Sehat Sahoolat

Platform Upgrade & AI Integration Blueprint

Service Scope / Technical Blueprint / Statement of Work for Website, Android, iOS, EMR, Doctor Portal, Admin Portal and Safe AI Integration

Implementation philosophy

Repair -> secure -> simplify -> integrate -> automate -> scale

Field	Detail
Prepared for	Sehat Sahoolat by Web Health Online Pvt Ltd
Purpose	Vendor-facing scope for platform stabilisation, UX rebuild, compliance remediation and staged AI integration
Version	1.0 working blueprint
Date	20 May 2026
Important note	This document is a technical and clinical-safety planning document. It is not legal advice; Pakistan, GDPR/UK/EU and future US legal positions require specialist legal review.

Contents

Evidence base reviewed

- Live website review of sehatsahoolat.com, including homepage, doctor listings, packages and onboarding journey.
- Google Play listing for Sehat Sahoolat, including data safety declaration, update history and app description.
- Apple App Store listing for Sehat Sahoolat, including privacy declaration, size, rating and feature description.
- Sehat Sahoolat user guide and patient FAQs covering registration, EMR, packages, appointments, follow-up and EMR access.
- Packages and pricing documents, including PAYG, credit bundles, subscription and doctor remuneration models.
- Financial projection documents FY2026-FY2030, especially assumptions around revenue, provider costs, hosting, security and subscriptions.
- Website QA/audit report identified via uploaded file library, including performance, accessibility, broken link, sitemap and responsive defects.
- Pakistan telemedicine policy document, including LTP/CTP concepts, EMR logging, ISO27001/Tier III hosting expectations, formulary-name prescribing and ATAP registration concept.
- WHO/ITU Digital Health Platform Handbook principles on digital health platform design, reusable components, interoperability, governance and privacy-by-design.

Highest-priority finding

The platform should not proceed directly into advanced AI clinical triage or doctor co-pilot features until security, privacy declarations, consent, access control, audit logs, EMR workflow reliability and patient/doctor/admin usability have been remediated and tested.

1. Executive Summary

Sehat Sahoolat already has several valuable assets: a live website, Android and iOS apps, a working registration flow, EMR creation, family/member model, package model, appointment request, doctor allocation, video consultation, prescription generation, and an existing base of overseas Pakistani-origin specialist doctors. The strategic proposition is strong: a virtual hospital, not just a doctor-booking marketplace, connecting Western-trained doctors to patients and families in Pakistan with continuity of care through an EMR.

The current platform, however, appears to be operating as an early MVP with visible technical, UX, performance, accessibility, security/privacy, content-quality and operational workflow issues. The website still states it is in beta; the website audit highlights large payloads, slow load, broken links, horizontal overflow, accessibility defects and missing sitemap; live app-store declarations require urgent privacy and security review, especially because a medical app handling EMR should not declare “no data collected” without careful legal and technical validation.

The upgrade opportunity is to turn Sehat Sahoolat into a clinically governed digital health platform with patient, family, doctor, admin, partner, compliance and AI modules built around a single longitudinal EMR. AI should be introduced in layers: first for safe non-clinical support, then structured symptom capture and routing, then EMR assistance, then doctor co-pilot features, and only after safety governance, audit trails and human review are in place.

Expected end-state: a secure, mobile-first, bilingual, family-centred virtual hospital platform with reliable patient onboarding, simplified EMR completion, doctor-friendly consultation workflow, admin control tower, verifiable prescriptions, payments/packages/subscriptions, notifications, audit logs, governance dashboard and staged AI assistance. The vendor should deliver not only code but documented architecture, QA evidence, security evidence, clinical safety evidence, handover documentation, training and an investor-ready product demo.

Current state	Main risk	Target end-state
MVP website/app/EMR live but beta-like	Low patient trust, high drop-off, difficult investor due diligence	Polished, fast, accessible, conversion-optimised platform
EMR is central but completion appears heavy	Users abandon before booking; poor data quality	Progressive EMR, complete-later flow, AI-assisted structured data capture
Doctor network is a major asset	Doctor adoption drops if workflow is clunky	Doctor portal with schedule, pre-consult summary, quick notes, prescription and earnings
App-store privacy/security declarations need review	Regulatory, data-protection and reputational exposure	Accurate privacy declarations, consent, encryption, DPA/BAA readiness, audit logs
AI opportunity is strong	Unsafe triage or hallucination if introduced too early	Rules-led, clinically governed AI with human-in-the-loop controls

2. Current-State Diagnosis

2.1 Patient experience assessment

Journey step	Current evidence/assumption	Upgrade requirement
Registration/login	Email verification, patient/doctor role selection and login exist.	Use social login/OTP as optional secondary route; passwordless login; clear role choice; MFA for staff, optional biometric for patients.
EMR completion	User must provide demographics, CNIC, photo, vitals, allergies, immunisation, family history, PMH, surgery, medications and upload reports.	Break into 5-7 short steps with progress bar, save-and-resume, “complete later”, plain language, Urdu option and AI form guidance.
Family members	Family subscription model supports up to 4 members and additional members.	Create a family dashboard with clear dependent profiles, consent, guardian logic, age restrictions and emergency contacts.
Package selection	PAYG, credit bundles and subscription options exist.	Build comparison cards with “best for” labels, total yearly cost, expiry rules, refund/cancellation summary and upgrade path.
Appointment booking	User chooses symptom, specialty/department or asks admin to allocate.	Reduce steps; add smart routing; show availability windows; add “not sure which doctor” guided route; automatic time-zone handling.
Consultation start	Reminder notifications at 30, 15, 5 minutes and at appointment time are described.	Add pre-call device test, fallback audio, “doctor running late” status, reconnect button and support escalation.

Prescription/EMR download	Prescription PDF with QR verification is part of intended workflow.	Improve prescription template, QR verification landing page, formulary-name support, pharmacy-friendly instructions, patient education attachment.
Payment/support	Payment methods and support are not consistently described in FAQs.	Add payment-status screen, invoices/receipts, refund/cancellation workflow, support ticket and WhatsApp support integration.

