TERMS OF REFERENCE (TOR) FOR THE PROCUREMENT OF AN INDEPENDENT TECHNICAL ADVISER (ITA) FOR THE DEVELOPMENT OF SONGHAI HEALTH TRUST LIMITED PROPRIETARY SOFTWARE PLATFORM DEVELOPMENT

Table of Contents

1. Project Background and Context

1.1 Project Description

Songhai Health Trust Limited is embarking on the development of a hybrid custom–modular Proprietary Software platform to automate critical Health Maintenance Organization (HMO) functions. These include claims processing, provider and enrollee management, call centre workflows, integrated finance, and zonal operations. The platform will leverage cloud-native principles, modular architecture, and secure data management to support long-term scalability and digital transformation.

1.2 Rationale

The complexity and strategic importance of this initiative necessitate the engagement of an Independent Technical Adviser (ITA). The ITA will provide unbiased oversight, bridging knowledge gaps in system architecture, compliance, and vendor evaluation. Their independent perspective will safeguard against vendor bias, ensure adherence to regulatory standards (NDPR, NHIA, HIPAA, ISO/IEC 27001), and align the project with Songhai's 2025–2030 Strategic Plan.

2. Objectives of the Advisory Role

The objective of engaging the Independent Technical Adviser (ITA) for the Songhai Health Trust Limited Proprietary Software platform project is to provide expert guidance and independent oversight that ensures the platform meets its functional, architectural, security, performance, and compliance standards while aligning with Songhai's strategic goals. The ITA will support structuring, negotiating, and executing the technical and operational aspects of the Proprietary Software project, ensuring the technical framework adheres to industry best practices and organizational objectives.

Specifically, the ITA will:

- Develop/Design the architecture.

- Provide independent verification and validation of project plans, vendor deliverables, and compliance requirements.

- Serve as the quality assurance backbone throughout the project's execution, minimizing risks and enhancing system quality.

- Ensure the platform is scalable and maintainable to support Songhai's future growth.

- Offer unbiased technical guidance spanning system architecture, security standards, performance optimization, and regulatory compliance.

- Bridge knowledge gaps on technical and operational fronts, especially relating to vendor evaluation and regulatory frameworks.

- Ensure Songhai Health Trust Limited achieves full ownership of the software's intellectual property, architecture, and data to reduce dependency on external vendors.

This engagement is essential to guarantee the proprietary platform's technical integrity, sustainability, and alignment with Songhai's 2025–2030 Strategic Plan, fostering long-term operational success and minimizing implementation risks.

2.1 Project Objectives

I.   Strengthen Organizational Ownership & Control
Ensure Songhai Health Trust Limited achieves full ownership of the software's intellectual property, architecture, and data to reduce dependency on external vendors and enable sovereign control in Nigeria's digital health landscape.

II. Enhance Operational Efficiency
Streamline core business processes by digitizing workflows, reducing manual tasks, increasing accuracy and productivity across departments, enabling data mining, fraud elimination, and AI/predictive modelling for claims processing.

III. Improve Data Security & Compliance
Implement a secure, internally managed system that meets all regulatory, privacy, and cybersecurity standards (NDPR, NDPA 2023, NHIA, HIPAA, ISO 27001) governing health and financial information.

IV. Build Internal Technical Capacity
Develop internal capability to run, host, support, and maintain the system, including staff training and establishment of in-house support structures aligned with national digital skilling initiatives.

V.   Achieve Cost Efficiency & Long-Term Sustainability
Lower long-term operating costs by eliminating ongoing licensing fees and reducing reliance on outsourced technical solutions through proprietary ownership.

VI. Integrate Organizational Systems
Create a unified platform that seamlessly integrates with existing tools, databases, and processes to support real-time insights and decision-making with NDHA interoperability.

VII.   Support Scalability & Future Growth
Design the platform to scale with organizational service expansions, technological needs, and operational complexity under NDHI national integration phases.

VIII.   Improve Service Delivery & Customer Experience
Enhance quality, speed, and reliability of services delivered to clients and stakeholders through automation and improved system availability.

IX.   Enable Data-Driven Decision Making
Implement robust analytics, dashboards, and reporting capabilities to support strategic planning, performance monitoring, and public health surveillance.

X.   Ensure System Reliability & Business Continuity
Build a resilient system with strong backup, disaster recovery, uptime, and failover mechanisms to ensure uninterrupted operations.

3. Scope of Work / Responsibilities

3.1 Needs Assessment

- Conduct detailed mapping of Songhai's existing IT assets, applications, infrastructure, and workflows to understand the current operational landscape.

