

# Hospital Patient Management System

## Patient Module — Features & UI Test Flow Guide

**Version 2.0.0 · February 2026 · CONFIDENTIAL** Prepared by Ai Nexus Engineering Team Updated: Added 6 new features — Appointment Scheduling, Patient Portal, Allergy Alerts, Visit History, Enhanced Duplicate Detection, SMS + In-App Notifications; added PATIENT role; international phone number support

---

### Table of Contents

#	Section	Status
1	Overview & System Architecture	UPDATED
2	User Roles & Permissions	UPDATED
3	Feature 1 — Authentication (Dev Login)	UPDATED
4	Feature 2 — Patient Registration	UPDATED
5	Feature 3 — Patient Search & Filtering	
6	Feature 4 — Patient Profile View	UPDATED
7	Feature 5 — Edit Patient	
8	Feature 6 — Deactivate / Activate Patient	
9	Feature 7 — Role-Based UI Visibility	UPDATED
10	Feature 8 — Sign Out	
11	Feature 9 — HIPAA Audit Trail	UPDATED
12	Feature 10 — Vitals History	
13	Feature 11 — Patient Insurance	
14	Feature 12 — Family Relationships	
15	Feature 13 — Patient Photo Upload	
16	Feature 14 — Patient ID Card (Print)	
17	Feature 15 — Duplicate Detection	
18	Feature 16 — CSV Export	
19	<b>Feature 17 — Appointment Scheduling &amp; Management</b>	<b>NEW</b>
20	<b>Feature 18 — Patient Self-Service Portal</b>	<b>NEW</b>
21	<b>Feature 19 — Structured Allergy &amp; Medication Alerts</b>	<b>NEW</b>
22	<b>Feature 20 — Visit History Timeline</b>	<b>NEW</b>

23	<b>Feature 21 — Enhanced Smart Duplicate Detection (Soundex)</b>	<b>NEW</b>
24	<b>Feature 22 — SMS + In-App Appointment Notifications</b>	<b>NEW</b>
25	Non-Functional Requirements Coverage	UPDATED
26	Complete Test Execution Checklist	UPDATED
27	Known Limitations & Out-of-Scope Items	UPDATED

## 1. Overview & System Architecture

The Patient Module is the foundational data layer of the Ai Nexus Hospital Management System. It provides HIPAA-compliant patient record management including registration, search, profile view, demographic updates, status management, vitals recording, insurance tracking, family relationships, photo management, appointment scheduling, patient self-service portal, allergy & medication alert management, visit history timeline, and a full HIPAA audit trail. All PHI is encrypted at rest (AES-256-GCM) and every access is immutably audit-logged.

Layer	Technology	Purpose
Frontend	React 18.3.1 + TypeScript + Ant Design 5	SPA at <a href="http://localhost">http://localhost</a>
API Gateway	Nginx (port 80)	Reverse-proxy; routes /api/* to backend
Backend	Spring Boot 3.4.1 / Java 17	REST API at hospital-api:8080
Security	Spring Security 6 + JWT (HMAC-SHA256)	Stateless auth + RBAC
Database	PostgreSQL 15	Patient records + immutable audit logs
Audit	AOP @AfterReturning + REQUIRES_NEW TX	All read/write actions logged
Encryption	AES-256-GCM (AttributeConverter)	PHI fields encrypted in DB
Search Index	Plaintext index cols + HMAC hashes	Enables search over encrypted data
Duplicate Detection	HMAC hash + Soundex phonetic index	Phone match + phonetic name match
Charts	Recharts	Vitals trend line charts
QR Code	qrcode.react	Patient ID card QR generation
SMS	Twilio SDK / MockSmsProvider	Appointment notifications via SMS
Events	Spring @Async + @TransactionalEventListener	Fire-and-forget notifications after DB commit

**Base URL:** <http://localhost> | **API Base:** <http://localhost/api/v1> | **Health:** <http://localhost/actuator/health>

## API Endpoints Summary

Resource	Endpoint	Methods	Roles
Auth (Staff)	/api/v1/auth/dev-login	POST	Public (dev)
Auth (Patient)	/api/v1/auth/patient-token	POST	Public (dev)
Patients	/api/v1/patients	GET, POST	Staff
Patient	/api/v1/patients/{patientId}	GET, PUT	Staff
Status	/api/v1/patients/{patientId}/status	PATCH	ADMIN
Photo	/api/v1/patients/{patientId}/photo	GET, POST, DELETE	Staff
Duplicates	/api/v1/patients/{patientId}/potential-duplicates	GET	Staff
Vitals	/api/v1/patients/{patientId}/vitals	GET, POST	Staff
Insurance	/api/v1/patients/{patientId}/insurance	GET, POST	Staff
Insurance item	/api/v1/patients/{patientId}/insurance/{id}	PUT, DELETE	Staff
Relationships	/api/v1/patients/{patientId}/relationships	GET, POST	Staff
Relationship item	/api/v1/patients/{patientId}/relationships/{relatedId}	DELETE	Staff
Audit Trail	/api/v1/patients/{patientId}/audit-trail	GET	ADMIN
CSV Export	/api/v1/patients/export/csv	GET	RECEPTIONIST ADMIN
<b>Appointments</b>	<b>/api/v1/patients/{patientId}/appointments</b>	<b>GET, POST</b>	<b>Staff</b>
<b>Appointment</b>	<b>/api/v1/patients/{patientId}/appointments/{id}</b>	<b>PUT</b>	<b>Staff</b>
<b>Cancel</b>	<b>/api/v1/patients/{patientId}/appointments/{id}/cancel</b>	<b>PATCH</b>	<b>RECEPTIONIST ADMIN</b>
<b>Upcoming</b>	<b>/api/v1/patients/{patientId}/appointments/upcoming</b>	<b>GET</b>	<b>Staff</b>
<b>Visit History</b>	<b>/api/v1/patients/{patientId}/appointments/history</b>	<b>GET</b>	<b>Staff</b>
<b>Global Appts</b>	<b>/api/v1/appointments</b>	<b>GET</b>	<b>RECEPTIONIST ADMIN</b>

Allergies	/api/v1/patients/{patientId}/allergies	GET, POST	Staff
Allergy item	/api/v1/patients/{patientId}/allergies/{id}	PUT, DELETE	Staff
Critical Check	/api/v1/patients/{patientId}/allergies/critical-check	GET	Staff
Portal Profile	/api/v1/portal/me	GET	PATIENT
Portal Appts	/api/v1/portal/me/appointments	GET	PATIENT
Portal Allergies	/api/v1/portal/me/allergies	GET	PATIENT
Portal Contact	/api/v1/portal/me/contact	PATCH	PATIENT
Notifications	/api/v1/portal/me/notifications	GET	PATIENT
Unread Count	/api/v1/portal/me/notifications/unread-count	GET	PATIENT
Mark Read	/api/v1/portal/me/notifications/{id}/read	PATCH	PATIENT
Mark All Read	/api/v1/portal/me/notifications/read-all	PATCH	PATIENT
SMS Log	/api/v1/dev/sms-log	GET	Staff (all)