2.2 Doctor experience assessment

Doctor module	Current evidence/assumption	Upgrade requirement
Onboarding and credentialing	Doctor profiles and country/qualification data appear on website; some profiles have missing/no data.	Structured doctor onboarding: identity, PMDC/PMC or international licence, indemnity, CV, specialty, languages, availability, consent to platform policies.
Availability management	Doctors can accept/refuse appointments in the app.	Calendar view, timezone conversion, default working windows, leave/unavailability, admin override and auto-allocation rules.
EMR access	Clinician access is described as time-limited and consent-based.	Role-based time-boxed access with audit logging, “reason for access”, break-glass emergency access policy and doctor attestation.
Consultation and notes	Video consultation and doctor note entry exist.	Single consultation workspace: patient summary, red flags, notes, diagnosis/problem list, plan, prescriptions, follow-up, attachments.
Prescription generation	Electronic prescription exists but template has spelling and visual defects.	Drug dictionary, generic/formulary names, dose/frequency/duration, allergy/interactions warning, QR verification and doctor sign-off.
Remuneration dashboard	Doctor remuneration models exist in pricing documents.	Doctor wallet/ledger: completed consults, paid/unpaid, rate basis, tax/withholding documentation, statements.
Medico-legal protection	Governance intent is strong but workflows need productisation.	Consent capture, audit logs, clinical incident reporting, complaint response, clinical review, indemnity record and consultation recording policy if used.

2.3 Admin experience assessment

Admin area	Observed gap	Upgrade requirement
Patient management	Admin reviews appointment requests and allocates doctors.	Admin control tower with queues, filters, patient status, package status, payment status, risk flag and pending actions.
Doctor management	Doctor profile data is visible but inconsistent in places.	Credentialing dashboard, document expiry, licence status, indemnity, specialties, languages, approval workflow.
Appointment allocation	Manual/admin allocation appears central.	Rules-based matching: specialty, urgency, language, country/time zone, availability, package, previous doctor continuity.
Payments/packages	PAYG/bundle/subscription model exists.	Plan management, coupon/referral engine, subscription renewal, bundle expiry, refund/no-show/cancellation automation.

Complaints/incidents	Not clearly productised in current public flow.	Complaint ticketing, clinical incident reporting, severity classification, RCA workflow, governance board review.
Audit/analytics	Needed for compliance and operations.	Audit logs, access logs, KPI dashboard, conversion funnel, doctor utilisation, no-show, churn, LTV/CAC, safety events.

2.4 Website and app quality assessment

- Homepage messaging has strong strategic themes: access, cost-effectiveness, continuity, integration, safety and quality. These should be retained but rewritten in tighter, patient-friendly English and Urdu.
- Doctor supply credibility is a strength, but profile quality must be standardised. Missing country/specialty fields, spelling errors and inconsistent profile content reduce trust.
- Website audit findings require remediation: slow LCP, large payloads, broken links, missing sitemap, horizontal overflow and accessibility issues.
- App-store privacy and security declarations should be reviewed immediately. If the app collects or processes EMR/health information, store declarations must accurately describe collection, encryption, deletion and sharing practices.
- Patient conversion should be redesigned around three buttons: “I need a doctor”, “I need help choosing a package”, and “I want to manage family health records”.

3. Recommended Target-State Platform

Sehat Sahoolat should be rebuilt conceptually as a virtual hospital platform: a longitudinal EMR plus clinical governance layer plus access to doctors, not merely an appointment marketplace. The platform should use reusable core components so patient identity, family profiles, consent, EMR, appointments, prescriptions, payments, notifications, audit logs and analytics are shared across web, Android, iOS, doctor and admin portals.

Target module	Scope
Patient web/app portal	Registration, login, family dashboard, package selection, appointment booking, uploads, prescription/EMR download, support.
Family account/dependent profiles	Household owner, dependents, parents, children, guardian consent, age-specific privacy rules.
Longitudinal EMR	Structured demographics, vitals, allergies, medications, PMH, family history, documents, consultations, prescriptions, follow-up.
AI-assisted onboarding	FAQ, registration help, EMR form help, package guidance, “not sure which doctor” routing.
Doctor portal	Schedule, patient summary, EMR access, video call, notes, prescriptions, follow-up, earnings, governance alerts.
Admin operations dashboard	Patient/doctor/package/payment/appointment/complaint queues, escalation, audit, analytics.
Clinical governance dashboard	Red flags, high-risk cases, complaints, incidents, medication safety, audit sampling, credentialing.
Appointment/video engine	Availability, matching, time zones, reminders, call lifecycle, fallback support.
QR prescription service	Unique prescription ID, QR verification, generic names, doctor sign-off, version history.
Payments/packages/subscriptions	PAYG, bundles, subscriptions, family plans, upgrade/downgrade, invoices, refunds.

Notifications	Email, SMS, WhatsApp, push, appointment reminders, renewal nudges, follow-up prompts.
Partner module	Labs, pharmacies, hospitals, insurers, corporate clients and referral tracking.
Compliance/audit module	Consent, privacy notices, DSAR, retention, access logs, audit trails, breach workflow.

