Ministry of Technology

Information and Communication Technology Agency of Sri Lanka

BIDDING DOCUMENT -– SECTION VI

SCHEDULE OF REQUIREMENT

(Volume 2 of 3)

(Single-Stage Two Envelope Bidding Procedure)

Procurement of Design, Development, and Implementation of an extended and integrated version of Hospital Health Information Management System (HHIMS) that featuring Diabetes Module to facilitate Diabetes Compass Project

IFB No: ICTA/GOSL/NCB/IS/2023/01

Employer: Chairman
Information and Communication Technology Agency of Sri Lanka
No 490,
6th Floor,
R. A. De Mel Mawatha,
Colombo 03.

September 2023

Abbreviations

Please note the following abbreviations used throughout this tender document.

API	Application program Interface
CR	Change Request
CICD	Continuous Integration and Continuous Delivery
DSRS	Detailed Software Requirement Specification
DSTD	Detailed Software Technical Design
FAQ	Frequently Asked Questions
NFR	Non Functional Requirements
NPF	National Policy Framework
LGC	Lanka Government Cloud
LGN	Lanka Government Network
OAT	Operational Acceptance
PoC	Proof of Concept
REST	Representational State Transfer
SRS	System Requirement Specification
SLA	Service Level Agreement
SPA	Software Process Audit
SQA	Software Quality Assurance
UAT	User Acceptance Certificate
UI	User Interface

Contents

Table of Figures

Procurement for Design, Development, and Implementation of an extended and integrated version of Hospital Health Information System (HHIMS) that featuring diabetes module to facilitate Diabetes Compass Project

1. Background

The Information and Communication Technology Agency (ICTA) of Sri Lanka is the apex ICT institution of the Government and has been mandated to take all necessary measures to implement the Government's Policy and Action Plan in relation to ICT.

The implementation of the Hospital Health Information Management System (HHIMS) under the Digital Health Project was a collaborative project implemented by ICTA and the Ministry of Health to establish and maintain Electronic Medical Record (EMR) systems in selected Government hospitals. The HHIMS has been implemented in more than 70 hospitals at present. Electronic medical records of more than 8 million patients are maintained in HHIMS and the number of patients and the records are increased on a daily basis. This system enhances the ability of health care professionals for effective diagnosis and coordinated care by providing patient's health information.

The Diabetes Compass Program of World Diabetes Foundation (WDF) supports vulnerability reduction and drives care optimization to improve the lives of people living with diabetes. The Diabetes Compass Program was launched in Sri Lanka in close collaboration with the Ministry of Health and the Sri Lanka College of Endocrinologists;

The WDF has identified the HHIMS as the designated software platform for facilities with diabetes and hypertension clinic services. In this context, WDF has proposed to integrate the Diabetes Compass Programme with the HHIMS and thereby extend the dedicated diabetes and hypertension modules within the HHIMS to enhance case management and data capture.

Therefore, ICTA has been requested to design, develop, and implement an extended and integrated version of HHIMS that features the Diabetes Compass Programme. This extended version of the HHIMS will be deployed at several selected facilities in the Kalutara District

2. Objective of the Project

In order to meet the Ministry of Health and WDF requirement to integrate with the HHIMS, ICTA intends to hire a Bidder to achieve the below stated brief scope of services within a period of seven (7) months, conforming to the industry standards, implementing, integrating with internal and external applications and providing support and maintenance for a period given under the scope of work.

The Bidder is required to design, develop, implement and maintain the solution. The total duration of the assignment comprises of time for system design, development, final deployment including periodic user training/ demonstrations/ operational acceptance (7 months) and support and maintenance is 12 months.

Key objectives of the assignment are as follows;

a) Design, develop, and implement an extended and integrated version of HHIMS that features a diabetes and hypertension module.
b) Deploy the upgraded version of HHIMS at 7 hospitals at Kalutara district
   - 5 currently operational Primary Care Facilities (5 Divisional Hospitals),
   - 1 currently operational upper level facility at the base hospital
   - 1 newly identified Primary Care Facility
c) Develop integration capabilities with the latest FHIR interoperability standards to HHIMS in order to share identified clinical data with external applications related to health information systems (HIS).
d) Support and maintenance of the upgraded HHIMS for the purpose of the Diabetes Compass program [above (a) to (c)] for twelve (12) months operational period.