## 2. User Roles & Permissions

The module enforces Role-Based Access Control (RBAC) at both the API layer (Spring Security) and the UI layer (conditional rendering). **Five roles** are supported in v2.0.0:

Role	Badge	Access Area	Login Flow
RECEPTIONIST	Blue	Patient management, registration, appointments	/login → select RECEPTIONIST
DOCTOR	Green	Clinical (vitals, allergies, appointment status updates)	/login → select DOCTOR
NURSE	Cyan	Clinical (vitals, allergies)	/login → select NURSE
ADMIN	Red	Full access including status changes and audit trail	/login → select ADMIN
PATIENT	Purple	<b>Self-service portal — own data only</b>	<b>/login → select PATIENT + enter Patient ID</b>

### Staff Permission Matrix

UI Capability	RECEPTIONIST	DOCTOR	NURSE	ADMIN
Register patient	✓	✗	✗	✓

Search / View patients	✓	✓	✓	✓
Edit patient	✓	x	x	✓
Deactivate / Activate	x	x	x	✓
Record vitals	x	✓	✓	✓
Manage allergies	✓	✓	✓	✓
Manage insurance	✓	x	x	✓
Manage relationships	✓	x	x	✓
Upload / Delete photo	✓	x	x	✓
Book appointment	✓	x	x	✓
Update appointment status	✓	✓	x	✓
Cancel appointment	✓	x	x	✓
View global appointments (/appointments)	✓	x	x	✓
CSV Export	✓	x	x	✓
Audit Trail	x	x	x	✓
View SMS Log (/dev/sms-log)	✓	✓	✓	✓

## PATIENT Portal Permissions

Capability	PATIENT Role
View own profile (read-only demographics)	✓
View own upcoming appointments	✓
View own allergies	✓
Update own contact info (phone, email, address)	✓
View own in-app notifications	✓
Mark notifications read	✓
Access /patients (staff pages)	x — 403
Access other patients' data	x — 403

How to login as any staff role: Go to <http://localhost/login> → enter any username → select role from dropdown → click Sign In.

How to login as PATIENT: Go to <http://localhost/login> → enter patient name → select **PATIENT** from dropdown → enter **Patient ID** (e.g. P2026001 ) → click Sign In → redirected to <http://localhost/portal>.

### 3. Feature 1 — Authentication (Dev Login) [UPDATED]

A development-only login page issues a real HMAC-SHA256 JWT token so the UI can be tested without a production Auth Module. The token is stored in `localStorage` and sent as `Authorization: Bearer <token>` on every API call. **v2.0.0 adds PATIENT role login with separate patient-token endpoint.**

#### UI Test Steps

#	Step	Action / Expected Result
1	Open browser	Navigate to <a href="http://localhost">http://localhost</a> — redirects to /login automatically
2	Enter username	Type any username, e.g. <code>receptionist1</code> , <code>dr.smith</code> , <code>nurse.jane</code> , <code>admin</code>
3	Select role	Choose from dropdown: RECEPTIONIST   DOCTOR   NURSE   ADMIN   <b>PATIENT</b>
4	Read role description	Description below dropdown explains permissions for selected role
5	Click Sign In	POST <code>/api/v1/auth/dev-login</code> → JWT token issued and stored
6	Observe header	Username + colour-coded role badge + Sign Out button appear
7	Confirm redirect	Staff → <code>/patients</code> ; <b>PATIENT</b> → <code>/portal</code>

#### PATIENT Login (Additional Step)

#	Step	Action / Expected Result
1	Select PATIENT role	Dropdown shows PATIENT option
2	Enter Patient ID field	New <b>Patient ID</b> field appears: enter e.g. <code>P2026001</code>
3	Enter username	Enter patient display name (e.g. <code>sarah.connor</code> )
4	Click Sign In	POST <code>/api/v1/auth/patient-token</code> → PATIENT JWT issued
5	Redirected to portal	Navigated to <a href="http://localhost/portal">http://localhost/portal</a>
6	Portal header	Shows "Welcome, Sarah" + Notification Bell + Sign Out

#### Test All 5 Roles

Username	Role	Expected	Redirect
<code>receptionist1</code>	RECEPTIONIST	Blue badge	<code>/patients</code>
<code>dr.smith</code>	DOCTOR	Green badge	<code>/patients</code>
<code>nurse.jane</code>	NURSE	Cyan badge	<code>/patients</code>
<code>admin</code>	ADMIN	Red badge	<code>/patients</code>
<code>sarah.connor</code> + <code>P2026001</code>	PATIENT	Purple badge	<code>/portal</code>

---

## 4. Feature 2 — Patient Registration [UPDATED — International Phone]

Allows RECEPTIONIST and ADMIN roles to register new patients. The system generates a unique Patient ID (format: P{year}{3-digit-seq} , e.g. P2026001 ). **v2.0.0 adds support for international E.164 phone numbers (e.g. +917026191993 for India).**

### 4.1 Prerequisites

Login as receptionist1 / RECEPTIONIST or admin / ADMIN before testing.

### 4.2 Happy Path — Register a New Patient

#	Step	Action
1	Navigate	From Patient List, click <b>Register New Patient</b> button (top-right)
2	Personal Info	First Name = Sarah, Last Name = Connor, DOB = 1985-07-04, Gender = Female
3	Contact Info (US)	Phone = +1-555-200-0001, Email = sarah.connor@example.com
4	Contact Info (International)	Phone = +917026191993 (India E.164 format — also valid)
5	Emergency Contact	Name = John Connor, Phone = +1-555-200-0002, Relationship = Son
6	Medical Info	Blood Group = B+, Known Allergies = Sulfa drugs, Chronic Conditions = Asthma
7	Submit	Click <b>Register Patient</b> button
8	Verify success	Toast: 'Patient registered – ID: P2026XXX'
9	Verify redirect	Automatically navigated to patient detail page

### 4.3 Phone Validation — Accepted Formats (v2.0.0)

Format	Example	Accepted
US standard	(312) 555-0101	✓
US with +1	+1-312-555-0101	✓
International E.164	+917026191993	✓ (new in v2.0.0)
E.164 any country	+447911123456 (UK)	✓ (new in v2.0.0)
Invalid	12345	✗ — error shown

### 4.4 Validation Testing

#	Test Case	Expected Result
1	Blank required field	Red error: 'First name is required'

2	Blank phone	Red error: 'Phone number is required'
3	Invalid phone format	Red error: 'Phone: international format +917026191993 or US format (XXX) XXX-XXXX'
4	Invalid email	Red error: 'Invalid email address'
5	Future date of birth	Date picker blocks future dates
6	Submit empty form	All required fields highlight red

#### 4.5 Duplicate Phone Warning

Register two patients with the same phone → Yellow warning (10s): 'Another patient with this phone number may already exist' . Second patient is still registered.