- Carry out stakeholder interviews and workshops including technical teams, call center staff, finance departments, and zonal operations to gather explicit and tacit requirements for the *Proprietary Software* platform.

- Identify interoperability points with legacy systems and third-party applications, articulating technical constraints and integration needs.

- Evaluate available data sources, data quality, and data governance policies to ensure adequacy for platform analytics and reporting.

- Establish baseline cybersecurity posture and compliance maturity against NHIA, NDPR, and HIPAA to inform design and risk mitigation controls.

3.2 Strategy and Planning

- Develop an IT strategy aligned with Songhai's digital transformation priorities, balancing rapid delivery with robust risk management.

- Adopt agile project management methodology including iterative planning, frequent reprioritization, and sprint-based delivery cycles to enhance responsiveness and flexibility.

- Define clear Key Performance Indicators (KPIs) such as system uptime, claims processing speed improvements, user satisfaction, and regulatory compliance scores.

- Incorporate scalability targets enabling phased expansions from Minimum Viable Product (MVP) to enterprise-scale deployment across all zones and functions.

- Integrate risk assessment checkpoints within planning phases to proactively identify technical, operational, and vendor risks and corresponding mitigation strategies.

3.3 Technical Guidance

- Architect the platform leveraging microservices to decouple functionalities for ease of maintenance, scalability, and independent deployment cycles.

- Specify secure API design standards enabling seamless communication with provider networks, enrollee portals, finance systems, and external regulators.

- Enforce multi-factor authentication and role-based access controls to enforce the principle of least privilege critical for sensitive health and financial data.

- Recommend use of encrypted data storage, end-to-end data transmission security standards (TLS/SSL), and real-time monitoring for suspicious activities to meet NDPR and HIPAA guidelines.

- Advise on containerization and orchestration technologies (e.g., Docker, Kubernetes) for cloud deployment flexibility and automated scaling.

- Design comprehensive disaster recovery and business continuity plans incorporating regular backups, failover strategies, and incident response workflows.

3.4 Procurement Support

- Draft clear and unambiguous RFPs and RFQs incorporating detailed functional, technical, and security requirements alongside SLAs and key milestones.

- Establish evaluation criteria weighting technical capability, regulatory compliance, vendor experience within healthcare Proprietary Software, implementation timeline, and total cost of ownership.

- Facilitate vendor pre-bid clarifications sessions to ensure consistent understanding across potential bidders and minimize ambiguities in proposals.

- Assemble an objective evaluation panel including technical leads, procurement officers, legal counsel, and end-user representatives to ensure holistic assessment.

- Negotiate vendor contracts embedding clauses for data protection responsibility, penalties for SLA violations, and post-deployment support commitments.

3.5 Implementation Oversight

- Implement a formal governance structure comprising project steering committees, technical working groups, and risk management boards with defined charters.

- Establish project management dashboards tracking sprint progress, defect densities, deployment frequencies, and technical debt metrics.

- Conduct weekly sprint reviews involving developers, testers, and business users to monitor deliverables and gather continuous feedback.

- Enforce change control management processes evaluating impact analysis, traceability, and roll-back plans prior to production deployments.

- Coordinate cybersecurity audits and penetration tests at critical phases to uncover vulnerabilities and verify mitigation effectiveness.

- Monitor vendor performance metrics including adherence to project timelines, quality of deliverables, responsiveness to issues, and escalation management.

3.6 Capacity Building

- Assess baseline technical expertise and capacity within Songhai's IT team to tailor upskilling programs on cloud architecture, microservices, and cybersecurity.

- Deliver structured training workshops, seminars, and hands-on labs covering system administration, monitoring tools, and incident management.

- Establish mentorship and knowledge-sharing platforms facilitating ongoing learning post-project completion and fostering a culture of continuous improvement.

- Support documentation of operational and troubleshooting manuals suitable for IT team and end-users to reduce dependence on vendor support.

3.7 Documentation and Reporting

- Mandate version-controlled documentation repositories housing architecture diagrams, API specs, test plans, issue logs, and compliance checklists ensuring accessibility and auditability.

- Draft concise bi-weekly status reports highlighting milestone achievements, blockers, risk profiles, and mitigation actions for operational stakeholders.

- Compile quarterly comprehensive technical review reports synthesizing quality assurance outcomes, security audit results, and compliance status for governance bodies.

- Collaborate with communication teams to produce executive summaries, knowledge articles, and project newsletters fostering stakeholder engagement and transparency.