4. Audit-Based Remediation Plan

4.1 P0 urgent blockers

Problem	Evidence/current issue	Business risk	Clinical/compliance risk	Technical fix	Owner	Effort	Acceptance criteria	Test method
App-store privacy/security declarations	Medical app lists EMR, appointments, audio/video/chat but declares no data collection and data not encrypted on Google Play.	Loss of patient trust, app-store scrutiny, investor concern.	Potential misleading declaration for special-category health data; privacy non-compliance.	Review actual data flows; update Google Play/App Store privacy nutrition labels; publish accurate privacy policy; verify encryption in transit/at rest.	Product owner + privacy lead + mobile lead	3-7 days	Declarations match actual data map; privacy policy linked; data deletion mechanism documented.	Data-flow walkthrough, app-store checklist, legal review.
Core security headers	Audit/remediation request includes HSTS, CSP, clickjacking and related controls.	High breach/reputation risk; lower due diligence score.	Health data exposure and cross-site attack risk.	Implement HSTS, CSP, X-Frame-Options/frame-ancestors, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.	DevOps/security engineer	3-5 days	SecurityHeaders.com or equivalent scores A/A+ without breaking site.	Automated header scan + regression test.
Authentication and RBAC	Doctor/admin/patient roles exist but need verified RBAC and MFA.	Privilege abuse, data leakage, operational errors.	Unauthorised EMR access; breach of confidentiality.	RBAC matrix, least privilege, MFA for admin/doctor, access expiry, session timeout.	Backend lead + security engineer	1-2 weeks	Every protected action mapped to role; failed access denied and logged.	RBAC unit/integration tests + manual negative testing.
Encryption and backup	Live app-store declaration says data is not encrypted; financial model underestimates data storage/security.	Major trust and investor risk.	PII/PHI breach risk.	TLS 1.2/1.3, database encryption at rest, encrypted file storage, key management, backups, restore tests.	DevOps/security engineer	1-2 weeks	All data encrypted in transit and at rest; backup restore tested.	SSL scan, cloud config review, restore drill.
Audit logs	Pakistan policy expects logs and EMR logging; clinical governance also requires traceability.	Unable to investigate complaints, disputes and misuse.	Medico-legal exposure; poor safety learning.	Immutable audit log for login, EMR view/edit, consent, appointment, prescription, payment, AI interaction.	Backend lead	2-3 weeks	Audit events searchable by patient, doctor, admin, date and action.	Audit test scripts and sample incident reconstruction.
Critical user journeys	Registration, EMR, package, appointment, consultation, prescription and payment must be stable.	Revenue and launch failure.	Patients may miss care or receive delayed unsafe advice.	End-to-end repair of patient/doctor/admin workflows, with QA test suite.	Product manager + QA lead	2-4 weeks	95%+ pass rate on defined E2E tests before release.	Manual and automated E2E testing.

4.2 P1 pre-launch fixes

Problem	Evidence/current issue	Business risk	Clinical/compliance risk	Technical fix	Owner	Effort	Acceptance criteria	Test method
Performance	Audit shows slow LCP and 19MB+ homepage payload.	High bounce rate and poor conversion.	Patients abandon booking; weaker emergency safety messaging.	Compress images/GIFs, WebP/AVIF, lazy loading, code splitting,	Frontend + DevOps	1-3 weeks	LCP <2.5s on target devices; homepage payload <3MB initial load.	Lighthouse, WebPageTest, real-device testing.

				cache/CDN, remove unused JS.				
Accessibility	Skip link missing; landmarks/list structure issues.	Excludes elderly/disabled users; poor public trust.	Patients may miss key warnings or instructions.	WCAG 2.2 AA baseline: landmarks, labels, alt text, contrast, keyboard navigation, skip link.	UX + frontend + QA	1-2 weeks	No critical axe violations; keyboard-only journey passes.	axe/Lighthouse + manual screen-reader checks.
SEO and link health	Broken links and missing sitemap found.	Lower discoverability and weaker credibility.	Patients may land on dead support/social links.	Fix links, sitemap.xml, robots.txt, canonical tags, schema.org medical organisation markup.	SEO/content + frontend	3-7 days	No broken internal links; sitemap submitted; Search Console clean.	Crawl scan + Search Console.
Content quality	Website contains spelling/grammar errors and inconsistent profile data.	Trust and investor credibility damage.	Confusion around doctors, packages and safety limitations.	Rewrite homepage, doctor profiles, FAQs, privacy, terms and emergency disclaimers in English/Urdu.	Content lead + clinical lead	1-2 weeks	Clinically approved, typo-free, bilingual pages.	Content QA and clinical review.
Onboarding simplification	EMR completion is comprehensive but heavy.	Drop-off before payment/booking.	Incomplete data undermines safe consultation.	Progressive EMR, save-and-resume, required/minimum dataset, AI helper.	Product + UX + backend	2-4 weeks	Median onboarding time reduced by 50%; completion rate improved.	Funnel analytics + usability testing.

4.3 P2 growth and optimisation

Problem	Why it matters	Business risk	Clinical/compliance risk	Technical fix	Owner	Effort	Acceptance criteria	Test method
Analytics dashboards	Needed for revenue, safety and investor reporting.	Poor decision-making.	Delayed safety detection.	KPI warehouse: signups, activations, conversion, consultations, no-shows, doctor utilisation, safety flags.	Data engineer + product	2-4 weeks	Dashboard refreshes daily; KPIs validated.	Data reconciliation.
CRM automation	Needed for reminders, renewals and missed appointment recovery.	Churn and revenue leakage.	Lost follow-up.	SendGrid/WhatsApp/SMS/push campaigns with consent and opt-out.	Growth + backend	2-4 weeks	Templates approved; opt-out works.	Campaign test and consent audit.
Referral and family growth	Commercial model depends on families/expats.	Slow acquisition.	Unclear responsibility for dependents.	Referral links, family invite, dependent consent, parent packages.	Product + growth	3-6 weeks	Track referral source and activation.	Referral test cases.
Partner integration	Labs/pharmacies/hospitals are future scale levers.	Missed ancillary revenue.	Unsafe unmanaged handoffs.	Partner directory, referral orders, status tracking, data-sharing agreements.	Partnerships + backend	6-12 weeks	Pilot partner workflow live with audit trail.	Partner UAT.

5. AI Integration Blueprint

AI must be layered on top of a stable and secure platform. It should start with non-clinical support and structured data capture, then evolve to clinically governed triage and doctor co-pilot tools. AI must never independently diagnose, prescribe, reassure emergencies or replace doctor judgement.