3. Scope of Services

Description	Bidders Compliance	Reference (Section No and Page NOs)
3.1 General Requirements The bidder shall fulfill/facilitate all of the following; 3.1.1. Understand the overall scope of the initiative. 3.1.2. The bidder is responsible for the design, development, deployment, support, and maintenance of the solution within the given timeline. 3.1.3. The employer will fulfill the facilities and services as indicated in **Section 5** "Services and Facilities provided by the employer" of the document. The bidder works in collaboration with the employer in order to fulfill the objectives of this project. 3.1.4. Further to the above, any dependent actions/services should be mentioned by the bidder to the employer in advance. 3.1.5. The bidder shall formulate an "Operational Manual" outlining, among others, maintenance and operational aspects. The operational manual shall include all relevant sub-manuals that would outline procedures and relevant criteria which would facilitate all stakeholders associated with this project for successful operational governance. 3.1.6. The bidder shall be responsible for the successful and timely delivery of the project. 3.1.7. The Project Director/Manager appointed by the bidder is responsible for the delivery of the project (single point of contact) and shall liaise with the Employer and work closely with the employer's project management team with regard to all matters related to the project.		

3.1.8. Project Director/Manager appointed by the bidder's responsibilities include among others;

    3.1.8.1.   Attending all project meetings

    3.1.8.2.   Ensure relevant project team members participate in project meetings

    3.1.8.3.   Ensure all internal and external communications and escalations are done to avoid delivery delays.

    3.1.8.4.   Delivery of the project successfully.

    3.1.8.5.   Submit weekly progress reports to the ICTA

    3.1.8.6.   Ensure the help desk and related support functions are in place.

3.1.9. The bidder shall submit a detailed project proposal at the commencement of the project and shall obtain acceptance from the employer.

3.1.10. The bidder shall ensure a smooth handover of the related project components and artifacts at the end of the contractual time period.

3.1.11. The items listed as requirements and deliverables must be used only as guidance of the deliverables and not as a limiting factor to providing additional information required that may not be listed here.

3.1.12. The Employer will NOT expected to use any commercial licenses for this development.

3.1.13. Adherence to common industry standards

    3.1.13.1.   The software, hardware, network & communication technologies proposed by the bidder MUST be based on non-propriety and common industry standards whenever such standards are available and applicable.

    3.1.13.2.   The bidder should study existing HHIMS application and required integrations with organizations and carry out any enhancements needed for the proposed solution in order to provide a more comprehensive service which will be reviewed by ICTA.

3.1.13.3.   The bidder may leverage their own environments for development and end-user application training in order to achieve the delivery timelines if needed.

3.1.13.4.   The bidder should follow templates if provided by ICTA for deliverables.

3.1.13.5.   Participate in Project Review Committee meetings and Project management committee Meetings as a member and present the status of the project when necessary.

3.2. Implementation Approach

3.2.1. The Bidder should study the existing HHIMS solution and should carry out requirement study with the stakeholders to identify new features and functionalities be implemented in HHIMS Solution. Refer to **Annex A and B** and other related artifacts.

3.2.2. Bidder should study and design improved user journeys.

3.2.3. On completing the above, a Detailed Software Requirements Specification (DSRS) and a Detailed Software Technical Design (DSTD), including the proposed solution architecture design should be submitted.

3.2.4. Upon obtaining approval from the committee appointed by ICTA for the above, the Bidder should design and develop the solution.

