# QA AUTOMATION READINESS CHECKLIST FOR HEALTHCARE ORGANIZATIONS

SOLUGENIX

## 1 STRATEGIC ALIGNMENT

- □ QA automation goals are aligned with regulatory priorities (e.g., timely claims processing, encounter data integrity, audit readiness).
- □ IT and QA strategy supports CMS and DHCS modernization initiatives (e.g., CMS Interoperability Rule, CalAIM, NCQA digital quality measurement).
- □ Executive sponsorship includes Compliance, Medical Management, and IT leadership.

## 2 PROCESS MATURITY

- □ Manual QA processes exist for high-impact functions (e.g., claims adjudication, member eligibility, provider search).
- □ Testing scenarios reflect Medi-Cal/Medicare business rules, benefit structures, and encounter data validation.
- □ Regression test cycles are in place to support state reporting timelines and code updates (e.g., ICD, CPT).

## 3 TEAM CAPABILITY

- □ QA and IT teams have experience working with core administration platforms (e.g., Cognizant TriZetto, HealthEdge, Salesforce Health Cloud).
- □ Teams are trained on healthcare-specific automation frameworks or have access to consultants with payer expertise.
- □ UAT includes state regulatory review (if required) and business owner signoff.

SOLUGENIX

## 4 TECHNOLOGY READINESS

□ Core systems and integrations (EDI 837/835, provider directories, member portals) can be tested via API or UI automation.

□ Environments support HIPAA-compliant test data (e.g., synthetic member data or obfuscated PHI).

□ Selected test tools are approved by IT security and fit into the org's broader modernization roadmap (e.g., cloud readiness, DevSecOps).

## 5 COMPLIANCE & SECURITY

□ Automation strategy supports HIPAA, HITECH, and CMS audit trail requirements.

□ Testing environments use non-production data with masking/scrambling as appropriate.

□ Change control and test logging meet CMS and DHCS documentation standards.

## 6 GOVERNANCE & OVERSIGHT

□ QA automation is governed by PMO or IT governance board with representation from compliance and business ops.

□ Vendor-provided systems are integrated into test planning (e.g., testing managed care platforms, PBMs, or delegated entities).

□ Reporting includes release readiness, risk heatmaps, and traceability back to business-critical functions.

## 7 METRICS & MONITORING

□ Metrics align with audit and performance indicators (e.g., encounter error rates, clean claim rate, code deployment success).

□ Dashboards provide visibility to operations, compliance, and executive stakeholders.

□ Post-deployment monitoring tools are in place to catch issues that automation may have missed (e.g., log analysis, anomaly detection).