya, we ensure that appropriate safeguards are in place before any cross-border transfer of personal data occurs, as required by Section 48 of the Data Protection Act, 2019. These safeguards may include:

- Contractual clauses with the receiving party that bind them to data protection standards equivalent to those under Kenyan law
- Confirmation that the receiving country or organization has been assessed as providing an adequate level of data protection
- Your explicit and informed consent to the specific transfer, where required

Health data, biometric data, and claims data processed through the Portal are, to the extent practicable, retained exclusively on Kenya-based infrastructure. Where cross-border processing is unavoidable for a specific operational function, we will update the information below accordingly.

CURRENT PROCESSING LOCATIONS

Portal & Member App data: Kenya-based cloud infrastructure. Certain analytics and support tools may process pseudonymized data in the European Union. You can contact us at any time for an up-to-date overview of specific processing locations and the safeguards in place.

8. WHO DO WE SHARE DATA WITH?

We share your personal data only where necessary to deliver the Services, and always under appropriate contractual and confidentiality safeguards. The following table sets out the categories of recipients and the purposes for which data is shared:

Recipient	Data Shared	Purpose
Payers (insurers, employers)	Member identity, eligibility, claims, pre-auth decisions, utilization data	Administration of your healthcare scheme; benefit settlement; regulatory and audit reporting
Healthcare providers (hospitals, clinics, pharmacies)	Member eligibility, active benefits, pre-auth status, and payment settlement data	To verify your entitlement at the point of care; to settle claims for treatment provided
Technology and platform partners (e.g. biometric system providers, payment processors)	The minimum data necessary to enable the specific platform function (e.g. biometric templates for verification, payment details for settlement)	To enable biometric identity verification, payment processing, and other core platform functions, under written data processing agreements
Cloud infrastructure and IT service providers	Platform data as hosted on their infrastructure	Hosting, maintenance, and security of the Portal and Member App, under strict written processor agreements
Regulators and public authorities	As required by law or regulatory direction	Compliance with the KDPA, Insurance Regulatory Authority requirements, NHIF/SHA regulations, and other applicable legal obligations
Fraud prevention and investigation bodies	Identity and claims data relevant to a specific investigation	Detection, investigation, and prevention of fraud, where there is a reasonable basis to suspect fraudulent activity
Professional advisors (auditors, legal counsel)	Limited data necessary for the specific advisory engagement	Legal advice, audit, and compliance reviews, subject to professional confidentiality obligations

WE DO NOT SELL YOUR DATA

ACS does not sell, rent, or trade your personal data — including your health data, biometric data, or claims information — to any third party for commercial purposes. We may share anonymised, non-identifiable aggregated data with Payers or partners for scheme analytics and service improvement, but this cannot be used to identify you as an individual.

9. YOUR RIGHTS AS A DATA SUBJECT

ACS is committed to facilitating the exercise of your rights under the Kenya Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021. The rights below apply where ACS is acting as a data controller in relation to your personal data. Where a Payer is the controller (for example, for scheme enrollment data provided to ACS), please contact the Payer to exercise your rights in relation to that processing, unless ACS has been appointed to handle such requests on the Payer's behalf.

Your Right	What It Means	How to Exercise It / Timeline
Right to be informed	To know how your data is collected, used, and shared — this statement fulfils this obligation	You have this right at all times; see this statement
Right of access	To request a copy of the personal data ACS holds about you, including what it is, why it is held, and with whom it has been shared	Submit a request to privacy@acs.co.ke ; ACS will respond within 21 days (as prescribed by the Data Protection (General) Regulations, 2021)
Right to rectification	To have inaccurate or incomplete personal data corrected. You may update certain data directly through the Member App; for other data, contact us	Contact us via the Member App or by email; ACS will respond within 21 days
Right to erasure	To request deletion of your personal data in certain circumstances — for example where it is no longer necessary for the purpose for which it was collected, or where it was unlawfully processed. This right is not absolute; we may need to retain certain data for legal or regulatory purposes	Submit a written request to privacy@acs.co.ke ; ACS will respond within 21 days
Right to restriction of processing	To request that we limit further processing of your data in certain circumstances, for example where you contest accuracy and we are verifying, or where processing is no longer necessary but you wish us to retain the data for a legal claim	Submit a written request to privacy@acs.co.ke
Right to object	To object to processing based on legitimate interest; and an absolute right to object to processing for direct marketing purposes at any time	For marketing: use in-app settings or the unsubscribe link in any communication. For other processing: submit a written request to privacy@acs.co.ke
Right to data portability	To receive certain personal data in a structured, commonly used, machine-readable format (such as a PDF or electronic file), where technically feasible	Submit a written request to privacy@acs.co.ke ; ACS will respond within 21 days
Right to lodge a complaint	To file a complaint with the Office of the Data Protection Commissioner (ODPC) if you believe your rights under the KDPA have been infringed	Contact the ODPC at www.odpc.go.ke or privacy@odpc.go.ke . We ask that you contact us first to allow us the opportunity to resolve your concern

To exercise any of these rights, you may contact ACS verbally or in writing using the details in Section 12. We may need to verify your identity before acting on your request, and may ask you to complete a short verification form. We will not charge a fee for a reasonable request, but may charge a reasonable administrative fee for repetitive or unfounded requests as permitted by law.

