Privacy Policy

Quecorex — Hospital, Clinic & Pharmacy Management Platform

Operated by Quecorex LLC • Effective Date: March 2, 2026 • Version 1.0

Data Controller	Quecorex LLC, a Delaware limited liability company
Platform	Quecorex (quecorex.com)
Privacy Contact	privacy@quecorex.com
Data Protection Officer	privacy@quecorex.com
Applicable Regulations	GDPR (EU) 2016/679 • NDPR (Nigeria) 2019 • HIPAA (USA) 45 CFR §164
Last Updated	March 2, 2026

1. WHO WE ARE

Quecorex is a hospital, clinic, and pharmacy management Software-as-a-Service (SaaS) platform developed and operated by Quecorex LLC, a company registered in the State of Delaware, United States of America.

Quecorex enables healthcare facilities — including hospitals, clinics, diagnostic centres, and pharmacies — to manage electronic patient records, pharmacy operations, radiology imaging, laboratory services, emergency department workflows, and hospital administration in a single integrated platform.

For the purposes of the EU General Data Protection Regulation (GDPR), Quecorex LLC acts as the Data Controller in respect of personal data processed through the Quecorex platform. Healthcare facilities that deploy Quecorex to manage their patients' data may act as independent Data Controllers, with Quecorex LLC acting as a Data Processor on their behalf under a Data Processing Agreement (DPA).

2. SCOPE OF THIS POLICY

This Privacy Policy applies to:

- Patients whose personal and health data is processed through Quecorex by a subscribing healthcare facility
- Clinicians, nurses, pharmacists, laboratory technicians, and other healthcare professionals using the platform
- Administrative staff of healthcare facilities using Quecorex
- Visitors to the Quecorex website (quecorex.com)
- Prospective customers and contacts who engage with Quecorex LLC for sales, support, or partnership purposes

This Policy applies regardless of where you are located. Where you are located in the European Economic Area (EEA), the United Kingdom, or another jurisdiction with data protection laws, additional rights and protections may apply as described in this Policy.

3. PERSONAL DATA WE COLLECT & PROCESS

3.1 Patient Data (Special Category / Health Data)

When a healthcare facility uses Quecorex to manage your care, we process the following categories of data on behalf of that facility:

- Identity data: full name, date of birth, gender, nationality, photograph (where provided)
- Contact data: residential address, telephone number, email address
- Identification data: national ID number, passport number, health insurance ID
- Clinical data: diagnoses, symptoms, medical history, treatment plans, clinical notes, allergies, immunisations
- Medication data: prescription records, dispensing history, controlled substance records
- Diagnostic imaging: DICOM files (X-ray, CT, MRI, ultrasound) and radiology reports
- Laboratory data: test orders, specimen records, results, and reference values
- Emergency data: triage category, presenting complaint, vital signs, disposition outcome
- Billing data: insurance details, invoices, payment records (payment card data processed by Stripe, not stored by Quecorex)

Health data is classified as Special Category Data under GDPR Article 9 and is afforded the highest level of protection under this Policy.

3.2 Staff & User Account Data

- Full name, job title, department, professional licence number
- Email address and contact details (for account access and notifications)
- Login credentials (passwords stored as bcrypt hashes; plaintext never retained)
- Activity logs (actions performed within the platform with timestamp and user ID)
- Payroll and HR data (for healthcare facilities using the HR module)

3.3 Website & Technical Data

- IP address, browser type, operating system, pages visited, referral source
- Cookies and similar tracking technologies (see Section 9)
- Enquiry and contact form submissions

4. HOW WE USE YOUR DATA & OUR LEGAL BASIS

We process personal data only where we have a lawful basis to do so. The table below summarises our primary processing purposes and the legal basis relied upon under GDPR:

Purpose	Legal Basis	Data Types Involved
Providing healthcare management services to subscribing facilities	Art. 6(1)(b) — Contract; Art. 9(2)(h) — Medical care	All patient and clinical data

Managing patient records and clinical documentation	Art. 6(1)(c) — Legal obligation; Art. 9(2)(h)	EMR/EHR, pharmacy, lab, radiology data
Delivering appointment and prescription notifications	Art. 6(1)(b) — Contract	Name, email, appointment reference
Emergency department processing where consent unavailable	Art. 6(1)(d) — Vital interests; Art. 9(2)(c)	Triage and emergency clinical data
Staff account management and access control	Art. 6(1)(b) — Employment contract	Staff identity and account data
Platform security monitoring and fraud prevention	Art. 6(1)(f) — Legitimate interests	System logs, IP address, activity data
Compliance with legal and regulatory obligations	Art. 6(1)(c) — Legal obligation	As required by applicable law
Telehealth consultation recordings (where consent given)	Art. 6(1)(a) — Consent; Art. 9(2)(h)	Video/audio, consultation notes
Marketing communications to prospects (opt-in only)	Art. 6(1)(a) — Consent	Name, email, organisation

5. HOW LONG WE KEEP YOUR DATA

We retain personal data only for as long as necessary for the purposes for which it was collected, or as required by applicable law. Our standard retention periods are:

- Patient clinical records: 10 years from last clinical encounter, or as required by applicable national health regulations, whichever is longer
- Diagnostic imaging (DICOM): 10 years; paediatric imaging retained until the patient turns 25 or 10 years after last contact, whichever is later
- Pharmacy and prescription records: 7 years (controlled substances as required by pharmaceutical law, typically 10+ years)
- Laboratory results: 7 years from date of result; longer for oncology or genetic testing
- Staff employment records: 7 years after end of employment
- System and access logs: 90 days for detailed logs; anonymised aggregates retained indefinitely
- Email delivery logs (AWS SES): 30 days
- Marketing contact data: until opt-out or 3 years of inactivity, whichever is sooner

At the end of the applicable retention period, personal data is securely deleted or anonymised in accordance with our data deletion procedure. Healthcare facilities may request early deletion subject to applicable legal obligations regarding medical recordkeeping.

6. WHO WE SHARE YOUR DATA WITH

6.1 Within the Healthcare Facility

Patient data is accessible only to authorised clinical and administrative staff of the subscribing healthcare facility, controlled by Role-Based Access Control (RBAC). Quecorex does not grant Quecorex LLC staff routine access to patient data.

6.2 Technology Sub-Processors

We use the following sub-processors to operate the Quecorex platform. Each sub-processor is bound by a Data Processing Agreement and, where applicable, a Business Associate Agreement (HIPAA):

Sub-Processor	Service	Data Processed

DigitalOcean	Cloud hosting & storage	All platform data (encrypted at rest)
Cloudflare	CDN, WAF, R2 object storage	DICOM imaging files, static assets, traffic
MongoDB Atlas	Database-as-a-Service	Clinical and operational data
Amazon Web Services	Transactional email (SES)	Recipient email, notification content
Stripe	Payment processing	Payment card data (PCI DSS compliant; not stored by Quecorex)

6.3 Legal Disclosures

We may disclose personal data to law enforcement, regulatory authorities, or courts where required by applicable law, a court order, or where necessary to protect the safety of individuals or prevent fraud. We will notify affected parties where legally permitted to do so.

6.4 What We Never Do

- We never sell your personal data to any third party
- We never share patient data with advertisers or marketing companies
- We never use patient health data for any purpose other than the delivery of the healthcare service

7. INTERNATIONAL DATA TRANSFERS

Quecorex infrastructure is hosted on DigitalOcean, Cloudflare, and Amazon Web Services, which may process data in the United States and other countries outside the EEA. Where personal data of EEA data subjects is transferred outside the EEA, we rely on one of the following safeguards:

- Standard Contractual Clauses (SCCs) approved by the European Commission under Article 46(2)(c) GDPR, incorporated into our agreements with each sub-processor
- Adequacy decisions of the European Commission, where applicable

Healthcare facilities deploying Quecorex for EU patients may request a copy of the relevant SCCs by contacting privacy@quecorex.com. Where technically feasible, EU data residency options (data stored in EU-region infrastructure) are available on request.

8. YOUR DATA PROTECTION RIGHTS

Depending on your location and the applicable law, you may have the following rights in relation to your personal data. For EU/EEA data subjects, these rights are guaranteed under the GDPR:

Your Right	GDPR Article	What This Means
Right to Access	Article 15	Request a copy of the personal data we hold about you
Right to Rectification	Article 16	Request correction of inaccurate or incomplete personal data
Right to Erasure	Article 17	Request deletion of your personal data (subject to legal retention obligations for medical records)
Right to Restriction	Article 18	Request that we limit how we use your personal data in certain circumstances
Right to Portability	Article 20	Receive your personal data in a structured, machine-readable format
Right to Object	Article 21	Object to processing based on legitimate interests or for direct marketing purposes
Right to Withdraw Consent	Article 7(3)	Withdraw consent at any time where processing is based on consent, without affecting prior processing
Rights re: Automated Decisions	Article 22	Not be subject to solely automated decisions that significantly affect you (Quecorex does not use such automated decision-making)

To exercise any of these rights, please contact us at privacy@quecorex.com. We will respond within 30 days. We may need to verify your identity before processing your request. If you are a patient of a healthcare facility using Quecorex, some requests may need to be directed to that facility as the primary Data Controller for your care.

If you are located in the EU/EEA and are not satisfied with our response, you have the right to lodge a complaint with your local supervisory authority. A list of EU supervisory authorities is available at: edpb.europa.eu/about-edpb/about-edpb/members_en

9. COOKIES & TRACKING TECHNOLOGIES

The Quecorex web application and website (quecorex.com) use cookies and similar technologies. We use the following categories of cookies:

- Strictly necessary cookies: Required for the platform to function (session management, authentication tokens, security). These cannot be disabled.
- Functional cookies: Remember your preferences and settings to improve your experience.
- Analytics cookies: Pseudonymised data on how the platform is used, to improve performance. Used only with your consent.
- Marketing cookies: Used on the public website only for understanding campaign effectiveness. Used only with your consent.

