AYULEX HMIS

Technology and security overview

For hospital IT, compliance and management teams evaluating Ayulex HMIS: how it is hosted, secured and administered, where data is kept, what it connects to, and how a hospital goes live.

The current versions of these details are published at hmis.ayulex.com/security and hmis.ayulex.com/trust.

01 At a glance

Hosting	India, Mumbai region: application and database
In transit	TLS on every connection, HSTS with preload
At rest	Database and backups encrypted
Backups	Automated, daily
Staff sign-in	Password plus authenticator-app code (TOTP); bot protection
Idle sessions	Signed out after 15 minutes without activity
Access	Role-based: standard roles and custom roles from 36 permissions, checked on the server
Audit trail	Append-only, enforced by the database; chart openings logged
Aadhaar	Never stored or logged
Interoperability	ABDM Milestone 1 built; HL7 FHIR R4 read API

02 What Ayulex HMIS covers

A hospital information system for outpatient and inpatient care. Each department works on its own screens, and everything it records lands on the same patient record, the same bill and the same reports. It runs in a current version of Chrome, Edge, Safari or Firefox; there is nothing to install on the hospital's computers.

Front office

Registration, appointments and online booking, OPD with a token display, telemedicine, patient portal

Inpatient care

Admissions, wards and nursing notes, discharge summaries, emergency department, operation theatres, wristbands

Diagnostics

Laboratory with barcoded sample labels, radiology reports, blood bank

Pharmacy and stores

Pharmacy, inventory with batches and expiry, your formulary

Finance

Billing, receipts and invoices, tariffs and packages, approvals for discounts and refunds

Administration

Staff, roster and payroll, quality and compliance, reports, roles and permissions, mortuary

03 Hosting and data location

- The application and its database run in India, in the Mumbai region.
- Patient records, bills, payments, deposits and insurance claims, uploaded files, staff accounts, roles, the audit trail and database backups are stored in India.
- A few features need an outside service, and each sends only what that feature needs: e-mails such as invitations and password resets; WhatsApp messages to patients, if the hospital connects its number; the bot check on the sign-in page; and the optional AI scribe's text, with names and identifiers removed, if the hospital switches the AI module on.
- Every outside service, what it receives and where it processes it is listed in the Ayulex HMIS Trust Center (hmis.ayulex.com/trust), kept current as it changes.

04 Security architecture

- TLS on every connection, with HSTS preload. HTTPS only.
- The database and its backups are encrypted at rest. Backups are automated and daily.
- Each hospital's records are kept separate, and every request is limited to the signed-in hospital.
- A strict Content Security Policy; the application cannot be embedded in other sites.
- Every input is validated on the server before it reaches the database.
- Rate limits and bot protection on sign-in and public forms. Patient-portal sign-in pauses for 15 minutes after five wrong attempts.
- Responses carrying patient data are marked no-store, so browsers and proxies keep no copy of them.
- Error reports are stripped of e-mail addresses, phone and ID numbers and tokens before they are stored.
- Every change runs automated security, workflow and clinical test suites, with more than 290 end-to-end checks against a real database.

05 Identity, access and administration

- Every account has a role. Ayulex HMIS ships standard roles, and administrators can build custom roles from 36 individual permissions.
- The server checks permissions on every request, so hiding a button is never the only protection.

- Staff sign in with a password and an authenticator-app code (TOTP). Idle sessions end after 15 minutes. A deactivated account is blocked at once.
- Front office staff can bill, but only approvers can give discounts, change prices or issue refunds.