#### 4.6 RBAC

DOCTOR/NURSE: Register New Patient button is NOT visible. Direct `POST /api/v1/patients` → 403 Forbidden.

---

### 5. Feature 3 — Patient Search & Filtering

*(Unchanged from v1.2.0 — see full test steps in that section. Advanced Filters: City, State, Age Range, Has Allergies toggle, Has Chronic Conditions toggle.)*

---

### 6. Feature 4 — Patient Profile View [UPDATED]

The patient detail page displays all patient information organized in sections. **v2.0.0 adds: Allergy Card with critical alert, Appointment Card (upcoming), Visit History Timeline.** Every access generates an immutable HIPAA READ audit log entry.

#### 6.1 Page Header Elements

Element	Description
Patient full name	Large heading
Patient ID	Subtitle — e.g. P2026001
MRN tag	Blue tag next to ID
Back to List	Returns to /patients
Audit Trail	Button — ADMIN only
Print ID Card	Button — all staff roles
Edit Patient	Button — RECEPTIONIST and ADMIN only
Deactivate/Activate	Button — ADMIN only

### 6.2 Information Cards (v2.0.0)

#	Card	What to Verify
1	<b>Critical Allergy Alert</b>	Red/orange banner at top if SEVERE or LIFE_THREATENING allergy exists
2	Personal Info	Status badge, photo/avatar, DOB, Age, Gender, Blood Group
3	Contact Info	Phone, Email, Address, City, State, ZIP
4	Emergency Contact	Name, Phone, Relationship
5	Medical Info	Known Allergies (free text), Chronic Conditions
6	<b>Allergies</b>	Structured allergy records with severity colour tags
7	Family Relationships	Linked patients with colour-coded relationship type tags
8	Insurance	Insurance records with PRIMARY badge
9	Vitals History	Latest readings, trend chart (≥2 entries), history table
10	<b>Visit History</b>	Timeline of completed appointments (newest first, up to 20)
11	<b>Upcoming Appointments</b>	AppointmentCard showing next scheduled/confirmed appointments
12	Record Info	Registered By, Registered At, Last Updated By, Last Updated At

### 6.3 RBAC — Action Buttons by Role (v2.0.0)

Role	Edit Patient	Deactivate	Audit Trail	Record Vitals	Insurance	Allergies	Photo
RECEPTIONIST	✓	✗	✗	✗	✓	✓	✓
DOCTOR	✗	✗	✗	✓	✗	✓	✗
NURSE	✗	✗	✗	✓	✗	✓	✗
ADMIN	✓	✓	✓	✓	✓	✓	✓

## 7. Feature 5 — Edit Patient

(Unchanged from v1.2.0 — phone validation now supports international E.164 format.)

## 8. Feature 6 — Deactivate / Activate Patient

(Unchanged from v1.2.0)

## 9. Feature 7 — Role-Based UI Visibility [UPDATED]

The UI adapts dynamically based on the logged-in user's role. **v2.0.0 adds PATIENT role column and new UI elements.**

### Staff UI Visibility

UI Element / Page	RECEPTIONIST	DOCTOR	NURSE	ADMIN
Register New Patient (List)	✓	✗	✗	✓
Export CSV (List)	✓	✗	✗	✓
Edit button per row (List)	✓	✗	✗	✓
Edit Patient button (Detail)	✓	✗	✗	✓
Deactivate Patient (Detail)	✗	✗	✗	✓
Activate Patient (Detail)	✗	✗	✗	✓
Audit Trail button (Detail)	✗	✗	✗	✓
Print ID Card (Detail)	✓	✓	✓	✓
Record Vitals button	✗	✓	✓	✓
Add Insurance (Detail)	✓	✗	✗	✓
Edit/Delete Insurance (Detail)	✓	✗	✗	✓
Add Family Link (Detail)	✓	✗	✗	✓
Upload/Delete Photo (Detail)	✓	✗	✗	✓
<b>Book Appointment (Detail)</b>	✓	✗	✗	✓
<b>Update Appointment Status</b>	✓	✓	✗	✓
<b>Cancel Appointment</b>	✓	✗	✗	✓
<b>Global Appointments page (/appointments)</b>	✓	✗	✗	✓
<b>Add/Edit/Delete Allergy</b>	✓	✓	✓	✓
<b>View SMS Log (/dev/sms-log)</b>	✓	✓	✓	✓
Patient list — view/search	✓	✓	✓	✓
Patient detail — view	✓	✓	✓	✓

### PATIENT Portal Visibility

UI Element	PATIENT Role
Portal page (/portal)	✓ Accessible
My Profile card (read-only)	✓
My Allergies table (read-only)	✓

My Upcoming Appointments table	✓
Update Contact Info form	✓
Notification Bell (header)	✓
Notification Drawer	✓
/patients (staff pages)	✗ Redirected

### How to Verify

#	Step	What to Check
1	Login as RECEPTIONIST	Register + Edit + Book Appt + Insurance + Relationships + CSV visible. No Deactivate, no Vitals record, no Audit Trail.
2	Logout → Login DOCTOR	Record Vitals + Add Allergy + Update Appt Status visible. No Register, no Edit, no Book, no Deactivate.
3	Logout → Login NURSE	Same as DOCTOR minus appointment status update.
4	Logout → Login ADMIN	All buttons visible including Deactivate/Activate, Audit Trail, Book Appt.
5	Logout → Login PATIENT	Portal page shown with My Profile, My Allergies, My Appointments, Notification Bell. No staff pages.

## 10. Feature 8 — Sign Out

(Unchanged from v1.2.0 — applies to both staff and PATIENT roles)

## 11. Feature 9 — HIPAA Audit Trail [UPDATED]

Every access to patient data generates an immutable audit log entry. **v2.0.0 adds new audit action types for appointments, allergies, and patient portal access.**

### 11.1 All Audit Action Types (v2.0.0)

User Action	API Endpoint	Audit Action
Register new patient	POST /api/v1/patients	PATIENT_CREATE
View patient detail	GET /api/v1/patients/{id}	PATIENT_READ
Submit edit form	PUT /api/v1/patients/{id}	PATIENT_UPDATE
Confirm deactivation	PATCH /api/v1/patients/{id}/status	PATIENT_DEACTIVATE