10. CHILDREN'S AND DEPENDENTS' DATA

Where a dependent covered under your healthcare scheme is a minor (a person under 18 years of age), ACS processes their personal data — including identity data and health information — as necessary to administer their benefit entitlements, on the basis of the consent and parental authority of the parent or guardian who enrolled them.

If you register a dependent minor through your Payer's enrolment process, you confirm that you are their parent or legal guardian, that you have authority to enroll them, and that you accept this privacy statement on their behalf. We will not knowingly process a minor's data without the consent of a parent or legal guardian.

The Member App is not designed for independent use by minors to create their own account. If you become aware that a child has accessed the Portal or Member App and submitted personal data without appropriate parental or guardian consent, please contact us immediately so we can review and take appropriate action.

11. DATA RETENTION

ACS retains personal data only for as long as is necessary for the purposes set out in this statement, including to comply with any applicable legal, regulatory, insurance, audit, or financial reporting requirements. The following schedule sets out our general approach by data category:

Data Category	Retention Period	Basis for Retention Period
Member registration & account data	Duration of active membership, plus 7 years from scheme expiry or as agreed with the Payer	Contractual obligation; IRA and financial audit requirements
Claims and pre-authorization records (including clinical documentation)	7 years from the date of the claim or pre-authorization decision, or as directed by the Payer	Insurance regulatory requirements; limitation periods for disputes and legal proceedings under Kenyan law
Biometric data (fingerprint templates)	Duration of active membership plus a reasonable re-enrolment grace period (not exceeding 7 years from scheme expiry), then permanently deleted	Explicit consent; necessity for fraud prevention during active cover; promptly deleted on expiry to minimize risk
Payment and financial records	7 years from the date of the transaction	Legal obligation under financial and tax regulations applicable in Kenya
Call recordings	Up to 1 year, unless the recording relates to a dispute or complaint, in which case until the matter is resolved	Quality assurance, training, and dispute resolution
Marketing preferences and opt-out records	Until you withdraw consent or opt out, plus 3 years thereafter to evidence the opt-out and prevent inadvertent re-contact	Legitimate interest; consent withdrawal records
Portal access and audit logs	3 years from the date of the log entry	Security monitoring, fraud investigation, and regulatory audit requirements
Member App usage analytics (pseudonymized)	12 months from collection	Service improvement; anonymized / pseudonymized so re-identification risk is minimal

Where retention is governed by a specific agreement between ACS and a Payer, the terms of that agreement — together with applicable law — will determine the retention period that applies to your data in that scheme context. You may contact us using the details in Section 12 for specific further information about the retention period applicable to your data.

When personal data is no longer required, ACS disposes of it securely — through permanent deletion of electronic records or secure physical destruction of any paper records — in accordance with our internal data disposal procedures.

12. CONTACT, DATA PROTECTION OFFICER & COMPLAINTS

12.1 Contact ACS

Where ACS is the controller of your personal data, the controlling entity is Afia Concept Solution Limited. For questions about this statement, to exercise any of your rights, or to report a suspected data breach, please contact us:

Entity	Afia Concept Solution Limited
Registered Address	Laiboni Centre, Lenana Road, P.O. Box 16531- 00100 GPO, Nairobi, Kenya
General Enquiries	info@acs.co.ke 0709 200000
Data & Privacy Queries	privacy@acs.co.ke
Member App Support	Via the in-app Help & Support function, or email customer@acs.co.ke
Website	www.acs.co.ke

12.2 Regulatory Complaints

If you are not satisfied with how we have handled your personal data or responded to a rights request, you have the right to lodge a complaint with the Office of the Data Protection Commissioner (ODPC):

Regulator	Office of the Data Protection Commissioner (ODPC)
Website	www.odpc.go.ke
Email	privacy@odpc.go.ke
Address	Britam Towers, 12th Floor, Hospital Road, Upper Hill, Nairobi, Kenya

We would welcome the opportunity to address and resolve any concern you have directly before a regulatory complaint is submitted, and we undertake to treat all complaints promptly, transparently, and fairly.

13. UPDATES TO THIS STATEMENT

ACS may update this privacy statement from time to time to reflect changes in our Services, our data processing practices, or applicable law. We will notify you of material changes — particularly those that affect how we process your health or biometric data — through a notification in the Member App, by SMS or email to your registered contact, or by a prominent notice on the Portal, before the changes take effect.

Your continued use of the Portal or Member App following notification of any changes constitutes your acknowledgement of the updated statement. The effective date at the top of this document indicates when the current version was last updated. We recommend reviewing this statement periodically.

AFIA CONCEPT SOLUTION LIMITED | PRIVACY STATEMENT | VERSION 2.0 | JULY 2026