Phase	Functions	Safety boundaries	Deliverable
AI Phase 1: Safe non-clinical assistant	FAQ bot, package explanation, registration help, EMR form guidance, appointment guidance, support ticket creation, bilingual English/Urdu.	No diagnosis, no prescribing, no emergency reassurance, disclaimer, red-flag redirection, handoff to human support.	Website/app bot with knowledge base and admin escalation.
AI Phase 2: Symptom triage and routing	Complaint capture, structured symptom history, red-flag detection, urgency classification, route to emergency/GP/specialty, package suggestion, pre-consult summary.	Rules-led triage approved by clinicians, red-flag library, audit trail, safety-netting, human review for uncertain cases.	Triage MVP for 10-15 common complaints.
AI Phase 3: EMR data-entry assistant	Conversational EMR completion, medications, allergies, PMH, family	Patient confirmation before saving; clear “not medical advice”; OCR confidence threshold.	Structured EMR assistant integrated into onboarding.

	history, lifestyle, immunisations, document upload, OCR extraction.		
AI Phase 4: Doctor co-pilot	AI scribe, consultation summary, differential checklist, drug interaction prompts, patient instruction/referral letter drafts.	Draft only; doctor approves every note/prescription/advice; audit trail and disclaimer.	Doctor pilot for selected clinicians and specialties.
AI Phase 5: Business/operations AI	Retention reminders, renewals, support-ticket classification, doctor onboarding, marketing lead scoring, investor KPI summaries.	No PHI sent to external LLM unless legally approved and technically controlled.	Admin/growth automation suite.

6. AI Architecture Options

Option	Examples	Advantages	Limitations	Recommendation
Option A: API-based AI	OpenAI, Anthropic, Google, Azure OpenAI	Fastest to implement; high quality; strong multilingual capability; scalable.	PHI/privacy risk if not configured; requires DPA/BAA where applicable; cost depends on volume; vendor lock-in.	Use for non-PHI FAQ and admin drafting first. Use PHI only after legal review, data minimisation, encryption and processor agreements.
Option B: Self-hosted open-source AI	Rasa, Llama/Mistral, Whisper, Tesseract OCR, medical open models	More privacy control; local hosting; custom workflows; lower third-party PHI exposure.	GPU/hosting cost; lower quality without tuning; more engineering; maintenance burden; clinical validation still required.	Useful for Rasa triage flows, self-hosted OCR/transcription for PHI and structured workflows.
Option C: Hybrid model	Rules engine + Rasa + approved content RAG + restricted LLM APIs + self-hosted OCR/transcription	Best balance of safety, cost, privacy and speed; keeps triage deterministic; uses LLM where helpful.	Requires architecture discipline, logging and policy controls.	Recommended for next 6-12 months.

Recommended AI architecture for the next 6-12 months

Adopt a hybrid model: rules-led triage and red-flag engine; Rasa or equivalent for deterministic workflows; approved patient-education RAG; external LLM only for non-PHI content unless legal agreements and technical safeguards are complete; self-host OCR/transcription where PHI is involved.

7. Clinical Safety and Governance Framework

Governance element	Scope	Required control
AI Clinical Safety Board	CMO/Medical Director, clinical safety lead, data protection/privacy lead, product lead, AI engineer, QA lead, patient representative, legal adviser as needed.	Approve AI scope, red flags, triage logic, disclaimers, audit sampling, incident review and release gates.
Chatbot boundaries	Bot can educate, collect information, route and escalate; cannot diagnose, prescribe, reassure emergencies or replace a doctor.	All clinical prompts use approved scripts and safety-netting.
Red-flag escalation	Chest pain, stroke symptoms, severe breathlessness, altered consciousness, severe bleeding, suicidal ideation, anaphylaxis, severe paediatric illness, pregnancy red flags, etc.	Immediate emergency advice: call local emergency services/go to nearest ER; notify admin where appropriate.
Human-in-the-loop	AI outputs are drafts or routing suggestions only.	Doctor/admin approval required for clinical notes, prescriptions, advice and high-risk triage.

Credentialing	Verify licence, specialty, country, indemnity, identity, training and platform clinical policy sign-off.	Doctor cannot consult until credentialing is complete.
Prescription governance	Generic/formulary names, allergy check, interaction warning, dose/frequency/duration, QR ID, doctor sign-off.	Clinical audit sample monthly.
Incident reporting	Clinical incidents, technical failures, wrong patient, prescription error, data breach, complaint.	Severity grading, immediate mitigation, RCA, learning actions and board review.
Children/safeguarding	Guardian consent, age-sensitive privacy, safeguarding escalation, child mental health red flags.	Dedicated policies before paediatric triage/AI expansion.
Consultation recording	Only if legally approved and transparently consented.	Define purpose, access, retention, encryption and deletion.

8. Compliance and Legal Requirements

Area	Requirement	Vendor/product action
Pakistan telemedicine	Platform should align with the draft policy expectations around licensed/certified telemedicine practitioners, secure ISO27001/Tier III style hosting, consultation logging, EMR fields, patient visit collation, formulary-name prescribing and ATAP registration concept.	Obtain current legal opinion and regulatory confirmation; implement technical evidence pack.
Pakistan EMR/prescription	Patient ID, demographics, chief complaint, disease/problem, labs/radiology where applicable, prescription and emergency referral fields must be captured.	Ensure EMR schema supports mandatory fields and exportable audit reports.
GDPR/UK/EU exposure	Because overseas doctors, expat families and future UK/EU markets are relevant, build GDPR-style controls early.	Lawful basis, explicit health-data consent, DPO/owner, DPIA, ROPA, DSAR, retention, cookie consent, SCCs, sub-processors, breach workflow.
HIPAA-style future USA readiness	Not necessarily legally applicable at Pakistan launch unless covered entity/business associate relationships arise, but useful for design.	Minimum necessary access, access controls, audit logs, encryption, BAA readiness, breach response.
Children and family accounts	Dependents under a parent account create consent/privacy risks.	Guardian consent, age thresholds, access restrictions, withdrawal and mature-minor policy if applicable.
AI compliance	AI introduces explainability, safety, logging and processor risks.	AI DPIA, model risk assessment, clinical validation, prompt/version logging, approved knowledge base.