Default permissions of the standard roles

Permission	Admin	Doctor	Nurse	Front office	Lab tech.	Pharmacist	Ward asst.
View patient records	Yes	Yes	Yes	Yes	Yes	Yes	–
Prescribe medicines	Yes	Yes	–	–	–	–	–
Record medicines given	Yes	–	Yes	–	–	–	–
Enter lab results	Yes	–	–	–	Yes	–	–
Dispense medicines	Yes	–	–	–	–	Yes	–
Create bills, collect payments	Yes	–	–	Yes	–	–	–
Approve discounts and refunds	Yes	–	–	–	–	–	–
Update bed status	Yes	–	Yes	–	–	–	Yes
Read the audit trail	Yes	–	–	–	–	–	–

06 Audit and accountability

- The audit trail records who opened a patient's chart and who changed what, with the time, IP address and device.
- It is append-only: the database itself rejects any attempt to edit or delete an entry.
- It can be filtered by date, user, action or record, for NABH and DPDP accountability reviews.
- Every record released through the FHIR interface is written to the audit trail, with the key that read it.

07 Privacy by design: the DPDP Act, 2023

- Consents are recorded with their purpose and, where needed, a witness. Patients can withdraw consent, and the withdrawal is recorded too.
- The waiting-area display shows token numbers, never names. Each role sees the parts of the record its work requires.
- Before the optional AI scribe sends any text for processing, names and other direct identifiers are removed.
- For ABHA verification, identifiers are encrypted with ABDM's public key before they leave the server. Aadhaar numbers and one-time codes are not stored or logged.

08 Interoperability

ABDM Milestone 1	Built	ABHA verification and creation from Aadhaar, with a one-time code to the patient's mobile. A verified ABHA is marked on the chart; one ABHA can be on only one patient record per hospital.
ABDM Milestones 2 and 3	In development	Sharing records with the patient's consent, and fetching them from other providers, building on the same client and the FHIR interface.
HL7 FHIR R4 API	Built, read-only	Patient, Encounter, MedicationRequest and Observation. Diagnoses in ICD-10, ICD-10-CM or ICD-11; vital signs in LOINC with UCUM units. Patients can be found by UHID, ABHA number or address, or phone.
API keys	Built	Issued by the hospital's administrator with the fhir:read scope and an expiry of up to two years. A key is shown once and stored only as a SHA-256 hash; it reads only its own hospital's records, and restricted patients are never released.
WhatsApp patient messages	Optional	Booking codes, confirmations and reminders, if the hospital connects its own number.
Devices	Supported	Standard USB barcode scanners, label printers for sample labels and wristbands, and any screen that opens a web page for the token display.

09 Implementation and support

Stage 1

Discovery

Each department walked through with its head; tariffs, bed layout, print formats and approval rules reviewed.

Result: A written scope and a dated plan.

Stage 2

Configuration

Departments, wards, beds, rates, packages, lab panels and formulary set up as the hospital; roles and staff accounts created.

Result: Checked by the heads of department.

Stage 3

Migration and training

Patients, doctors and opening stock brought across; each role trained on its own screens, in small groups and by shift.

Result: Staff who have practised their own day.

Stage 4

Go-live and support

A go-live day and hour chosen around the patient load, with our team close at hand; the first weeks reviewed.

Result: Support by phone and e-mail from then on.

What the hospital needs: computers with a current browser, a stable broadband connection (a second one from a different provider for critical areas), A4 printers, and optionally a label printer, barcode scanners and a screen for the token display.

10 Certification, responsibilities and contacts

- NABH accredits hospitals, not software, and the DPDP Act places duties on the hospital as well as on Ayulex. Ayulex HMIS provides the controls and the records those obligations call for.
- Security questionnaires are answered in writing. Ayulex does not claim certifications it does not hold.
- To report a security issue, write to admin@ayulex.com with "Security" in the subject line, as described at www.ayulex.com/security-policy, and allow reasonable time for a fix before disclosing it.
- Demonstrations: www.ayulex.com/demo or +91 62027 92298. Questions about this document: admin@ayulex.com.

Ayulex Inc. · TiLi Center, 2nd Floor, MV119 JL Building, Mission Veng, Aizawl, Mizoram 796005, India

Version 1.0 · November 2026