CI/CD & Monitoring Plan — XYZ Health Solutions

This document defines the CI/CD pipeline, analyst checkpoints, monitoring strategy, and maintenance workflows for the Patient Management System. It balances automation with compliance-focused oversight to ensure HIPAA-safe and reliable releases.

Part 1: CI/CD Pipeline

Stage	Description	Outputs	Responsible	Informed	Analyst Checkpoint?
Code Commit & Build	Developers push code; build compiles artifacts	Build artifact	Dev Team	QA, Analyst	No
Static Analysis & Security Scan	Automated HIPAA/security scans	Security report	DevOps, Security	Analyst, Compliance	Yes
Unit Tests (TDD)	Logic validation, lockout enforcement	Unit test reports	QA Automation	Analyst	Yes
Integration Testing	Verify cross-module workflows	Integration report	QA	Analyst	Yes
Staging Deployment	Deploy to staging	Staging release	DevOps	Business, Analyst	No
Regression + Compliance	Run REQ-APPT-01 cases	Test logs	QA + Analyst	Compliance	Yes
Manual Checkpoint	Validate logs, errors, audit	Analyst sign-off	Analyst	PM, Compliance	Yes
Release Approval	Go/No-Go decision	Signed approval	Business + Compliance	All Stakeholders	Yes
Production Deployment	Release to production	Live system	DevOps	Business	No
Smoke Tests	Verify booking, record access	Smoke test logs	QA	Analyst	Yes

Monitoring Activation	Enable dashboards + alerts	Monitoring live	DevOps	Analyst, On-call	Yes

CI/CD Risks & Mitigation

Risk	Impact	Severity	Mitigation
Failed tests bypassed	Defective logic deployed	High	Enforce analyst sign-off, CI/CD gate checks
PHI exposed in logs	HIPAA violation	Critical	Mask logs, analyst compliance review
Misconfigured alerts	Incidents undetected	High	Simulate failures pre-release, validate alerts

Monitoring Metrics (with Thresholds)

- Booking Success Rate ≥ 98% (warning < 95%)
- Unauthorized Access Attempts ≤ 10/hour (critical if > 50/hour)
- Failed Login/Error Rate ≤ 2% (critical if > 5%)
- Duplicate Booking Attempts Blocked (100% block required)
- API Response Time < 500ms (warning > 750ms, critical > 1s)
- Audit Log Completeness (100%)
- System Availability ≥ 99.9% uptime

Alerting & Escalation (RACI)

Severity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Warning (Yellow)	QA/DevOps	Analyst	Compliance	Business
High (Orange)	On-call DevOps	Analyst	Security, QA	PM, Compliance
Critical (Red, HIPAA)	DevOps + Analyst	Compliance Officer	CIO, Legal	Regulators, Business

Maintenance Checklist

Daily: QA checks unauthorized attempts, DevOps reviews dashboards, Analyst validates audit logs.

Weekly: QA reruns regression, DevOps patches dependencies, Analyst validates HIPAA compliance.

Monthly: Compliance audits logs, DevOps rotates secrets, Analyst runs incident drill.

Incident Response Workflow

Severity	Response	Communication
Severity 1 (Critical, HIPAA)	Immediate PagerDuty to Analyst + Compliance, escalate CIO, regulator reporting	PagerDuty, Email, Exec Briefing
Severity 2 (High, no PHI)	On-call DevOps + QA rollback/fix, Analyst validates	Slack #ops, Jira
Severity 3 (Medium, minor)	Log bug, schedule fix next sprint	Jira ticket, Analyst follow-up

Analyst Summary

This CI/CD and monitoring plan ensures reliable and HIPAA-compliant deployments. By embedding analyst checkpoints, defining risk mitigation strategies, and establishing clear escalation and maintenance routines, the organization can safeguard patient data, maintain operational stability, and uphold trust.