9. Recommended Technical Architecture

Diagram-style textual architecture:

```
[Web App / Android / iOS]
        |
[API Gateway + WAF + Rate Limiting]
        |
[Authentication & Identity Service] -- MFA -- RBAC -- Session Management
        |
[Core Backend Services]
   |-- Patient & Family Profile Service
   |-- EMR Service
   |-- Appointment & Scheduling Service
   |-- Video Consultation Service
   |-- Prescription & QR Verification Service
   |-- Package/Subscription/Payment Service
   |-- Notification Service: Email/SMS/WhatsApp/Push
```

```
   |-- Support/Ticketing Service
   |-- Doctor Credentialing & Earnings Service
   |-- Admin Operations Service
        |
[AI Orchestration Layer]
   |-- Rules/Triage Engine
   |-- Rasa/Structured Bot Flow Engine
   |-- Approved Knowledge Base + RAG
   |-- LLM API Gateway with PHI controls
   |-- OCR Pipeline
   |-- Transcription Pipeline
   |-- AI Interaction Log
        |
[Data Layer]
   |-- Relational EMR Database
   |-- Encrypted Document/Object Storage
   |-- Audit Log Store (append-only)
   |-- Analytics Warehouse
   |-- Consent/Privacy Store
        |
[Security/Operations]
   |-- Monitoring and Observability
   |-- Backup and Disaster Recovery
   |-- Secrets/KMS
   |-- CI/CD + Staging + Rollback
   |-- Vulnerability Scanning and Pen Testing
        |
[Partner APIs]
   |-- Labs
   |-- Pharmacies
   |-- Hospitals
   |-- Insurers/Corporate Clients
```

Component	Core requirements
Frontend web/mobile	Mobile-first, bilingual, responsive, accessible, reusable design system, offline-friendly draft saving where practical.
Backend API	Versioned REST/GraphQL APIs, validation, rate limiting, idempotent payment/appointment actions, central error handling.
Auth/RBAC	Patient/family owner/dependent/doctor/admin/super-admin/support/clinical governance roles; MFA for staff.
Video	Secure video provider integration, waiting room, connection test, fallback audio, call event logging.
Prescription	QR verification, doctor sign-off, versioning, generic drug support, audit history.
AI orchestration	No direct UI-to-LLM calls; central policy, logging, safety filters, redaction, knowledge-base control.
Monitoring	Error rates, latency, uptime, call failures, payment failures, app crashes, security events.

10. Data Architecture and Interoperability

Data object	Minimum fields/design
Patient	patient_id, family_account_id, demographics, CNIC/passport where legally required, contact, emergency contact, consent status, language preference.
Family member	member_id, relationship, guardian, age, consent, access permissions, active/dormant status.

Doctor	doctor_id, identity, licence(s), specialty, country, languages, indemnity, credentialing status, availability, remuneration model.
Appointment	appointment_id, patient/member, doctor, package/payment, symptoms, urgency, consent, time zone, status, call events, outcome.
Consultation notes	subjective, objective, assessment/problem list, plan, safety-netting, follow-up, referrals, doctor sign-off, version history.
Prescription	prescription_id, medication generic/formulary name, dose, route, frequency, duration, notes, QR status, doctor sign-off.
Consent	consent_id, purpose, user, scope, version, timestamp, withdrawal, linked appointment/EMR access.
AI interaction log	interaction_id, user, intent, input category, red flags, routing, model/rules version, output, escalation, reviewer if any.
Audit log	actor, role, action, record, timestamp, IP/device, before/after where applicable, reason for access.

- FHIR-readiness: do not attempt full FHIR implementation immediately, but map Patient, Practitioner, Encounter, Observation, MedicationRequest, AllergyIntolerance, DiagnosticReport and DocumentReference to future FHIR resources.
- Terminology: use practical local lists initially, with future mapping to ICD-10/ICD-11, SNOMED CT, LOINC and RxNorm/local formulary equivalents where licensing and practicality allow.
- Export: every patient should have an exportable EMR PDF and consultation summary PDF with QR-verifiable prescription where relevant.
- Partner integration: labs/pharmacies/hospitals should start with secure portal/referral export, then API integration once workflows are validated.

11. UX/UI Redesign Scope

Area	UX scope
Patient app	Simple onboarding; complete-later EMR; progress bar; family dashboard; urgent symptom warning; booking in fewer steps; upload reports; package comparison; subscription management; prescription/EMR download; bilingual English/Urdu; accessibility.
Doctor portal/app	Daily schedule; patient summary; timed EMR access; AI pre-consult summary; video call; notes; prescription; follow-up plan; earnings; clinical governance alerts.
Admin portal	Appointment queue; doctor matching; patient support; payment status; doctor verification; package management; complaints; audit trails; analytics; role-based controls.
Design system	Brand palette, reusable components, accessible buttons/forms/cards, bilingual typography, icons, empty states, error states, loading states.
Mobile-first accessibility	WCAG 2.2 AA baseline, keyboard navigation, screen-reader labels, contrast, large tap targets, simple Urdu/English wording.