Click Activate Patient	PATCH /api/v1/patients/{id}/status	PATIENT_ACTIVATE
Record vitals	POST /api/v1/patients/{id}/vitals	VITALS_CREATE
View vitals list	GET /api/v1/patients/{id}/vitals	VITALS_READ
Add insurance	POST /api/v1/patients/{id}/insurance	INSURANCE_CREATE
Update insurance	PUT /api/v1/patients/{id}/insurance/{id}	INSURANCE_UPDATE
Delete insurance	DELETE /api/v1/patients/{id}/insurance/{id}	INSURANCE_DELETE
Add family relationship	POST /api/v1/patients/{id}/relationships	RELATIONSHIP_ADD
Remove family relationship	DELETE /api/v1/patients/{id}/relationships/{id}	RELATIONSHIP_REMOVE
Upload patient photo	POST /api/v1/patients/{id}/photo	PHOTO_UPLOAD
Delete patient photo	DELETE /api/v1/patients/{id}/photo	PHOTO_DELETE
<b>Book appointment</b>	<b>POST /api/v1/patients/{id}/appointments</b>	<b>APPOINTMENT_BOOK</b>
<b>Update appointment</b>	<b>PUT /api/v1/patients/{id}/appointments/{id}</b>	<b>APPOINTMENT_UPDATE</b>
<b>Cancel appointment</b>	<b>PATCH /api/v1/patients/{id}/appointments/{id}/cancel</b>	<b>APPOINTMENT_CANCEL</b>
<b>Add allergy</b>	<b>POST /api/v1/patients/{id}/allergies</b>	<b>ALLERGY_CREATE</b>
<b>Update allergy</b>	<b>PUT /api/v1/patients/{id}/allergies/{id}</b>	<b>ALLERGY_UPDATE</b>
<b>Delete allergy</b>	<b>DELETE /api/v1/patients/{id}/allergies/{id}</b>	<b>ALLERGY_DELETE</b>
<b>Patient portal access</b>	<b>GET /api/v1/portal/me</b>	<b>PORTAL_ACCESS</b>
<b>Patient updates contact</b>	<b>PATCH /api/v1/portal/me/contact</b>	<b>PORTAL_CONTACT_UPDATE</b>

## 11.2 Audit Trail UI Modal (ADMIN only)

(Unchanged from v1.2.0 — modal accessible from patient detail page header)

## 12–18. Features 10–16 (Vitals, Insurance, Family, Photo, ID Card, Duplicate Detection, CSV Export)

(Unchanged from v1.2.0 — refer to previous version for full test steps.)

**Quick reference:** *Vitals (DOCTOR/NURSE/ADMIN record), Insurance (RECEPTIONIST/ADMIN manage), Family Relationships (RECEPTIONIST/ADMIN link), Photo Upload (RECEPTIONIST/ADMIN upload, all view), ID Card Print (all roles), Duplicate Detection (auto-check on detail page load), CSV Export (RECEPTIONIST/ADMIN only).*

## 19. Feature 17 — Appointment Scheduling & Management [NEW]

Allows RECEPTIONIST and ADMIN roles to book patient appointments. DOCTOR, RECEPTIONIST, and ADMIN can update appointment status. An **Appointment Card** appears on the patient detail page. A **Global Appointments List** page is available at `/appointments` for RECEPTIONIST and ADMIN. When an appointment is booked, confirmed, cancelled, or completed, the patient receives automatic SMS + in-app notifications (see Feature 22).

### 19.1 Prerequisites

Login as `receptionist1 / RECEPTIONIST` or `admin / ADMIN` to book. Login as `dr.smith / DOCTOR` to confirm/complete.

### 19.2 Book an Appointment — Happy Path

#	Step	Action / Expected Result
1	Open patient detail	Navigate to any active patient's detail page
2	Locate Appointment Card	Scroll to the Appointments section
3	Click Book Appointment	Button in card header (visible for RECEPTIONIST and ADMIN) → modal opens
4	Select date	Date picker — future dates only (past dates are disabled)
5	Select time	Time picker — 15-minute increments (HH:mm format)
6	Select type	Choose from: Consultation, Follow-Up, Procedure, Routine Checkup, Emergency
7	Doctor name	Enter Dr. Johnson (optional)
8	Department	Enter Cardiology (optional)
9	Reason for visit	Enter reason text (optional, max 1000 chars)
10	Submit	Click <b>Book</b> → POST <code>/api/v1/patients/{id}/appointments</code>
11	Verify success	Toast: 'Appointment booked'; new row appears in Appointments card
12	Verify notification	Patient receives APPOINTMENT_BOOKED in-app notification + SMS (if phone on record)

### 19.3 Appointment Fields

Field	Required	Format	Notes
Date	Yes	YYYY-MM-DD	Future dates only
Time	Yes	HH:mm	15-minute steps
Type	Yes	Enum	CONSULTATION, FOLLOW_UP, PROCEDURE, ROUTINE_CHECKUP, EMERGENCY
Doctor Name	No	String	Max 200 chars
Department	No	String	Max 200 chars
Reason for Visit	No	String	Max 1000 chars

### 19.4 Appointment Status Flow

SCHEDULED → CONFIRMED → COMPLETED
↳ CANCELLED
↳ NO_SHOW

Status	Description	Colour
SCHEDULED	Newly booked — awaiting confirmation	Blue
CONFIRMED	Confirmed by staff	Geekblue
COMPLETED	Visit completed — appears in Visit History	Green
CANCELLED	Cancelled by staff	Grey
NO_SHOW	Patient did not attend	Red

### 19.5 Update Appointment Status — Happy Path

#	Step	Action / Expected Result
1	Open patient detail	Navigate to any patient with a SCHEDULED appointment
2	Locate appointment row	In the Appointment Card
3	Click Update / Edit	Select new status from dropdown
4	CONFIRM status	Click Confirm → PUT /api/v1/patients/{id}/appointments/{id}
5	Verify notification	Patient receives APPOINTMENT_CONFIRMED notification + SMS
6	COMPLETE visit	Change status to COMPLETED → add Diagnosis and Visit Notes (optional)

7	Verify notification	Patient receives APPOINTMENT_COMPLETED notification + SMS
8	Verify visit history	Completed appointment appears in Visit History Timeline card

## 19.6 Cancel Appointment

#	Step	Expected Result
1	Click Cancel Appointment	Confirmation dialog appears
2	Confirm	PATCH /api/v1/patients/{id}/appointments/{id}/cancel → status = CANCELLED
3	Verify notification	Patient receives APPOINTMENT_CANCELLED notification + SMS
4	Verify	Appointment no longer appears in Upcoming Appointments (Appointment Card)

## 19.7 Global Appointment List (/appointments)

#	Step	Expected Result
1	Navigate	Go to <a href="http://localhost/appointments">http://localhost/appointments</a>
2	View all appointments	Paginated table across all patients (20 per page)
3	Filter by Patient ID	Enter P2026001 → only that patient's appointments
4	Filter by Status	Select SCHEDULED → only scheduled appointments
5	Filter by Date Range	Select range → only appointments in that window
6	Click Patient ID	Navigates to that patient's detail page
7	As DOCTOR	Global appointments page not accessible (404/redirect)

## 19.8 RBAC Test

Action	RECEPTIONIST	DOCTOR	NURSE	ADMIN
Book Appointment	✓	✗	✗	✓
Update Status	✓	✓	✗	✓
Cancel	✓	✗	✗	✓
Global Appointment List	✓	✗	✗	✓

Direct API POST /api/v1/patients/{id}/appointments as NURSE → 403 Forbidden.

## 20. Feature 18 — Patient Self-Service Portal [NEW]

A read-only self-service portal at /portal for **PATIENT** role only. Patients can view their own profile, allergies, upcoming appointments, and in-app notifications. They can also update their own contact

information. Staff roles cannot access portal endpoints (403).

