Post-Launch Risk Management: A Practical Checklist

Use this checklist quarterly and after major releases, integrations, or compliance updates to ensure your platform remains secure, compliant, and audit-ready.

Compliance

[ ] HIPAA / GDPR / applicable regional compliance reviewed in past 12 months
[ ] All BAAs current and counter-signed
[ ] Penetration test completed in past 12 months with findings addressed
[ ] Role-based access control (RBAC) reviewed in past 90 days
[ ] Incident response plan tested in past 6 months
[ ] Audit logs retained for required duration (minimum 6 years for HIPAA)

Infrastructure

[ ] Monitoring and alerting active on all production services
[ ] RTO and RPO targets documented and tested
[ ] Disaster recovery drill completed in past 6 months
[ ] SSL/TLS certificates valid for at least 60 more days
[ ] Dependency vulnerability scan run in past 30 days

Data Integrity

[ ] FHIR resource validation against current terminology servers
[ ] MPI deduplication reviewed in past 90 days
[ ] Patient consent records aligned with current processing register
[ ] Data residency audit completed for all cloud regions in use
[ ] PHI data flow diagram current and accurate

Change Management

[ ] Change classification policy documented and followed
[ ] Rollback procedure tested for last 3 deployments
[ ] Hospital integration partners notified of upcoming API changes
[ ] SaMD design change log current (if applicable)
[ ] Post-market surveillance report up to date (if applicable)

Unchecked items don't always indicate a problem but they can reveal hidden risks that impact hospital partnerships, compliance audits, and future growth.

Book a free 1:1 consultation with our HealthTech engineering experts to identify your highest-priority risks and build a practical remediation plan.