3.8 Additional Responsibilities

- Mediate technical disputes between vendors, ensuring alignment with architectural principles and project objectives.

- Lead configuration management efforts standardizing environments across development, staging, and production ensuring consistency and traceability.

- Provide strategic insights on emerging technologies, compliance trends, and market innovations to future-proof platform capabilities.

4. Deliverables

4.1 Inception Report

- Comprehensive baseline evaluation of Songhai's existing IT systems, workflows, and readiness for Proprietary Software adoption.

- Detailed stakeholder needs assessment findings including functional and non-functional requirements covering claims processing, enrollee/provider management, finance integration, and call center operations.

- Risk assessment profiling technical, regulatory, and vendor-related risks with proposed mitigation frameworks.

- Advisory engagement plan specifying methodology, milestones, reporting cadence, quality assurance protocols, and communication strategies aligned with Songhai's 2025–2030 Strategy.

4.2 System Architecture Blueprint

- Detailed architecture models illustrating microservices layout, data flow diagrams, API designs, and cloud infrastructure components supportive of scalability and security.

- Security architecture specifying encryption standards, multi-factor authentication flows, role-based access control models, data residency

guidelines, and incident response framework in line with NDPR, NHIA, and HIPAA.

- Integration design illustrating interoperability strategies for connecting legacy systems, external providers, payment gateways, and regulatory data feeds.

- Disaster Recovery and Business Continuity plans outlining failover mechanisms, backup schedules, recovery time objectives (RTO), and recovery point objectives (RPO).

4.3 Procurement Inputs

- Complete and clear RFP and RFQ documents defining technical specifications, compliance requirements, implementation timelines, SLAs, and penalty clauses.

- Vendor qualification criteria incorporating previous healthcare Proprietary Software experience, compliance certifications, financial stability, and post-deployment support capabilities.

- Bid evaluation frameworks with weighted scoring matrices emphasizing security, scalability, delivery track record, and total cost of ownership.

- Answers to vendor clarifications and formal addenda ensuring fair and transparent procurement process.

4.4 Regular Progress Reports

- Bi-weekly status reports containing deliverables status, sprint retrospectives, emergent issues, risk profiles, and action plans.

- Quantitative dashboards tracking defect rates, test coverage, deployment frequency, and KPI attainment (e.g., claims processing time reduction, user adoption).

- Narrative summaries highlighting key decisions, vendor evaluations, and strategic recommendations.

- Quarterly comprehensive reports consolidating technical, security, operational, and compliance progress for management oversight.

4.5 Stakeholder Presentations

- Tailored presentations at critical milestones (project initiation, architecture approval, MVP delivery, UAT, go-live) with executive dashboards.

- Visual risk heatmaps, progress charts, compliance summaries, and financial spend reports supporting informed decision-making.

4.6 Risk Management Documents

- Continuously updated risk register documenting risk IDs, descriptions, ownership, impact, likelihood, and mitigation status.

- Scenario-based contingency plans including cybersecurity incident response and vendor fallback strategies.

- Communication protocols for escalating risk exposure to executive levels promptly.

4.7 Compliance Audit Reports

- Regulatory adherence assessments against NDPR, NHIA, HIPAA, ISO 27001, and local data privacy laws.

- Privacy Impact Assessments identifying data protection risks and recommending mitigation measures.

- Gap closure action plans prioritized by risk severity and resource availability.

4.8 Technical Due Diligence Report

- Objective evaluations of vendor technical architecture, cloud infrastructure readiness, data security, and compliance with healthcare norms.

- Vendor qualifications analysis including past healthcare Proprietary Software projects and operational reliability.

4.9 Requirements Validation Report

- Traceability matrices linking business requirements to system functionalities with documented validation evidence.

- Gaps analysis and resolution tracking, ensuring user acceptance criteria are fully met.

4.10 Development Oversight Reports

- Sprint-wise records tracking feature completion, defect identification, resolution progress, and regression test results.

- Measures to manage technical debt and ensure sustainable code quality.

4.11 Testing & Quality Assurance Review

- Evaluation of testing coverage (unit, integration, system, security, UAT), automation effectiveness, and defect resolution turnaround times.

- Security penetration test outcomes and remediation status.

4.12 Security & Compliance Audit Summary

- Security posture summaries including incident response readiness, control effectiveness, audit findings, and training programs status.

4.13 Go-Live Readiness Assessment

- Formal verification of technical stability, data integrity, user training, support readiness, and cutover plans for seamless transition.