3.2.5. The implementation shall span across the following stages of the software development lifecycle

3.2.5.1.   Planning

3.2.5.2.   Development and customization

3.2.5.3.   Set-up of staging and production environment including required tools

3.2.5.4.   Unit Testing, System Testing, Integration Testing, Performance Testing

3.2.5.5.   UAT

3.2.5.6.   Release management

3.2.5.7.   Continuous build (Continuous Integration, Continuous Deployment)

3.2.5.8.   Deploy

3.2.5.9.   OAT

3.2.5.10. Enhancement and augmentation		
3.2.5.11. Technical Support, Troubleshooting, Identification, and Resolution		
3.2.5.12. Change and version control		
3.2.5.13. Patch management		
3.2.5.14. L1, L2, and L3 support for all applications		
3.2.6. The entire solution shall be web-based and web-enabled.		
3.2.7. The proposed solution should be browser independent and able to access with less configuration in the client workstation.		
3.2.8. The proposed solution should be compatible with the HHIMS technology stack and should be able to deploy into staging and production in cloud platform provided by ICTA.		
3.2.9. The Bidder should consider the use of existing source code of HHIMS solution wherever possible with the intention of reducing the time and cost of the development while ensuring the objectives stated above.		
3.2.10. Standards used in the System shall be compatible with existing Technology Stack of the HHIMS (Refer Annex A - Overview of the Current HHIMS System)		
3.2.11. The Bidder should study and apply the Sri Lanka FHIR profiles to the HHIMS system developments.		
3.2.12. The Bidder should define the Infrastructure resource requirements based on the deployment architecture.		
3.2.13. The Bidder should study and facilitate API integrations to external systems.		
3.2.14. The Bidder should propose and develop the required APIs. Bidder should provide an API specification document.		

3.2.15. The Bidder should follow the proper coding standard and maintain project source code in the ICTA GITHub system and upload all the relevant documents to the ICTA Document Management.		
3.2.16. Source code should be regularly updated when making changes to the system.		
3.2.17. The configuration file required for the deployment should be committed to the source code repository in a separate folder structure		
3.2.18. All IP rights of the source code should be with ICTA		
3.2.19. Adopt a proper application release procedure to release the applications to the environments during the deployment in the staging/ production environments at the cloud (configure, replicate and data migration to the server).		
3.2.20. The Bidder should follow templates if provided by ICTA for deliverables.		
3.2.21. Bidder should formulate test plans, and test cases, The UAT shall be conducted to give acceptance and commence operations.		
3.2.22. Developed solution shall be audited by Sri Lanka Computer Emergency Readiness Team (SLCERT) to identify system security vulnerabilities. The Bidder shall fix all security related recommendations as per the report submitted by SLCERT; prior to solution launch and during the support and maintenance period.		
3.2.23. The proposed solution should have a proper data backup plan and equip with a high availability and fault tolerance plan as per the project requirements.		
3.2.24. The Bidder should conduct meetings/ workshops when necessary to identify and verify the requirements with all the relevant stakeholders. Bidder should propose any		

business process improvement if required as well. ICTA will assist in coordinating these meetings.		
3.2.25. The Bidder is expected to improve the given architecture as per the Client's requirement. Refer to **Annex E.**		13
3.2.26. The Bidder should submit all deliverables as specified in **Section 4**		
3.2.27. ICTA intends to launch the proposed solution in seven (7) months period. One (01) year of Support and Maintenance will commence from the date of operational.		
3.2.28. The Bidder should present an application prototype covering major functionalities of the proposed solution such as, but not limited to user scenarios, workflows, document management.		
3.2.29. The bidder should implement all non-functional requirements (security, governance including role-based security, user lifecycle management, and complete audit trails, etc.) mentioned in the Annex C.		
3.2.30. The Bidder should propose the most appropriate technical solution to secure and expose data.		
3.2.31. The Bidder should understand and ensure the existing data volume and data complexity and provide data migration strategy accordingly. Moreover, data transformation strategy should follow the proper industry standards and proper control mechanisms in transforming these data in to the new solution.		
3.2.32. The Bidder should migrate the existing data of HHIMS (at given locations) to the newly developed system.		
3.2.33. The Bidder should ensure the high availability of the system and proper disaster recovery with a proper system backup procedure.		

3.2.34. The Bidder should provide support and maintenance services, from the date of operational and for a period of 1 year and adhere to the Service Level Agreement (SLA), during the period. Refer to Annex D.

3.2.35. The Bidder should attend to any issues reported and carry out configuration changes (if required), apply relevant security patches, update and tuning of performance, etc. to make sure the security of the solution during the support and maintenance period.

