Privacy Policy

Revision dated 15 November 2026

1. Scope and who we are

FortyPharma is a web and mobile pharmacy-management service provided by FortyHives Innovations Ltd, Crown Plaza, Room 12, Kutus, Kirinyaga County, Kenya. This Privacy Policy applies to the FortyPharma website, web console, mobile applications, support channels and related services.

This policy is intended to provide clear information consistent with the Kenya Data Protection Act, 2019, the Data Protection (General) Regulations and internationally recognised privacy principles. Additional rights may apply under laws such as the EU General Data Protection Regulation, the UK GDPR or other local privacy laws when their territorial requirements are met.

FortyPharma is a product of FortyHives Innovations Ltd. Our business address is Crown Plaza, Room 12, Kutus, Kirinyaga County, Kenya. Contact: support@fortycare.com; +254 718 505 072; fortycare.com.

2. Controller and processor roles

Our privacy role depends on the information and the context in which it is processed:

FortyPharma as controller: we determine how account registration, subscription, billing, website, security, support and service-usage information is processed.

Customer business as controller: the subscribing business determines why and how it records information about its customers, suppliers, staff and transactions in FortyPharma.

FortyPharma as processor or service provider: we process business records on the subscribing business’s instructions to host and provide the service.

Business responsibility: each subscribing business must provide required notices, establish a lawful basis and configure staff access appropriately for personal data it enters into FortyPharma.

Business personal-data processing is governed by section 26 of the Terms of Service and any applicable signed data-processing agreement. The customer’s notices must also explain its own processing; this Privacy Policy does not replace them.

FortyPharma customers, including pharmacies, determine the purposes for which they collect and use patient and dispensing records. FortyHives processes those records on the customer’s documented instructions to provide the contracted service. Each party must apply its respective obligations for sensitive health data under applicable law.

3. Personal data we collect

Category · Examples

Account and identity · Name, business name, email address, phone number, username, role, language and account identifiers.

Subscription and billing · Plan, payment reference, payment status, invoice and receipt records, billing history and tax-related information.

Business content · Products, prices, branches, staff roles, customers, suppliers, sales, purchases, expenses, inventory, invoices, statements and reports entered by authorised users.

Support and communications · Questions, tickets, WhatsApp, telephone or email communications, feedback and troubleshooting information.

Technical and security · IP address, device, browser, operating system, session, login, audit, error, diagnostic and security-event information.

Website and analytics · Consent choice, referring page, campaign parameters, page engagement and conversion actions when analytics consent is provided.

Connected services · Identifiers, status information and records received from integrations or providers authorised by the customer, subject to their terms.

Required identity, contact, authentication and billing fields are identified in the relevant form or order. If required information is not provided, we may be unable to create or secure the account, fulfil an order, issue required records or provide the requested feature. Optional feedback and marketing choices are not conditions of core service access. Business administrators may supply data about their staff or contacts; those individuals should also consult the business's privacy notice.

Customer records may include patient identifiers, prescriptions, medicines supplied, dispensing records and related health information. Partner programme records may include referral codes, onboarding assignments, commission records and payout details. Keep patient records out of routine support messages, referral submissions and marketing materials.

4. Sources of personal data

Directly from account holders, administrators, staff users and people who contact us.

From the subscribing business when it creates users or enters business records.

Automatically from devices, browsers, logs, cookies and similar technologies.

From payment providers, app stores or integrated services when required to verify a transaction or provide a requested feature.

From authorised representatives, professional advisers, regulators or lawful public authorities where appropriate.

5. Purposes and lawful bases

We process personal data only where there is a valid purpose and lawful basis. The applicable basis depends on the activity and jurisdiction.

Purpose · Typical lawful basis

Provide accounts, subscriptions, applications, support and requested functionality · Performance of a contract or steps requested before entering a contract.

Operate authentication, permissions, audit trails, fraud prevention and service security · Contract necessity, legitimate interests and compliance with legal obligations.