### 20.1 Prerequisites

Patient must exist in the system (e.g. `P2026001` ). Login using PATIENT role with the Patient ID.

### 20.2 Portal Login Steps

#	Step	Action / Expected Result
1	Navigate	Go to <a href="http://localhost/login">http://localhost/login</a>
2	Enter display name	Type patient's name e.g. sarah.connor
3	Select PATIENT role	Choose PATIENT from dropdown
4	Enter Patient ID	New field appears — enter P2026001
5	Click Sign In	POST /api/v1/auth/patient-token → PATIENT JWT issued
6	Portal loads	Redirected to <a href="http://localhost/portal">http://localhost/portal</a>
7	Verify header	Shows "Welcome, Sarah" + Notification Bell + Sign Out

### 20.3 Portal Sections

#	Section	Content	Editable?
1	My Profile	Name, DOB, Gender, Blood Group, Phone (masked), Email	No
2	My Allergies	Table with allergy name, type, severity tag, reaction	No (view only)
3	My Upcoming Appointments	Table with date, time, type, doctor, department, status	No
4	Update My Contact Info	Form: phone, email, address, city, state, ZIP	Yes

### 20.4 Phone Masking

Phone is displayed with last 4 digits visible, rest masked with \* (e.g. `+1-***-***-0001` ). This prevents full PHI exposure in the browser while confirming the number on file.

### 20.5 Update Contact Information — Happy Path

#	Step	Action / Expected Result
1	Scroll to contact form	"Update My Contact Information" card at bottom
2	Enter new phone	+917026191993 (E.164 international accepted)
3	Enter new email	newemail@example.com
4	Submit	PATCH /api/v1/portal/me/contact

5	Verify success	Toast: 'Contact information updated'
6	Verify profile	My Profile card reflects updated data after refresh
7	Verify audit	PORTAL_CONTACT_UPDATE entry in audit_logs

## 20.6 Access Control Tests

#	Test	Expected Result
1	Staff accesses /api/v1/portal/me	403 Forbidden
2	PATIENT accesses /api/v1/patients	API returns 403; UI redirects
3	PATIENT accesses another patient's ID	403 — resolved from JWT, not URL
4	Expired/invalid token	401 Unauthorized

## 21. Feature 19 — Structured Allergy & Medication Alerts [NEW]

RECEPTIONIST, DOCTOR, NURSE, and ADMIN roles can add, edit, and deactivate (soft-delete) structured allergy records for a patient. A **Critical Allergy Alert** banner automatically appears at the top of the patient detail page when any SEVERE or LIFE\_THREATENING allergy is on record. PHI fields (allergy name, reaction, notes) are AES-256-GCM encrypted in the database.

### 21.1 Prerequisites

Login as `receptionist1 / RECEPTIONIST`, `dr.smith / DOCTOR`, `nurse.jane / NURSE`, or `admin / ADMIN`.

### 21.2 Add Allergy — Happy Path

#	Step	Action / Expected Result
1	Open patient detail	Navigate to any patient's detail page
2	Scroll to Allergies card	Card shows existing allergies (or empty state)
3	Click Add Allergy	Button in card header → modal opens
4	Allergy Name	Enter Penicillin
5	Type	Select Drug
6	Severity	Select Severe
7	Reaction	Enter Anaphylaxis
8	Onset Date	Select onset date (optional)
9	Notes	Enter any clinical notes (optional)
10	Submit	Click <b>Save</b> → POST /api/v1/patients/{id}/allergies
11	Verify success	Toast: 'Allergy added'; record appears in Allergies card

12	Verify critical alert	Red/orange banner at top of page: 'Critical allergy on record'
----	-----------------------	--

### 21.3 Allergy Fields

Field	Required	Values	Notes
Allergy Name	Yes	Free text	AES-256-GCM encrypted
Allergy Type	Yes	DRUG, FOOD, ENVIRONMENTAL, OTHER	
Severity	Yes	MILD, MODERATE, SEVERE, LIFE_THREATENING	
Reaction	No	Free text	AES-256-GCM encrypted
Onset Date	No	YYYY-MM-DD	
Notes	No	Free text	AES-256-GCM encrypted

### 21.4 Critical Allergy Alert

State	Alert Display
No allergies	No alert
MILD or MODERATE allergies only	No alert
Any SEVERE allergy	Orange/red alert banner: 'Critical allergy on record'
Any LIFE_THREATENING allergy	Same alert banner (prominently shown)

### 21.5 Severity Colour Coding

Severity	Tag Colour	Weight in Table
MILD	Green	Normal
MODERATE	Orange	Normal
SEVERE	Red	Normal
LIFE_THREATENING	Red	<b>Bold</b> (fontWeight: 700)

### 21.6 Edit Allergy

#	Step	Expected Result
1	Click Edit on allergy row	Modal opens pre-populated
2	Update severity	Change from MODERATE → SEVERE
3	Submit	PUT /api/v1/patients/{id}/allergies/{id}

4	Verify	Updated severity shown; critical alert appears if now SEVERE+
---	--------	---

## 21.7 Delete (Deactivate) Allergy

#	Step	Expected Result
1	Click Delete on allergy row	Popconfirm appears: 'Remove this allergy?'
2	Confirm	DELETE /api/v1/patients/{id}/allergies/{id} → soft-delete (is_active=false)
3	Verify	Record removed from Allergies card display
4	Note	Record is NOT physically deleted — is_active=false in DB

## 21.8 RBAC Test

Action	RECEPTIONIST	DOCTOR	NURSE	ADMIN
View allergies	✓	✓	✓	✓
Add allergy	✓	✓	✓	✓
Edit allergy	✓	✓	✓	✓
Delete allergy	✓	✓	✓	✓

Direct API POST /api/v1/patients/{id}/allergies as PATIENT → 403 Forbidden.

## 22. Feature 20 — Visit History Timeline [NEW]

A visual timeline of completed patient visits (appointments with status **COMPLETED** ) appears on the patient detail page. The timeline shows up to the 20 most recent visits, ordered newest first. Each visit entry shows date, time, appointment type (colour-coded), doctor name, department, diagnosis (if recorded), and visit notes.

### 22.1 Prerequisites

At least one appointment for the patient must have been updated to **COMPLETED** status.