You can manage cookie preferences at any time via the cookie settings panel on the Quecorex website. Strictly necessary cookies cannot be refused as they are essential to the operation of the platform. Withdrawing consent for non-essential cookies will not affect your access to healthcare services.

10. HOW WE PROTECT YOUR DATA

We implement industry-standard technical and organisational security measures to protect personal data against unauthorised access, loss, alteration, or disclosure. Our security programme includes:

- Encryption of all personal data in transit using TLS 1.2/1.3 and at rest using AES-256
- Role-Based Access Control (RBAC) ensuring staff access only the data necessary for their role
- Multi-factor authentication (MFA) for administrative accounts
- Comprehensive audit logging of all access to personal and health data
- Cloudflare Web Application Firewall (WAF) and bot management
- Regular security assessments and infrastructure monitoring via Grafana/Loki/Prometheus
- HIPAA-aligned infrastructure and Business Associate Agreements with all relevant vendors
- Annual HIPAA Security Risk Assessment (see our Security & Trust page)

While we take all reasonable steps to protect your data, no system is entirely immune from risk. In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify you and the relevant supervisory authority in accordance with our legal obligations (within 72 hours under GDPR).

11. CHILDREN'S DATA

Quecorex may process health data of minors (persons under 18) as part of paediatric clinical care provided by subscribing healthcare facilities. Such processing occurs solely under the lawful basis of Article 9(2)(h) GDPR (medical care) and is governed by the policies of the relevant healthcare facility.

The Quecorex platform and website are not directed at children for independent use. We do not knowingly collect personal data from children for marketing or non-clinical purposes.

12. NIGERIA DATA PROTECTION REGULATION (NDPR)

For users and patients located in Nigeria, Quecorex processes personal data in compliance with the Nigeria Data Protection Regulation 2019 (NDPR) and the Nigeria Data Protection Act 2023 (NDPA). As a data controller registered with the Nigeria Information Technology Development Agency (NITDA), we:

- Conduct annual data protection audits as required by the NDPR
- Maintain a Data Protection Officer (DPO) responsible for data protection compliance
- Obtain lawful consent or rely on appropriate legal bases before processing personal data
- Implement the technical and organisational security measures described in Section 10
- Provide data subjects with rights of access, rectification, and erasure consistent with the NDPR

Nigerian data subjects may direct complaints to the National Information Technology Development Agency (NITDA) at nitda.gov.ng.

12.1 Other African Jurisdictions

Africa is a continent of 54 countries, each with its own data protection laws. Where Quecorex operates in African jurisdictions beyond Nigeria — including but not limited to South Africa (POPIA), Kenya (Data Protection Act 2019), Ghana (Data Protection Act 2012), Egypt (Personal Data Protection Law 2020), and Rwanda (Law on the Protection of Personal Data 2021) — we are committed to complying with the applicable local data protection legislation in those countries.

Healthcare facilities deploying Quecorex in these jurisdictions are advised to confirm applicable local requirements with their own legal counsel. Quecorex will work with subscribing facilities to put in place any additional data processing terms required by local law.

As Quecorex expands into additional African markets, this section will be updated to reflect jurisdiction-specific compliance obligations. Facilities with questions about a specific country's requirements may contact privacy@quecorex.com.

13. HIPAA NOTICE (UNITED STATES)

For healthcare facilities and patients located in the United States, Quecorex processes Protected Health Information (PHI) as a Business Associate under the Health Insurance Portability and Accountability Act (HIPAA). We:

- Execute a Business Associate Agreement (BAA) with all covered entity clients prior to processing PHI
- Implement the HIPAA Security Rule safeguards (administrative, physical, and technical) as documented in our HIPAA Security Risk Assessment
- Maintain a breach notification procedure consistent with the HIPAA Breach Notification Rule (45 CFR §164.400)
- Do not use or disclose PHI except as permitted by the BAA and applicable law

US patients with questions about their HIPAA rights should contact the healthcare facility that manages their care, which acts as the HIPAA Covered Entity. Questions about Quecorex's HIPAA compliance may be directed to privacy@quecorex.com.

14. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. We will notify you of material changes by:

- Posting the updated Policy on this page with a new effective date
- Sending an email notification to registered users and facility administrators
- Displaying a notice within the Quecorex platform

Continued use of Quecorex after the effective date of a revised Policy constitutes acceptance of the changes. Where changes require a new consent, we will obtain it before continuing to process your data on that basis.

15. CONTACT US

If you have any questions, concerns, or requests relating to this Privacy Policy or the processing of your personal data, please contact us:

Privacy / DPO Contact	privacy@quecorex.com
Data Controller	Quecorex LLC, Delaware, United States of America
Website	quecorex.com/privacy
Response Time	We aim to respond to all data protection enquiries within 30 days
EU Representative	To be appointed. Contact privacy@quecorex.com for current details.

Effective Date: March 2, 2026 | This policy changes annually or whenever Quecorex introduces a material change to its data processing practices.