12. Healthbot Conversation Design

Flow	User intent	Bot questions	Decision points/safety-netting	Data saved	Handoff

General greeting	User opens website/app bot.	Ask language, ask whether emergency, offer registration/package/booking/EMR/help.	Emergency yes -> ER advice. Unsure -> red-flag screen.	Greeting intent, language, emergency status.	Human support/admin if user stuck.
New patient registration	User wants to register.	Ask patient/doctor role, email/phone, country/time zone, family account option.	Failed verification -> support; underage -> guardian route.	Registration draft and consent status.	Admin/support.
Symptom triage	User describes complaint.	Age, sex, duration, severity, red flags, PMH, meds, allergies, pregnancy where relevant.	Red flags -> emergency; unclear -> admin nurse review; non-urgent -> specialty route.	Structured symptom summary.	Emergency/admin/doctor.
Package recommendation	User asks what to buy.	Who is it for, one-off vs family, chronic disease, expected use, expat family need.	Complex chronic/family -> subscription; one-off -> PAYG; repeated care -> bundle.	Package recommendation and reason.	Sales/admin.
EMR completion	User needs help filling EMR.	Guide through demographics, vitals, allergies, medications, PMH, family history, uploads.	Missing mandatory -> save draft; concerning symptom -> route.	Structured EMR fields pending confirmation.	Human support/doctor.
Medication list capture	User lists medicines.	Name, dose, frequency, duration, reason, start date, prescribing doctor, side effects.	High-risk meds -> flag for doctor review.	Medication table draft.	Doctor/admin.
Upload report	User uploads prescription/lab/imaging.	Ask document type/date/source; run OCR; show extracted data; ask confirmation.	Low OCR confidence -> manual entry; abnormal results -> advise booking, no diagnosis.	Document metadata and confirmed extracted fields.	Doctor/admin.
Book appointment	User wants a doctor.	Member, complaint, preferred language/time, specialty or not sure, package/payment.	Red flags -> emergency; no doctor available -> waitlist/admin.	Appointment request.	Admin allocation/doctor.
Follow-up reminder	Post-consult plan due.	Ask if symptoms improved, meds started, tests done, red flags.	Worsening/red flags -> urgent review/ER; stable -> book follow-up or upload results.	Follow-up status.	Doctor/admin.
Doctor recruitment screening	Doctor wants to join.	Country, specialty, licence, qualifications, language, availability, indemnity.	Incomplete credentials -> pending; high-demand specialty -> fast-track.	Doctor onboarding lead.	Credentialing/admin.
Support complaint	User reports problem.	Issue type, appointment/payment/technical/clinical, severity, screenshots.	Clinical harm -> incident; payment -> finance; tech -> support.	Ticket and severity.	Support/governance.

13. Business Model Integration

Commercial model	Technical support required
PAYG	One-off registration/consultation, payment, single EMR, optional EMR export, one follow-up rule, invoice/receipt.
Credit bundles	Bundle purchase, expiry tracking, family use up to defined limit, credit balance, renewal/upgrade prompts, unused-credit policy.
Subscription	Monthly/annual billing, family members, discounted consultations, unlimited EMR export, renewal, failed payment recovery.
Family/expat packages	Sponsor account abroad, dependents in Pakistan, multi-timezone notifications, payment from abroad, family health dashboard.
Chronic disease packages	Condition registry, scheduled reviews, labs reminders, medication review, care plan, KPI tracking.
Second opinion	Upload records, specialist selection, structured report, turnaround time SLA, optional MDT review.
Travel/portable EMR	Exportable health summary, vaccination, allergies, medications, QR verification, travel letter.

Doctor onboarding packages	Doctor subscription/equity/charity remuneration profiles, family benefit tracking, credentialing.
Corporate packages	Employer dashboard, employee eligibility, utilisation reports, anonymised analytics, consent firewall.
Partner referrals	Referral order, consent, partner status, results upload, commission tracking where legally permitted.

14. Phased Roadmap

Phase	Timeline	Deliverables	Dependencies	Risks	Acceptance criteria
Phase 0: Discovery and documentation	2-3 weeks	Code audit, infrastructure audit, security audit, UX audit, clinical workflow audit, database audit, compliance gap review, stakeholder interviews, product backlog.	Access to code/repos/server/app store/admin panels; stakeholder availability.	Incomplete access or poor documentation.	Audit report, architecture map, risk register, prioritised backlog signed off.
Phase 1: Stabilise and secure	4-6 weeks	Critical bug fixes, security headers, encryption, RBAC, MFA, backup, logging, app-store privacy correction, performance quick wins.	Discovery complete; staging environment.	Breaking existing flows; urgent security gaps.	P0 issues closed; staging and production release with rollback plan.
Phase 2: UX rebuild and core workflow repair	8-12 weeks	Patient, doctor, admin journeys; EMR simplification; package/payment repair; notifications; app updates.	Design system, analytics baseline, payment gateway access.	Scope creep; app-store delays.	Core journeys pass UAT; conversion metrics measurable; app updates submitted.
Phase 3: AI assistant MVP	6-8 weeks	FAQ bot, onboarding assistant, EMR assistant, safe routing bot, support bot.	Approved knowledge base; safety scripts; AI governance board.	Unsafe bot responses; PHI handling.	AI MVP passes scripted safety tests and logs all interactions.
Phase 4: Clinical triage and doctor co-pilot	8-12 weeks	Red-flag triage, pre-consult summary, AI scribe, prescription safety checks, governance dashboard.	Stable EMR, triage protocols, doctor pilot group.	Medico-legal risk; clinician resistance.	Pilot shows safety pass rate, doctor approval workflow and incident escalation.
Phase 5: Scale and integrations	12-24 weeks	Labs/pharmacies/hospitals/insurers/corporates, analytics warehouse, international expansion readiness.	Partner agreements; compliance review.	Partner integration delays; regulatory differences.	At least two partner pilots live with audited data-sharing workflow.

15. 90-Day Action Plan

Timebox	Actions
Days 1-15	Secure access to repositories, hosting, databases, app-store consoles, payment gateway, video provider, email/SMS/WhatsApp providers; freeze emergency changes; create staging environment; map data flows; confirm privacy declarations.
Days 16-30	Close P0 security headers/RBAC/MFA/encryption/backup gaps; correct app-store privacy declarations; publish updated privacy/cookie/terms/emergency disclaimer; define clinical safety board.
Days 31-45	Repair patient registration/EMR/package/booking journey; fix slow homepage, broken links, sitemap, responsive issues and accessibility blockers; add analytics events.
Days 46-60	Repair doctor workflow: availability, EMR access, notes, prescription, follow-up, earnings; standardise doctor profiles and credentialing workflow.

Days 61-75	Repair admin control tower: appointment queue, allocation, payments, refunds/no-show, support tickets, complaints, audit logs and KPI dashboard.
Days 76-90	Launch AI Phase 1 bot in controlled beta; run safety tests; complete UAT; prepare investor demo; produce handover documentation and maintenance plan.