### 22.2 View Visit History

#	Step	Expected Result
1	Open patient detail	Navigate to any patient's detail page
2	Scroll to Visit History card	Card appears below the Appointments section
3	Empty state	'No visit history' shown if no completed appointments
4	After completing appointment	Timeline entry appears automatically
5	Date column	Bold date on left side of timeline

6	Content	Type tag (colour-coded) + Doctor name + Department
7	Diagnosis	Shown in bold if recorded: 'Diagnosis: Hypertension'
8	Visit notes	Shown in secondary text below diagnosis

### 22.3 Appointment Type Colours in Timeline

Type	Colour
CONSULTATION	Blue
FOLLOW_UP	Cyan
PROCEDURE	Purple
ROUTINE_CHECKUP	Green
EMERGENCY	Red

### 22.4 Complete a Visit (to populate timeline)

#	Step	Action
1	Book an appointment	RECEPTIONIST books CONSULTATION for patient
2	Confirm appointment	DOCTOR/RECEPTIONIST updates status → CONFIRMED
3	Complete visit	DOCTOR updates status → COMPLETED; adds Diagnosis = 'Influenza A' + Visit Notes
4	Verify timeline	New entry appears in Visit History Timeline card
5	Verify portal	PATIENT logs in to portal; completed visit NOT shown in "My Upcoming Appointments"

### 22.5 Access Control

All staff roles can view the Visit History Timeline. PATIENT cannot access staff patient detail pages (403).

## 23. Feature 21 — Enhanced Smart Duplicate Detection (Soundex) [NEW]

Building on the v1.2.0 duplicate detection (exact phone HMAC match + exact name+DOB match), **v2.0.0 adds Soundex phonetic name indexing**. This catches near-miss duplicates where names are spelled differently but sound the same (e.g. "Connor" vs "Conner", "Smith" vs "Smyth"). Soundex codes are computed in Java and stored in indexed `first_name_soundex` / `last_name_soundex` columns.

### 23.1 Duplicate Detection Criteria (v2.0.0)

Method	Example Match	Version Added
--------	---------------	---------------

Exact phone HMAC	+1-555-200-0001 = +1-555-200-0001	v1.2.0
Exact name + DOB	John Smith, 1980-01-15 = same	v1.2.0
<b>Soundex + same DOB</b>	<b>Connor ≈ Conner + same DOB</b>	<b>v2.0.0</b>

## 23.2 Test Steps — Soundex Duplicate Detection

#	Step	Action / Expected Result
1	Register Patient A	Register John Connor, DOB 1980-01-15
2	Register Patient B	Register Jon Conner, DOB 1980-01-15 (phonetically similar)
3	Open Patient A detail	Navigate to Patient A's page
4	Observe alert	Yellow warning: '1 possible duplicate patient detected'
5	Click View Duplicates	Modal lists Patient B (phonetic match)
6	Open Patient B detail	Same alert points back to Patient A
7	Register Patient C	Register John Smith, DOB 1985-03-20 (different soundex)
8	Open Patient C	No duplicate alert shown

## 23.3 Duplicate Alert States

State	Display
0 duplicates	No alert rendered
1 duplicate	'1 possible duplicate patient detected'
2+ duplicates	'N possible duplicate patients detected'

## 23.4 View Duplicates Modal

Column	Content
Patient ID	Clickable link to that patient
Full Name	First + Last name
Date of Birth	Formatted date
Phone	Phone number
Status	Active / Inactive badge

# 24. Feature 22 — SMS + In-App Appointment Notifications [NEW]

When appointment lifecycle events occur, the system automatically sends:

- **SMS** to the patient's registered phone number (via Twilio in production, MockSmsProvider in dev)

- **In-app notification** stored in the database, visible via the Notification Bell in the Patient Portal

All notifications are fire-and-forget ( `@Async` + `@TransactionalEventListener(AFTER_COMMIT)` ) — they never block the API response and only fire after a successful database commit.

## 24.1 Notification Triggers

Event	In-App Type	SMS Message
Appointment booked	APPOINTMENT_BOOKED	Hi! Appointment confirmed: {date} {time} with {doctor} ({dept}). Ref: {patientId} – Ai Nexus Hospital
Appointment confirmed	APPOINTMENT_CONFIRMED	Your appointment {date} at {time} is now confirmed. See you soon! – Ai Nexus Hospital
Appointment cancelled	APPOINTMENT_CANCELLED	Your appointment on {date} at {time} has been cancelled. Please call us to reschedule. – Ai Nexus Hospital
Appointment completed	APPOINTMENT_COMPLETED	Your visit is complete. Log in to your portal to review your visit notes. – Ai Nexus Hospital
24h reminder (8am daily)	APPOINTMENT_REMINDER	Reminder: Appointment tomorrow {date} at {time} with {doctor}. – Ai Nexus Hospital

## 24.2 SMS Provider Configuration

Mode	Condition	Behaviour
Mock (dev/default)	TWILIO_ACCOUNT_SID env var blank	Writes to sms_delivery_log table; no real SMS sent
Twilio (production)	TWILIO_ACCOUNT_SID env var set	Sends real SMS via Twilio REST API

**To switch to real Twilio SMS:** Set `TWILIO_ACCOUNT_SID` , `TWILIO_AUTH_TOKEN` , `TWILIO_FROM_NUMBER` in `.env` and rebuild.

**Patient phone must be in E.164 format** (e.g. `+917026191993` ) for international SMS delivery.

## 24.3 In-App Notification Bell — Test Steps

#	Step	Action / Expected Result
1	Login as PATIENT	Go to /portal with PATIENT role + Patient ID
2	Book appointment (as RECEPTIONIST)	Open new browser tab → login as RECEPTIONIST → book appointment for this patient
3	Switch back to PATIENT tab	Portal auto-refreshes unread count every 30 seconds
4	Observe bell icon	Notification bell in header shows numeric badge (e.g. 1)
5	Click bell	Right-side drawer opens (380px wide) titled <b>Notifications</b>

6	View notification	Shows: type icon, <b>bold title</b> (unread), message, '2 minutes ago'
7	Unread styling	Blue left border (3px solid #1677ff) + bold title
8	Click notification	Marks as read — border disappears, title becomes normal, badge decrements
9	Mark All Read	"Mark all read" button in drawer header (only shown when unread > 0)
10	After mark all read	Badge shows 0 (hidden — badge not shown when 0)
11	Empty state	'No notifications yet' shown when list is empty

## 24.4 Notification Icon Types

Type	Icon	Colour
APPOINTMENT_BOOKED	CalendarOutlined	Green
APPOINTMENT_CONFIRMED	CalendarOutlined	Blue
APPOINTMENT_CANCELLED	CloseCircleOutlined	Red
APPOINTMENT_REMINDER	ClockCircleOutlined	Orange
APPOINTMENT_COMPLETED	CheckCircleOutlined	Blue

## 24.5 SMS Mock Log Test Steps (as Staff)

#	Step	Action / Expected Result
1	Login as any staff role	RECEPTIONIST, DOCTOR, NURSE, or ADMIN
2	Navigate	Go to GET /api/v1/dev/sms-log (via API or curl)
3	Verify entries	After booking appointment — SMS log has entry
4	Verify fields	provider=MOCK, status=SENT, patientId=P2026XXX
5	Verify message	Message text contains appointment date
6	Cancel appointment	New log entry appears with CANCELLED message
7	PATIENT role test	GET /api/v1/dev/sms-log as PATIENT → <b>403 Forbidden</b>

## 24.6 24h Daily Reminder Scheduler

#	Detail	Value
Schedule	@Scheduled(cron = "0 0 8 * * *")	Daily 8:00am server time
Scope	All SCHEDULED or CONFIRMED appointments tomorrow	