4.14 Final Acceptance Recommendation

- Formal sign-off document certifying contract fulfillment, system functionality, security, and operational readiness for official launch.

4.15 Comprehensive Close-Out Report

- Review of project achievements and compliance certifications.

- Lessons learned and recommended improvements.

- Documentation of knowledge transfer and post-implementation support agreements.

5. Required Qualifications and Experience

5.1 Individual Independent Technical Adviser (ITA) Qualifications and Competencies

Technical Expertise:

- Proven years of cogent experience in software engineering, enterprise IT systems, cloud architectures, and Proprietary Software platform development with a focus on healthcare or insurance sectors.

- Proven expertise in APIs, microservices, DevOps methodologies, modular architectures, and cloud platforms such as AWS and Azure.

Regulatory and Industry Knowledge:

- Deep familiarity with Nigerian healthcare sector regulations, including NHIA, NDPR, NDPA 2023, data protection, cybersecurity, and compliance frameworks such as HIPAA and ISO/IEC standards.

Professional Skills:

- Strong problem-solving and analytical capabilities.

- Superior documentation, communication, and stakeholder engagement experience.

- Demonstrated project leadership and advisory skills on large IT projects.

Education and Certifications:

- Master's degree in information technology, Computer Science, Engineering, or equivalent.

- Certifications such as AWS/Azure Solutions Architect, PMP, Agile Scrum Master, CISA, CISSP, and TOGAF strongly preferred.

Additional Requirements:

- Valid professional indemnity insurance coverage.

- Operational independence free from conflicts of interest.

5.2 ITA Company Qualifications

- Multidisciplinary teams with a combined experience of 7 to 15 years in technical leadership of healthcare Proprietary Software and regulated software projects.

- Proven understanding of regulatory landscapes relevant to Nigerian HMOs, data privacy, and cybersecurity.

- Established governance and project management practices, including risk management and vendor oversight.

- Advanced professional certifications among team members.

- Commitment to operational independence and conflict of interest management.

6. Timeframe and Institutional Arrangements

- Engagement duration: 12 to 15 months covering all project phases from architecture, development, testing to go-live and stabilization.

- Reporting: Bi-weekly operational reports to Managing Director; quarterly strategic reviews to Finance & General-Purpose Committee.

- Mode of operation: Hybrid onsite presence in Abuja with remote work and periodic visits to zonal offices.

- Contractual terms embody confidentiality, independence, and clear termination guidelines.

7. Reporting and Governance

- Direct reporting to Managing Director for day-to-day technical oversight and progress monitoring.

- Monthly and quarterly detailed reports for Finance & General-Purpose Committee.

- Active participation in steering committee meetings for strategic alignment and governance.

- Comprehensive documentation of all advisory activities, findings, and decisions in structured reports.

8. Confidentiality and Conflict of Interest

- ITA shall sign strict Non-Disclosure Agreements protecting Songhai's proprietary and sensitive data.

- Access to confidential information limited to authorized project staff only.

- Declaration of any actual or potential conflicts of interest with project vendors or stakeholders.

- Commitment to uphold highest confidentiality standards throughout engagement.

9. Expected Outcomes

- Delivery of a technically sound, secure, scalable, and compliant proprietary platform aligned with strategic organizational goals.

- Minimization of project risks including technical, operational, regulatory, and vendor performance through rigorous independent oversight.

- Enhanced project transparency, governance, accountability, and stakeholder confidence.

- Safeguard Songhai's interests through impartial vendor evaluations and quality assurance activities.

- Facilitate faster and better-informed executive decisions via timely and accurate technical insights.

- Enable Songhai's competitive positioning in Nigeria's healthcare market with a state-of-the-art digital platform.

10. Other Provisions

- All intellectual property rights and data ownership remain exclusively with Songhai Health Trust Limited.

- The ITA shall foster a culture of continuous improvement, adaptability, and innovation within the project framework.

- Comprehensive knowledge transfer and capacity building to empower Songhai's institutional sustainability post-project.

- The engagement shall comply fully with applicable Nigerian laws, international standards, and ethical business practices.

11. Conclusion

This Terms of Reference document establishes a comprehensive framework for engaging an Independent Technical Adviser to provide expert, unbiased, and strategic oversight of Songhai Health Trust Limited's proprietary software platform development. By detailing qualifications, responsibilities, deliverables, governance, and expected outcomes tailored to the healthcare Proprietary Software environment in Nigeria, this ToR ensures clarity of purpose and accountability, ultimately contributing to the successful delivery of a transformative digital health solution.