16. Team and Vendor Requirements

Role	Required responsibility
Technical architect	Own target architecture, integration patterns, security design, scalability and documentation.
Senior backend developer	APIs, EMR, RBAC, payments, audit logs, integrations.
Frontend web developer	Website, patient/admin web, responsive and accessibility work.
Android developer	Android app stabilisation, push notifications, app-store compliance.
iOS developer	iOS app stabilisation, Apple privacy/accessibility/release compliance.
DevOps/security engineer	Cloud, CI/CD, WAF, TLS, backup, monitoring, pen-test remediation.
AI/ML engineer	AI orchestration, Rasa/LLM integration, OCR/transcription, logging, guardrails.
UX/UI designer	User research, wireframes, design system, prototypes, bilingual mobile-first UI.
QA automation tester	Test plans, E2E tests, device matrix, regression, release sign-off.
Privacy/compliance consultant	DPIA/ROPA/DSAR/cookie/sub-processor/data transfer controls; legal coordination.
Clinical safety lead	Red flags, triage logic, clinical workflows, incident reporting, safety case.
Project manager	Sprint planning, risk log, reporting, stakeholder meetings and delivery discipline.

Vendor operating rules

- Two-week sprints with weekly written progress report: completed, in progress, blocked, risks, decisions needed, next week.
- Shared product backlog with priority, owner, dependency, acceptance criteria and test status for every item.
- Source code must be in Sehat Sahoolat-controlled repository from day one. No vendor-only code custody.
- Separate development, staging and production environments. Production deployment only after written release checklist and rollback plan.
- Documentation is a deliverable: architecture, API, database schema, deployment, security controls, AI logic, QA evidence and admin manuals.
- IP ownership, source-code handover, credentials, cloud assets, app-store assets, domain/DNS, payment gateway, video provider and email provider access must be contractually controlled by Web Health Online Pvt Ltd.
- Maintenance retainer must include SLA, bug response, security updates, monitoring, backup verification and monthly performance/security reports.

17. Acceptance Criteria and Testing Plan

Test area	Measurable acceptance criteria

Functional testing	100% P0/P1 workflows pass: registration, verification, EMR, family, package, booking, payment, consultation, prescription, follow-up, support.
Patient journey testing	A new patient can register, create minimal EMR, choose package, pay, book, attend call and download prescription/EMR without admin workaround.
Doctor journey testing	Doctor can manage availability, view permitted EMR, start call, write notes, prescribe, add follow-up and see earnings.
Admin testing	Admin can allocate appointments, manage packages/payments/refunds, credential doctors, handle complaints, see audit trails and dashboards.
Payment testing	Success, failure, cancellation, refund, subscription renewal, failed renewal and duplicate webhook events handled safely.
Notification testing	Email/SMS/WhatsApp/push reminders arrive at expected times with consent and opt-out rules.
Video testing	Cross-platform audio/video, reconnection, fallback, waiting room, call start/end events and support escalation pass.
Prescription testing	QR verification, generic name, allergy warning, doctor sign-off, PDF rendering and version history pass.
AI safety testing	Bot refuses diagnosis/prescribing, escalates red flags, provides emergency redirection, logs interaction and shows disclaimer.
Accessibility testing	WCAG 2.2 AA target for key flows; no critical axe issues; keyboard and screen-reader flow tested.
Privacy/GDPR workflow testing	Consent, privacy notice, cookie consent, data access request, deletion/retention and breach workflow tested.
Penetration testing	No critical/high vulnerabilities before go-live; medium vulnerabilities risk-accepted or remediated with plan.
Load testing	Target concurrent users defined; appointment booking, EMR retrieval and video start do not degrade beyond SLA.
Mobile device testing	iOS/Android device matrix, low bandwidth, older devices, timezone, push notifications and app-store release testing.

18. Risk Register

Risk	Likelihood	Impact	Mitigation
AI hallucination	High	High	Use rules-led flows, approved content, retrieval from curated knowledge base, safety filters, human review, logging.
Unsafe triage	High	High	Clinician-approved red flags, emergency escalation, no diagnosis, audit sampling, safety board.
Poor OCR accuracy	Medium	Medium	Confidence score, patient confirmation, doctor review, manual correction, never auto-act on OCR alone.
Medico-legal exposure	High	High	Consent, credentialing, indemnity, clinical governance, audit logs, incident process, legal review.

GDPR/privacy non-compliance	High	High	DPIA, DPO/owner, DSAR, ROPA, retention, cookie consent, processor agreements, data minimisation.
Data breach	Medium	High	Encryption, MFA, RBAC, WAF, vulnerability scans, pen tests, audit logs, backup, incident response.
Doctor adoption failure	Medium	High	Doctor-friendly portal, remuneration transparency, support, training, feedback loop.
Patient drop-off	High	High	Simplify onboarding, progressive EMR, clear packages, WhatsApp support, analytics-driven optimisation.
App-store rejection	Medium	Medium	Correct privacy labels, content policy review, crash-free builds, accessibility and permission rationale.
Cost overruns	Medium	High	Fixed milestones, change control, MoSCoW scope, sprint demos, budget burn reporting.
Vendor lock-in	Medium	High	Source code ownership, open standards, API docs, containerisation, data export, exit plan.
Poor documentation/handover	High	High	Contractual deliverables; withhold final payment until docs, training and access handover complete.
Scalability failure	Medium	High	Load testing, cloud architecture, caching, queueing, monitoring, capacity planning.

19. Final Vendor Deliverables

- Technical audit report and current architecture diagram.
- Code audit report with risk-rated findings.
- Database schema review and migration plan.
- Security remediation report with evidence and re-test results.
- UX wireframes and clickable prototypes for patient, doctor and admin journeys.
- Updated patient website/app and mobile app releases.
- Updated doctor portal/app and admin portal.
- AI chatbot MVP and AI triage logic documentation.
- EMR integration documentation and API documentation.
- Consent, privacy, cookie and data-rights workflow implementation.
- QA test plans, test reports, device matrix and UAT sign-off.
- Deployment documentation, staging/production setup and rollback plan.
- Admin/doctor training videos/manuals.
- Maintenance and SLA plan.
- Source-code handover and credentials/access inventory.
- Compliance evidence pack for investors and regulators.
- Investor-ready product demo including patient, doctor, admin and AI flows.