Notification type	APPOINTMENT_REMINDER	
PHI safety	Only patientId + count logged — no phone/message in logs	

## 24.7 Access Control Tests

#	Test	Expected
1	Staff accesses /api/v1/portal/me/notifications	403 Forbidden
2	PATIENT accesses /api/v1/dev/sms-log	403 Forbidden
3	PATIENT sees only own notifications	patientId resolved from JWT — cannot see others

## 25. Non-Functional Requirements Coverage [UPDATED]

NFR Category	Requirement	Implementation	Status
Performance	Search results < 2s	Indexed search columns + debounce	✓
Performance	Registration < 3s	Async API + optimistic UI	✓
Performance	Vitals recording < 2s	Lightweight payload, REQUIRES_NEW TX	✓
<b>Performance</b>	<b>Appointment booking &lt; 2s</b>	<b>Async event publishing; booking TX separate from notification</b>	✓
Security	AES-256 encryption at rest for PHI	AttributeConverter on all PHI fields	✓
Security	JWT-based stateless auth	HMAC-SHA256 JWT, 8hr expiry	✓
Security	RBAC enforced at API level	Spring Security URL-level rules	✓
Security	Audit logs immutable	DB trigger blocks UPDATE / DELETE	✓
Security	Audit log 6-year retention	Archive table + Flyway migration	✓
Security	Photo access requires JWT	Blob served through authenticated API	✓

Security	No PHI in audit logs	Only patient_id, username, action logged	✓
<b>Security</b>	<b>No PHI in SMS logs</b>	<b>Only patientId + status logged; message not logged</b>	✓
<b>Security</b>	<b>Notifications scoped to patient</b>	<b>patientId resolved from JWT claim, not URL</b>	✓
<b>Security</b>	<b>Allergy PHI encrypted</b>	<b>allergy_name, reaction, notes AES-256-GCM encrypted</b>	✓
Usability	Inline validation on blur	Zod + react-hook-form mode: onBlur	✓
Usability	300ms search debounce	useDebounce hook	✓
Usability	Success notifications auto-dismiss	Ant Design notification duration=5	✓
Usability	Confirmation for destructive actions	ConfirmModal + Popconfirm	✓
Usability	WCAG 2.1 AA — colour + text labels	StatusBadge: colour + text always	✓
Usability	Vitals trend chart	Recharts LineChart (≥2 readings)	✓
<b>Usability</b>	<b>Notification bell auto-refresh</b>	<b>useUnreadCount polls every 30s</b>	✓
<b>Usability</b>	<b>Relative timestamps in notifications</b>	<b>dayjs.fromNow() for notification age</b>	✓
Data Integrity	Unique Patient ID	DB sequence + PatientIdGeneratorService	✓
Data Integrity	Future DOB blocked	DatePicker disabledDate	✓
Data Integrity	Records never permanently deleted	Soft delete via status only	✓
Data Integrity	Bidirectional relationships	Both directions stored; inverse auto-computed	✓
Data Integrity	BMI auto-calculated	weightKg / (heightM²)	✓

Data Integrity	Notifications only on commit	@TransactionalEventListener(AFTER_COMMIT)	✓
Data Integrity	Allergy soft-delete	is_active=false; records retained for audit	✓
Data Integrity	Future appointment dates only	DatePicker disabledDate in BookAppointmentModal	✓
Responsive	Mobile 320px to desktop 2560px	Ant Design grid system (Col/Row)	✓

## 26. Complete Test Execution Checklist [UPDATED]

Work through this checklist in order. Check off each item as you complete it.

### Login

- ☐ Login as `receptionist1 / RECEPTIONIST` → blue badge in header
- ☐ Login as `dr.smith / DOCTOR` → green badge
- ☐ Login as `nurse.jane / NURSE` → cyan badge
- ☐ Login as `admin / ADMIN` → red badge
- ☐ Login as **PATIENT** role → enter Patient ID `P2026001` → purple badge → redirected to `/portal`

### Registration

- ☐ Register Sarah Connor (all fields filled) → success toast + redirect to detail
- ☐ Register patient with E.164 international phone `+917026191993` → accepted ✓
- ☐ Blur empty First Name field → inline error shown
- ☐ Enter invalid email → inline error shown
- ☐ Try future date of birth → date picker blocks it
- ☐ Register second patient with same phone → yellow duplicate warning toast (10s)
- ☐ Login as DOCTOR → Register button not visible; CSV Export button not visible

### Patient List & Search

- ☐ Active patients shown by default
- ☐ Search by name → results filter live (300ms debounce)
- ☐ Search by Patient ID → exact match found
- ☐ Search by MRN → exact match found
- ☐ Search by phone number → results filter
- ☐ Apply Status = Inactive filter
- ☐ Apply Gender filter
- ☐ Expand Advanced Filters → City, State, Age From/To, Has Allergies, Has Chronic toggles visible
- ☐ Combine search + basic + advanced filter
- ☐ Search with no match → 'No patients found'

- ☐ Click patient row → navigates to detail page

## Profile View

- ☐ All sections visible: Personal Info, Contact, Emergency, Medical, Allergies, Family, Insurance, Vitals, Visit History, Upcoming Appointments, Record Info
- ☐ **Critical Allergy Alert visible if SEVERE/LIFE\_THREATENING allergy exists**
- ☐ MRN tag shown in page header (if assigned)
- ☐ Active patient shows green status badge
- ☐ As DOCTOR: Record Vitals + Add Allergy visible; no Book Appointment button
- ☐ As RECEPTIONIST: Edit, Book Appointment, Insurance visible; no Record Vitals
- ☐ As ADMIN: all buttons visible
- ☐ Back to List button returns to /patients

## Edit Patient

- ☐ Open edit form → all fields pre-populated
- ☐ Update phone to +917026191993 (international) → saved ✓
- ☐ Change address and submit → success toast
- ☐ Cancel discards changes

## Status Management

- ☐ As ADMIN: Deactivate Patient → confirmation modal
- ☐ Confirm deactivation → status changes to INACTIVE
- ☐ Activate patient → immediate, no confirmation
- ☐ As RECEPTIONIST: no Deactivate/Activate button visible

## Vitals History

- ☐ As DOCTOR: Record Vitals button visible; record new entry
- ☐ After 2+ entries: Recharts trend chart appears
- ☐ As RECEPTIONIST: Record Vitals button not visible

## Insurance

- ☐ As RECEPTIONIST: Add Insurance → save → appears with PRIMARY badge
- ☐ Edit insurance → modal pre-populated
- ☐ Delete insurance → confirmation → removed

## Family Relationships

- ☐ Add SPOUSE → appears in both patients
- ☐ Add PARENT/CHILD → inverse types shown
- ☐ Remove relationship → removed from both patients

## Photo Upload

- ☐ Upload JPEG ≤2MB → photo replaces avatar
- ☐ Upload .gif or >2MB → error message
- ☐ Delete photo → avatar restored

