

AfyaApp — Legal Pack

Terms & Conditions and Privacy Policy for patients and health facilities in the Republic of Kenya. Last updated 5 August 2026. Available online at <https://afyaapp.store/terms> and <https://afyaapp.store/privacy>.

This document is maintained by the app owner to explain how medical records and personal data are handled on AfyaApp. It is not legal advice, and it is not a certification, accreditation or audit by any government body.

Part A — Terms & Conditions

1. Legal framework

AfyaApp is operated in Kenya and is designed to be used in accordance with, among others:

- The Constitution of Kenya, 2010 — Article 31 (privacy) and Article 43 (health).
- The Health Act, No. 21 of 2017 — Sections 8–13 on health information, confidentiality of patient records and conditions for disclosure.
- The Data Protection Act, No. 24 of 2019 and the Data Protection (General) Regulations, 2021 — health data as sensitive personal data.
- The Social Health Insurance Act, No. 16 of 2023 — Social Health Authority (SHA) membership and claims data.
- The Computer Misuse and Cybercrimes Act, No. 5 of 2018 — unauthorised access to records.
- KMPDC and Nursing Council of Kenya professional conduct rules for practitioners entering clinical data.

2. Who the parties are

The patient is the **data subject**. The registered health facility that creates clinical entries is a **data controller** for the records it creates. AfyaApp acts as a **data processor** providing the technical platform, and as a controller only for account and security data needed to run the service.

3. Eligibility and accounts

- Patients aged 18 and above register with a valid Kenyan National ID number.
- For patients below 18 years a birth certificate number is required, and the account must be opened and operated by a parent or legal guardian.
- Health facilities must be licensed in Kenya and must submit a valid licence for verification before creating clinical records.
- You are responsible for keeping your password and one-time codes confidential. Sharing login credentials is a breach of these terms.

4. Ownership and accuracy of medical records

Under the Health Act, 2017 the information in a health record belongs to the patient, while the record itself is held in trust by the health facility that created it. Clinical entries — diagnoses, prescriptions, lab results and uploaded documents — are **append-only**. They cannot be silently deleted, so the medical history remains a reliable clinical and legal record. Corrections are made

by adding a corrective entry, and every entry carries the attending practitioner's name and licence number.

A patient who believes a record is inaccurate may request rectification through the facility that created it, and may escalate to the Office of the Data Protection Commissioner (ODPC).

5. Consent to access records

- A facility may only view a patient's records where the patient has granted consent on AfyaApp, where the facility created the record, or under the emergency provision in clause 6.
- Consent is specific, informed and may be revoked by the patient at any time from the patient portal.
- Revoking consent does not delete records already lawfully created, and does not undo lawful disclosures already made.

6. Emergency (break-glass) access

Section 11 of the Health Act, 2017 permits disclosure of health information without the patient's consent where necessary to prevent a serious threat to the health or life of the patient or another person. AfyaApp implements this as a break-glass action which:

- requires the practitioner to state a reason before access is granted;
- grants time-limited access only;
- is permanently logged with the facility, the user, the reason and the timestamp;
- is visible to the patient and to platform administrators for review.

Misuse of break-glass access may amount to an offence under Kenyan law and will result in suspension of the facility's account.

7. Data storage, security and retention

- Records are transmitted over encrypted connections and stored in access-controlled databases and private file storage.
- Access is enforced per-account: a facility can only reach the records it is entitled to under clause 5 or 6.
- Health records are retained in line with Kenyan health records retention practice — adult records for at least 6 years from the last entry, and records of minors until at least 6 years after they turn 18 — unless a longer period is required by law.
- Where personal data is stored or processed outside Kenya, it is done in line with Sections 48 and 49 of the Data Protection Act, 2019.

8. Your rights as a data subject

Under Part V of the Data Protection Act, 2019 you may request to:

- be informed of the use of your personal data;
- access your personal data held on AfyaApp;
- have inaccurate or misleading data corrected;
- object to processing, or request deletion of data that is no longer required by law to be kept;
- lodge a complaint with the Office of the Data Protection Commissioner.

9. SHA membership data

Where you add a Social Health Authority membership number, it is used only to link your visits, prescriptions and lab results to your cover. AfyaApp is not the SHA, does not decide benefits or claims, and does not guarantee that a claim will be honoured.

10. Acceptable use

- Do not access, copy or share another person's health record without lawful basis.
- Do not upload false, defamatory or unlawful content.
- Do not attempt to bypass access controls, scrape data, or interfere with the platform.

11. No emergency or clinical substitute

AfyaApp is a records platform. It does not provide diagnosis or treatment and must not be relied on in a medical emergency. In an emergency, call your nearest health facility or emergency service immediately.

12. Availability and liability

The service is provided on an “as available” basis. To the extent permitted by Kenyan law, AfyaApp is not liable for clinical decisions made by practitioners, for data entered incorrectly by a facility, or for loss arising from connectivity failures. Nothing in these terms excludes liability that cannot be excluded by law.

13. Suspension and termination

Accounts may be suspended where these terms are breached, where a facility's licence is not verified or lapses, or where access logs indicate misuse. Medical records are retained as required under clause 7 even after an account is closed.

14. Changes to these terms

These terms may be updated to reflect changes in Kenyan law or in the service. Material changes will be notified in the app, and continued use after the effective date is acceptance of the updated terms.

15. Governing law and contact

These terms are governed by the laws of Kenya and disputes are subject to the jurisdiction of the Kenyan courts. For privacy requests, security reports or questions about these terms, contact the app owner through the support channel shown in your portal.