Appendix A: Feature Backlog in MoSCoW Format

Priority	Features

Must have	Security headers; encryption; MFA for admin/doctor; RBAC; audit logs; accurate privacy labels; consent; core patient/doctor/admin workflow repair; EMR save/resume; package/payment stability; QR prescription; backup/restore; bug-free app releases; support ticketing.
Should have	Bilingual English/Urdu UI; AI FAQ/onboarding bot; doctor earnings; admin KPI dashboard; profile standardisation; accessibility AA; WhatsApp reminders; referral tracking; subscription renewal automation.
Could have	AI scribe pilot; OCR extraction; chronic-care dashboards; family health timeline; partner portal; corporate dashboard; loyalty/referral programme; in-app health education library.
Won't have in first 90 days	Autonomous diagnosis; autonomous prescribing; open-ended clinical chatbot without rules; unsupervised AI triage; deep hospital/lab/pharmacy API integrations without contracts; US HIPAA launch claims without legal review.

Appendix B: Sample User Stories

Feature	User story	Acceptance criteria
Patient registration	As a new patient, I want to register with email/phone and verify my identity so that I can create a secure account.	Given a valid email/phone, when I submit registration, then I receive verification and can log in after successful verification.
Family dashboard	As a family account owner, I want to add my spouse/parents/children so that I can manage their care under one account.	Each member has a unique ID, consent/guardian status, EMR and package eligibility.
Progressive EMR	As a patient, I want to complete the EMR in short sections so that I do not abandon the process.	Progress is saved; mandatory minimum dataset is clear; user can resume later.
Doctor EMR access	As a doctor, I want access to relevant EMR before the appointment so that I can prepare safely.	Access is time-limited, consent-based and logged.
Admin allocation	As an admin, I want to match patients to doctors by specialty, urgency, language and availability so that appointments are handled efficiently.	Matching recommendation is visible and editable with reason logging.
AI red flag	As a patient using the bot, I want urgent symptoms to trigger emergency advice so that I do not wait for a routine appointment.	Bot displays emergency advice, logs red flag and offers support handoff.
Prescription QR	As a patient/pharmacy, I want to verify a prescription QR code so that I can confirm authenticity.	QR opens verification page showing non-sensitive prescription status and metadata.

Appendix C: Sample Chatbot Scripts

C1. Safe opening script

Hello, I am the Sehat Sahoolat assistant. I can help with registration, packages, appointments, EMR forms and general guidance. I cannot diagnose, prescribe or replace a doctor. If you have chest pain, severe breathing difficulty, signs of stroke, severe bleeding, loss of consciousness, suicidal thoughts or any life-threatening symptom, please go to the nearest emergency department or call local emergency services immediately. Would you like to continue in English or Urdu?

C2. Symptom capture script

Please briefly describe the main problem. How old is the patient? How long has this been happening? Is it getting worse? Do you have any severe symptoms such as chest pain, severe breathlessness, weakness of one side, confusion, severe bleeding, high fever in a young child, pregnancy-related bleeding, or thoughts of self-harm?

C3. Package recommendation script

I can help you choose a package. Is this for one consultation, repeated care, chronic disease care, or a family member in Pakistan? Do you expect to use the service once, a few times, or regularly over the year?

C4. Doctor recruitment script

Thank you for your interest in joining Sehat Sahoolat. Please provide your full name, current country of practice, specialty, licence/registration number, years of experience, languages, availability and indemnity status. Our credentialing team will verify your details before your profile becomes active.

Appendix D: Developer Checklist

Security

- [ ] HSTS/CSP/clickjacking controls
- [ ] TLS scan pass
- [ ] MFA for admin/doctor
- [ ] RBAC matrix implemented
- [ ] Secrets stored securely
- [ ] Backups encrypted and restore-tested
- [ ] Audit logs immutable/searchable

Privacy

- [ ] Data inventory complete
- [ ] Privacy policy updated
- [ ] Cookie consent implemented
- [ ] DSAR workflow
- [ ] Data deletion/retention rules
- [ ] Sub-processor list
- [ ] App-store labels corrected

Core product

- [ ] Registration verified
- [ ] EMR save/resume
- [ ] Family accounts
- [ ] Package/payment flow
- [ ] Appointment allocation
- [ ] Video call
- [ ] Prescription QR
- [ ] Notifications

AI

- [ ] Approved knowledge base
- [ ] No diagnosis/prescribing
- [ ] Red-flag escalation
- [ ] Prompt/model version logging
- [ ] PHI controls
- [ ] Human handoff
- [ ] Safety test suite

Quality

- [ ] Automated tests
- [ ] Device matrix
- [ ] Accessibility tests
- [ ] Performance budget
- [ ] Load test
- [ ] Pen-test retest
- [ ] UAT sign-off

Handover

- [ ] Repo access
- [ ] Deployment docs
- [ ] API docs
- [ ] Database schema
- [ ] Training manuals
- [ ] Runbook
- [ ] SLA/maintenance plan

References and source notes

- Sehat Sahoolat website and public package/onboarding pages, reviewed 20 May 2026.
- Google Play listing for Sehat Sahoolat, reviewed 20 May 2026.
- Apple App Store listing for Sehat Sahoolat, reviewed 20 May 2026.
- Sehat Sahoolat user guide and Patient FAQs supplied in project files.
- Sehat Sahoolat packages/pricing and financial projection files supplied in project files.
- Pakistan Telemedicine Policy document supplied in project files.
- WHO/ITU Digital Health Platform Handbook, 2020, supplied in project files.
- Website QA/audit report in project file library, created 5 May 2026.