## Patient ID Card

- ☐ Print ID Card modal opens with QR code
- ☐ Click Print → browser print dialog

## Duplicate Detection

- ☐ Register two patients with same name + DOB → yellow alert on detail page
- ☐ **Register phonetically-similar names (Connor / Conner) + same DOB → Soundex alert**
- ☐ Click View Duplicates → modal lists duplicates

## CSV Export

- ☐ As RECEPTIONIST: Export CSV → downloaded
- ☐ Apply filters then Export CSV → CSV respects filters
- ☐ As DOCTOR: Export CSV button not visible

## HIPAA Audit Trail

- ☐ After registration: PATIENT\_CREATE in audit\_logs
- ☐ After viewing detail: PATIENT\_READ in audit\_logs
- ☐ After editing: PATIENT\_UPDATE in audit\_logs
- ☐ **After booking appointment: APPOINTMENT\_BOOK in audit\_logs**
- ☐ **After adding allergy: ALLERGY\_CREATE in audit\_logs**
- ☐ **After patient portal access: PORTAL\_ACCESS in audit\_logs**
- ☐ As ADMIN: Audit Trail modal → colour-coded entries
- ☐ Attempt UPDATE on audit\_logs → immutability error

## Appointment Scheduling [NEW]

- ☐ As RECEPTIONIST: Book Appointment button visible on patient detail
- ☐ Book appointment (type: Consultation, future date, time, doctor name) → success toast
- ☐ **Patient receives APPOINTMENT\_BOOKED in-app notification (check portal bell)**
- ☐ As DOCTOR: Update appointment status → CONFIRMED → success
- ☐ **Patient receives APPOINTMENT\_CONFIRMED notification**
- ☐ As RECEPTIONIST: Cancel appointment → CANCELLED → notification sent
- ☐ As DOCTOR: Complete appointment (COMPLETED) → add Diagnosis → success
- ☐ Completed appointment appears in Visit History Timeline
- ☐ As RECEPTIONIST: Global Appointments page (/appointments) → paginated list
- ☐ Filter global appointments by Patient ID, Status, Date Range
- ☐ As DOCTOR: Book Appointment button NOT visible; /appointments not accessible

## Patient Portal [NEW]

- ☐ Login as PATIENT with valid Patient ID → redirected to /portal
- ☐ My Profile shows masked phone (last 4 digits visible)
- ☐ My Allergies table shows all active allergies
- ☐ My Upcoming Appointments shows SCHEDULED/CONFIRMED appointments only
- ☐ Update Contact Info → new phone/email → success toast → profile updated
- ☐ Staff login: GET /api/v1/portal/me → 403 Forbidden

- ☐ PATIENT login: `GET /api/v1/patients` → not accessible

### Allergy Management [NEW]

- ☐ As RECEPTIONIST: Add Allergy → Drug / Severe / Anaphylaxis → saved
- ☐ Critical Allergy Alert (red banner) appears on detail page
- ☐ As DOCTOR: Add Allergy button visible and functional
- ☐ Edit allergy → severity updated → alert updates
- ☐ Delete allergy → Popconfirm → removed from card
- ☐ LIFE\_THREATENING allergy → row shows in **bold** in allergy table
- ☐ As PATIENT via portal: allergies visible in My Allergies (read-only)

### Visit History Timeline [NEW]

- ☐ No completed visits → 'No visit history' empty state
- ☐ After completing appointment → entry appears in timeline
- ☐ Type tag colour-coded correctly
- ☐ Diagnosis text displayed if recorded
- ☐ Timeline shows newest visit first
- ☐ Up to 20 entries shown

### SMS + In-App Notifications [NEW]

- ☐ Book appointment as RECEPTIONIST → switch to PATIENT portal tab
- ☐ Bell badge count increases (within 30 seconds auto-refresh)
- ☐ Click bell → Notification Drawer opens (380px, right side)
- ☐ Unread notification: blue left border + bold title
- ☐ Notification shows type icon, message, relative time ( '2 minutes ago' )
- ☐ Click notification → marks read, border disappears, badge decrements
- ☐ "Mark all read" button visible when unread > 0; hidden when 0
- ☐ Click "Mark all read" → all notifications cleared, badge hidden
- ☐ Cancel appointment → APPOINTMENT\_CANCELLED notification in bell
- ☐ Staff: `GET /api/v1/dev/sms-log` → entries show provider=MOCK, status=SENT
- ☐ SMS log message contains appointment date
- ☐ Cancellation creates separate SMS log entry
- ☐ PATIENT role: `GET /api/v1/dev/sms-log` → 403 Forbidden
- ☐ Empty notifications list → 'No notifications yet' shown

### Sign Out

- ☐ Click Sign Out → redirected to /login
- ☐ Visit /patients after sign out → 401 error shown

---

## 27. Known Limitations & Out-of-Scope Items [UPDATED]

The following items are intentionally not implemented in the Patient Module — they are explicitly deferred to other modules:

Item	Owner Module	PRD Reference
Multi-Factor Authentication (MFA)	Auth Module	§7 HIPAA Technical Safeguards
15-minute session timeout	Auth Module	§7 HIPAA Technical Safeguards
Production HTTPS/TLS termination	Infrastructure/Nginx	§6 Security NFR
User management (create/assign roles)	Auth Module	§10 Dependencies
<del>Appointment scheduling</del>	<del>Appointment Module</del>	<del>§9 Out of Scope</del> <b>Implemented in v2.0.0</b>
Prescription management	EMR Module	§9 Out of Scope
EMR / clinical notes (full)	EMR Module	§9 Out of Scope
Billing & payment processing	Billing Module	§9 Out of Scope
Reporting and analytics dashboards	Reporting Module	§9 Out of Scope
Real-time SMS (production Twilio)	Requires Twilio account setup	SMS environment config §3

**Twilio SMS in Development:** By default, the system uses `MockSmsProvider` — all SMS are logged to the `sms_delivery_log` table with `provider=MOCK`, not actually sent. To enable real SMS: set `TWILIO_ACCOUNT_SID`, `TWILIO_AUTH_TOKEN`, `TWILIO_FROM_NUMBER` in `.env`; ensure patient phone is in E.164 format; enable destination country in Twilio Geo Permissions; verify destination numbers (trial accounts only).

**Production Deployment Blocker:** This module MUST NOT be deployed to production without a HIPAA-compliant Auth Module providing MFA and session timeout. The dev-login endpoint ( `DevAuthController` ) issues JWTs without MFA and must be removed or disabled before production deployment.

---

*Document prepared by the Ai Nexus Engineering Team · Patient Module v2.0.0 · February 2026 ·  
CONFIDENTIAL — Internal Use Only Previous version: v1.2.0 (16 features) · This version: v2.0.0 (22 features  
— added Appointment Scheduling, Patient Portal, Structured Allergy Alerts, Visit History Timeline, Enhanced  
Duplicate Detection (Soundex), SMS + In-App Notifications, PATIENT role, International Phone Support)*