Process payments, invoices, receipts, tax records and financial administration · Contract necessity and legal obligations.

Maintain, troubleshoot and improve reliability and usability · Legitimate interests, provided those interests do not override individual rights.

Send essential service, security, billing and policy notices · Contract necessity, legal obligations and legitimate interests.

Send optional marketing messages · Consent where required, or legitimate interests where permitted with an effective opt-out.

Use non-essential analytics · Consent through the website consent control.

Respond to legal requests and protect rights, safety and property · Legal obligations and legitimate interests.

Where processing is based on consent, consent may be withdrawn at any time without affecting processing that was lawful before withdrawal.

Our legitimate interests are protecting users and the service against fraud and misuse, maintaining reliable systems, resolving support issues and defending legal rights. We consider necessity and the impact on individuals before relying on that basis. A business contract does not automatically provide a contractual lawful basis for every employee's or customer's personal data; we use an appropriate basis for the individual and processing activity.

6. Sharing and service providers

We do not sell personal data for money. We may disclose only the information reasonably necessary to:

Hosting, infrastructure, database, communications, analytics, payment, app-store and customer-support providers that help deliver FortyPharma.

Professional advisers, auditors and insurers under confidentiality duties.

A buyer, investor or successor in a proposed or completed restructuring, subject to appropriate protections.

Courts, regulators, law-enforcement agencies or other parties where disclosure is legally required or necessary to protect rights and safety.

A third party connected by a customer or user, where the customer has instructed or authorised the connection.

Service providers are expected to process information only for agreed purposes and to apply appropriate confidentiality and security measures. Details of material provider categories may be requested through the privacy contact below.

7. International data transfers

FortyPharma and its service providers may process information in countries other than the country in which the user is located. Where a transfer is restricted by applicable law, we will use a legally recognised transfer basis and appropriate safeguards, such as adequacy decisions, contractual protections, approved transfer clauses, consent where valid, or another permitted mechanism.

No transfer mechanism eliminates every risk. We assess the nature of the information, destination, provider and available safeguards when determining an appropriate approach.

Contact support@fortycare.com for the relevant provider categories, processing locations and information on the safeguards applicable to your data, including how to obtain a copy where available. A statement in this policy does not itself authorise a restricted transfer. Any required transfer agreement, assessment, regulator approval or other safeguard must be in place before the restricted processing occurs. The protections and mechanisms applicable to Kenyan, EEA and UK transfers may differ.

8. Retention and deletion

We retain personal data only for as long as reasonably necessary for the relevant purpose, contract, security need or legal obligation. Retention depends on the record type, account status, dispute risk and statutory requirements.

Record type · Retention approach

Active account and business content · Retained while the account is active and as needed to provide the service.

Billing, tax and financial records · Retained for the period required by accounting, tax, audit and legal obligations.

Support and security records · Retained as needed to resolve issues, investigate misuse, maintain auditability and protect legal rights.

Marketing preferences · Retained as needed to respect opt-in or opt-out choices.

Analytics and technical data · Retained according to configured service settings and then deleted, aggregated or anonymised where appropriate.

Closed accounts · Deleted, anonymised or restricted after applicable operational and legal retention periods, unless longer retention is required for a claim, investigation or legal duty.

Businesses should export records required for accounting, tax or operational purposes before expiry, cancellation or deletion. Backup copies may persist for a limited period until overwritten in the ordinary backup cycle.

Retention is assessed separately for each purpose. Account closure starts review of business content for return or deletion; statutory accounting records, substantiated security investigations, unresolved disputes and evidence of agreement may require separate restricted retention. Once those reasons end, records should be deleted or irreversibly anonymised. Access to retained closed-account information is limited to the relevant purpose. You may request the criteria or applicable period for a particular record; a retention period is not extended merely because storage is available.

9. Security and personal-data breaches

We use reasonable administrative, technical and organisational measures designed to protect personal data, including access controls, role permissions, authentication, logging, change management, infrastructure protections and incident-response procedures appropriate to the service and risk.

