UCIP

Security & POPIA Compliance

For hospitals and healthcare facilities
Generated: 03 June 2026

AES-256	TLS 1.2+	TOTP 2FA	72-Hour
Encryption at rest	Encryption in transit	Multi-factor authentication	Breach notification SLA

Why hospitals trust UCIP

When an EMS provider connects to your hospital system, you need absolute confidence that patient data is handled properly. UCIP was built specifically for South African healthcare - not adapted from a generic platform. Every feature, every data flow, every security measure was designed with POPIA, HPCSA guidelines, and the National Health Act in mind.

Data encryption - every layer, every field

Patient identifiers
ID numbers, dates of birth, and contact details are encrypted using AES-256 via ActiveRecord Encryption. Even with raw database access, only ciphertext is visible.

Medical records
Allergies, current medications, medical conditions, and clinical handoff data (ISBAR) are all encrypted at rest. Custom clinical forms are encrypted before storage.

Digital signatures
Patient consent signatures captured on-device are encrypted before transmission and stored as encrypted data.

Authentication secrets
Passwords are hashed with bcrypt. 2FA secrets and API keys for integrations are encrypted. PINs use separate bcrypt hashing with lockout after 3 failures.

Access control - who sees what

Organisation isolation
Every query is scoped to the user's organisation. A user from Organisation A cannot see patients, sessions, or staff from Organisation B - enforced at the database query level, not just the UI.

Role-based access control
Three roles - Admin, Clinician, Paramedic - each with specific permissions. Admin functions require the admin role.

Mandatory two-factor authentication
Admin and clinician accounts must enable TOTP-based two-factor authentication before accessing the system.

Short-lived sessions
API tokens expire after 15 minutes. Refresh tokens have a 30-day maximum. Mobile PINs lock after 3 failed attempts.

Complete audit trail

Every action on patient data is logged:

* Who - user identity (name, role, organisation)

* What - action performed (view, create, update, export, share)
* Which record - specific patient, session, or resource accessed
* When - precise timestamp
* Where - IP address and device (user agent)
* What changed - specific fields modified on updates

Audit logs are immutable and available for regulatory inspection at any time.

Automated data retention

UCIP automatically enforces medical record retention periods per HPCSA guidelines:

Category	Retention Period
Adult patient records	6 years after last care session
Minor patient records	Until patient turns 21
Financial records	5 years (SARS requirement)
Staff records	5 years post-employment

Anonymisation replaces all identifying information with "REDACTED" and clears sensitive fields. This process runs automatically every day.

Breach detection and notification

* Security incidents are classified by type and severity (low to critical)
* The system tracks the 72-hour notification deadline per POPIA Section 22
* Organisation admins are immediately alerted when an incident is recorded
* Built-in email templates for Information Regulator notification comply with Section 22(3)
* Affected patient notifications include what happened, what data was involved, and protective steps
* Full incident lifecycle tracking: detected > investigating > contained > resolved > closed

Consent tracking

UCIP tracks four types of patient consent:

* Data processing consent - Recorded before patient data is captured
* Data sharing consent - Recorded before clinical data is shared with receiving facilities
* Research consent - Optional, for anonymised data in quality improvement
* Communication consent - Consent to contact the patient via email or phone

Each consent is timestamped, attributed, and revocable. The API indicates consent status on every patient record.

Data subject rights

Patients can exercise their POPIA rights through a dedicated online form:

* Right of access (Section 23) - request a copy of personal information
* Right to correction (Section 24) - request correction of inaccurate data
* Right to deletion (Section 24) - request deletion, subject to retention requirements
* Right to object (Section 11(3)) - object to processing
* Data portability - receive a copy of data in a portable format

All requests are tracked with reference numbers and a 30-day response SLA. Identity is verified using SA ID numbers.

Secure session sharing with hospitals

* Share links use cryptographically random tokens - they cannot be guessed
* Links have configurable expiry
* Every access is logged (who, when, how many times)
* Collaborator access is role-based (view only, can comment, full contributor)

* Hospital portal access requires separate authentication
* No patient data is ever sent via email - only secure links

No sensitive data in logs

Application logs are scrubbed of all sensitive information:

* Patient identifiers (ID numbers, dates of birth, email, phone)
* Medical data (allergies, conditions, medications, blood type)
* Clinical data (ISBAR handoff data, vital signs, clinical notes)
* Authentication data (passwords, tokens, 2FA secrets, PINs)
* Digital signatures

Web security headers

Header	Purpose
Content Security Policy	Prevents cross-site scripting (XSS) and injection attacks
X-Frame-Options: SAMEORIGIN	Prevents clickjacking
X-Content-Type-Options: nosniff	Prevents MIME type confusion
Referrer-Policy	Prevents URL leakage
Permissions-Policy	Restricts camera, microphone, and geolocation access

South African regulatory compliance

POPIA (Protection of Personal Information Act, 2013)
Full compliance with all 8 conditions. Processing activities register maintained. Information Officer registered.

PAIA (Promotion of Access to Information Act, 2000)
Section 51 manual published and publicly available.

HPCSA Guidelines
Medical record retention periods enforced automatically. HPCSA registration numbers tracked for clinical staff with expiry alerting.

National Health Act
Patient record management compliant with requirements for medical record keeping.

Processing activities register

Activity	Data Categories	Legal Basis	Retention
Patient care records	Name, ID, DOB, medical history, vitals	Section 32 (healthcare)	6 years / age 21
ISBAR handoff	Patient identity, situation, background	Section 32 (healthcare)	6 years / age 21
Consent management	Consent type, grantor, timestamp, signature	Section 27(1)(a) (consent)	Duration of record
Billing and invoicing	Client name, service details, amounts	Section 27(1)(d) (legal)	5 years (SARS)
AI clinical documentation	De-identified clinical text	Section 32 + DPA	Not retained by AI
Staff accounts	Name, email, role, HPCSA number	Section 27(1)(b) (contract)	5 years post-employment
Dispatch and booking	Locations, patient name, priority	Section 32 (healthcare)	6 years
Custom clinical forms	Variable per template	Section 32 (healthcare)	6 years / age 21
Audit logging	User, action, resource, IP, timestamp	Condition 1 (accountability)	Duration of retention
Security incidents	Incident details, affected records	Section 22 (breach)	Indefinite

Third-party data processors

Processor	Data Shared	Cross-border	Safeguards
AI Providers	De-identified clinical text	Yes (US)	DPA, TLS, no training
Xero	Invoice data, client names	Yes (NZ/AU)	DPA via terms, OAuth
Sage	Invoice data, client names	No (SA)	Encrypted API, HTTPS
Cloud Infrastructure	All app data (encrypted)	Configurable	AES-256, TLS, DPA
Email Provider	Email addresses, notifications	Varies	TLS, DPA
Paystack	Subscription payments	No (SA)	PCI-DSS, no health data

---

Information Officer

Drikus van der Walt
Email: privacy@ucip.co.za

Information Regulator

Tel: 010 023 5200 | Email: complaints.IR@justice.gov.za

This document was generated on 03 June 2026 and reflects the current state of UCIP's security and compliance measures.