Part B — Privacy Policy

1. Legal basis and framework

AfyaApp processes personal data in accordance with, among others:

- The Constitution of Kenya, 2010 — Article 31, the right to privacy.
- The Data Protection Act, No. 24 of 2019 and the Data Protection (General) Regulations, 2021 — health data is **sensitive personal data** under Section 2.
- The Health Act, No. 21 of 2017 — Sections 8–13 on confidentiality of patient information and lawful disclosure.
- The Social Health Insurance Act, No. 16 of 2023 — SHA membership data.
- The Computer Misuse and Cybercrimes Act, No. 5 of 2018.

Our lawful bases under Sections 30 and 45 of the Data Protection Act are: your consent, performance of the service you asked for, compliance with a legal obligation, provision of health care by a licensed practitioner under a duty of confidentiality, and protection of the vital interests of a data subject in an emergency.

2. Who is responsible for your data

The patient is the **data subject**. Each registered health facility is a **data controller** for the clinical records it creates. AfyaApp is a **data processor** for those records, and a controller only for the account, authentication and security data needed to operate the platform.

3. What we collect

- **Identity data:** full name, National ID number, birth certificate number for patients under 18, date of birth, gender.
- **Contact data:** email address and phone number used for sign-in codes and account recovery.
- **Health data:** diagnoses, prescriptions, lab results, uploaded medical documents, blood group, weight and height.
- **Insurance data:** Social Health Authority (SHA) membership number.
- **Facility data:** hospital name, registration and licence details, and the name and licence number of the practitioner making an entry.
- **Profile media:** an optional profile photograph, stored privately.
- **Technical and audit data:** sign-in events, consent grants and revocations, and emergency (break-glass) access logs with the reason given.

4. How we use it

- To create and secure your account, including one-time codes sent to your email.
- To let you and the facilities you authorise view an accurate, continuous medical history.
- To let licensed facilities record diagnoses, prescriptions, lab results and documents.
- To link your care to your SHA cover where you provide a membership number.
- To verify that a facility is licensed before it can create clinical records.
- To keep audit logs so that access to your records can be reviewed.

We do not sell personal data, and we do not use your health data for advertising or profiling.

5. Who can see your records

- You, the patient, at any time from your portal.
- A health facility that created the record.
- A health facility to which you have granted consent — consent is specific, informed, and revocable at any time from the patient portal.
- A practitioner invoking emergency (break-glass) access under Section 11 of the Health Act, 2017. This is time-limited, requires a stated reason, and is permanently logged and visible to you.
- Platform administrators, strictly for verification, security and abuse review.

Revoking consent stops future access; it does not delete records already lawfully created.

6. Processors and third parties

We use a small number of service providers strictly to run the platform: cloud database, authentication and encrypted file storage; a transactional email provider to deliver one-time sign-in and password reset codes; and Google, only where you choose to sign in with a Google account. These providers act on our instructions and are bound by confidentiality and data protection obligations. We do not share health data with advertisers, insurers or employers.

7. Transfers outside Kenya

Some infrastructure providers may process data outside Kenya. Where this happens it is carried out in line with Sections 48 and 49 of the Data Protection Act, 2019 — on the basis of appropriate safeguards, contractual protections, and confirmation that the data will receive an adequate level of protection.

8. Security

- All traffic is transmitted over encrypted (HTTPS/TLS) connections.
- Records are held in access-controlled databases with row-level access rules enforced per account.
- Medical documents and profile photos are kept in private storage reachable only through short-lived signed links.
- Sign-in requires a password plus a one-time code sent to your registered email, valid for 15 minutes.
- Passwords and one-time codes are stored only in hashed form.
- Emergency access and consent changes are permanently logged.

9. Retention

Health records are retained in line with Kenyan health records retention practice — adult records for at least 6 years from the last entry, and records of minors until at least 6 years after they turn 18 — unless a longer period is required by law. Clinical entries are append-only: corrections are made by adding a corrective entry rather than erasing history. Account, authentication and audit data is kept for as long as the account is active and for a reasonable period afterwards for security and legal purposes. One-time codes are deleted or expired within 15 minutes.

10. Your rights

Under Part V of the Data Protection Act, 2019 you have the right to:

- be informed of how your personal data is used;
- access the personal data we hold about you;
- request correction of inaccurate or misleading data;
- object to processing, or request deletion of data we are not legally required to keep;
- request a copy of your data in a portable format;
- withdraw consent given to a facility at any time;
- lodge a complaint with the Office of the Data Protection Commissioner (ODPC).

To exercise a right, use the support channel shown in your portal. We respond within the timelines set by the Data Protection (Complaints Handling) Regulations.

11. Children's data

Accounts for patients under 18 must be opened and operated by a parent or legal guardian, and a birth certificate number is required. Consent for processing a child's health data is given by the guardian, in line with Section 33 of the Data Protection Act, 2019.

12. Cookies and offline storage

AfyaApp uses only the storage needed to run the service: a session token to keep you signed in, and — on the installable app — an offline cache so your own records remain readable during poor connectivity. Cached data is stored on your device and cleared when you sign out or uninstall the app. We do not use advertising or cross-site tracking cookies.

13. Data breaches

Where a breach poses a real risk of harm, we will notify the Office of the Data Protection Commissioner within 72 hours of becoming aware of it, and notify affected data subjects without undue delay, as required by Section 43 of the Data Protection Act, 2019.

14. Changes and contact

This policy may be updated to reflect changes in Kenyan law or in the service. Material changes will be notified in the app. For privacy requests, security reports or questions about this policy, contact the app owner through the support channel shown in your portal. You may also complain to the Office of the Data Protection Commissioner, Kenya.