No online system is completely secure. Users must protect credentials, maintain secure devices, review staff permissions and notify us promptly of suspected unauthorised access. Where a personal-data breach triggers a legal notification duty, we will notify the relevant authority and affected individuals as required by applicable law.

10. Your privacy rights

Depending on applicable law and our role, individuals may have rights to:

Be informed about the collection and use of personal data.

Request access to personal data and obtain a copy where applicable.

Request correction of inaccurate or incomplete information.

Request deletion or erasure where the legal conditions are met.

Request restriction of processing or object to certain processing.

Withdraw consent where consent is the lawful basis.

Receive certain information in a portable format where the right applies.

Object to direct marketing at any time.

Complain to the Office of the Data Protection Commissioner in Kenya or another competent supervisory authority.

When FortyPharma acts only as a processor for a subscribing business, requests concerning that business's records should normally be directed to the business first. We will assist the business as required. We may verify identity, request clarification and refuse or charge for requests only where permitted by law, such as requests that are manifestly unfounded or excessive.

Send a request to support@fortycare.com with "Privacy Request" in the subject, the right you wish to exercise and enough information to locate the records. An authorised representative may act for you subject to proportionate verification. We will respond within the deadline applicable to the particular right and jurisdiction and explain any lawful extension, restriction or refusal. Where EU or UK GDPR applies, requests are generally answered within one month, with a permitted extension for complexity or number of requests explained within that first month; shorter Kenyan deadlines apply where required. Exercising a right does not require purchasing a service.

Object to direct marketing at any time. Use the message's opt-out method or email support@fortycare.com. Withdraw optional consent through the relevant preference control or that email address; withdrawing consent is as easy as giving it. These choices do not stop messages necessary for account security, billing or service delivery. Accepting Terms or acknowledging this notice does not opt you into marketing.

11. Cookies, local storage and analytics

The FortyCare website, FortyPharma console and apps use essential cookies or local storage for functions such as sign-in, security and preferences. You can manage browser storage in your browser settings. Clearing or blocking essential storage can affect sign-in and other functions.

Where optional analytics is enabled, we use it to understand website use and improve the service. We apply any consent requirement that applies to that measurement. Patient records, prescriptions and authentication secrets must be kept out of analytics and tracking tools.

12. Marketing communications

We may send product information, updates or offers where permitted by law. Marketing messages will identify FortyPharma or FortyHives Innovations Ltd and provide a reasonable method to opt out. Opting out of marketing does not stop essential account, security, billing or service communications.

13. Automated decision-making

The service uses rules to manage access, subscriptions and trial eligibility. If a decision based solely on automated processing has legal or similarly significant effects on you, applicable data-protection rights and safeguards apply. Contact FortyCare to ask for information or request a review where available.

14. Children

FortyPharma is designed for businesses and authorised business users and is not intended for children to create independent accounts. A business that records information relating to a child must have an appropriate lawful basis and apply any additional protections required by law.

15. Changes to this policy

We may update this Privacy Policy to reflect service, provider, security, business or legal changes. Material changes will be communicated through the website, application, email or another appropriate channel. The updated effective date will appear at the top of the policy.

16. Contact, rights requests and complaints

Privacy requests and questions may be sent to support@fortycare.com, by telephone at +254 718 505 072, or through the account deletion request page. Include enough information to identify the account and the right being exercised, but do not send passwords or unnecessary sensitive information.

If a concern is not resolved, a person may lodge a complaint with the Office of the Data Protection Commissioner in Kenya or another competent authority in their jurisdiction. This right is not affected by contacting us first.

Related documents: Terms of Service and Refund Policy.

You may complain directly to Kenya’s Office of the Data Protection Commissioner. Where applicable, you may also contact the UK Information Commissioner or your competent EEA supervisory authority. You do not have to contact us first or waive other remedies.

Read this policy on FortyCare