3.2.36. The Bidder should hand over the source code and relevant updated documents to ICTA at the **end of the S&M** period with proper knowledge transfer sessions to the ICTA technology team including the following updated artifacts.

    3.2.36.1.1.   Detailed Software Requirement Specification

    3.2.36.1.2.   System Architecture Design Document

    3.2.36.1.3.   Detailed Software Technical Documentation (DSTD)

    3.2.36.1.4.   Solutions Installation Guide (including deployment view)

    3.2.36.1.5.   QA Test Plan, Test Cases, and Test Scripts

    3.2.36.1.6.   Application User Manual

    3.2.36.1.7.   Deployment guide, patch, and issue fix delivery approach

3.2.37. The Bidder should accommodate change requests (CR) after obtaining the approval from the Change Control Board and as per the CR rate agreed in the Contract.

3.2.38. The Bidder should participate in Project Review meetings and present the status of the project when necessary.

Description	Bidders Compliance	Reference (Section No and Page NOs)
3.2.39. The Bidder should work collaboratively with ICTA and some government organizations throughout the tenure of the project. 3.2.40. The Bidder should sign a Non-Disclosure Agreement (NDA) at the signing of the Contract where applicable.		15

Description	Bidders Compliance	Reference (Section No and Page NOs)

3.3. System Administration and Management Functions
 	
3.3.1.The proposed solution needs to support any functional requests raised by the Government Hospitals. Each support level will be organized as below.
    3.3.1.1.1.   Level 1 (L1): Superusers, IT staff from each Government hospitals to manage basic queries and basic user management activities.
      3.3.1.1.1.1. Level 2 (L2): ICTA staff to manage the Super Administrator role with basic technical support and user management activities.
    3.3.1.1.2.   Level 3 (L3): Vendor technical team to resolve any technical issues with a pre-defined SLA.
 	
3.4. Architectural Requirements
 	
3.4.1.The Bidder should study the existing infrastructure and capabilities of LGC and should provide detailed specifications with the technical design.		

3.4.2. The proposed solution needs to be deployed in Lanka Government Cloud (LGC) by the Bidder and ICTA will provide hardware infrastructure at the ICTA Data Center as Infrastructure as a Service (IaaS).

3.4.3. Hospitals have access to the LGC via Lanka Government Network (LGN). The proposed solution will be accessed by the individual users via LGN.

3.4.4. The proposed solution needs to be deployed on the existing LGC OpenStack environment where Bidder will be given admin access to OpenStack tenants and they can deploy virtual instances, and create networks, security groups, and cloud storage.

3.4.5. Recommend implementing the system to comply with a high-level architecture diagram is given in **Annex E**. Please note that this is an indicative illustration only. If there are any changes suggested by the bidder, ICTA will evaluate the same.

3.4.6. The Bidder must ensure that the architecture is open and scalable by design.

3.4.7. Screen designs (UI/UX) along with user journeys need to be reviewed and approved by ICTA technical committee

3.5. Performance Requirements

3.5.1. The proposed solution will cater to the requirements of hospitals. Initial 200 users will get on boarded with this project within the first 6 months. The solution needs to maintain acceptable performance levels throughout this expansion.

3.5.2. Solution performance levels will be measured primarily with the end-user experience. These expected end-user experience levels need to be maintained even while the back-end office functionalities such as backup process, archiving process, etc… are getting executed.

3.5.3. With the proposed solution, a performance level with concurrency behaviors needs to be submitted (preferred through a graph). Concurrency intervals to be considered between 500 and 1000.

3.5.4. Expected general web application performance as mentioned in Non-functional requirements in **Annex C**.		
3.5.5. Within the LGC virtual network throughput will be up to 10 Gbps. Memory CPU storage can be extended depending on the requirement.		
3.5.6. The Bidder should provide the minimum hardware requirement, network-related performance parameters (bandwidth, latency, jitter, packet loss, etc.), and hosting-related performance parameters (disk IOPs) to run the solution as per the expectations specified above.		
3.5.7. In the event of a performance-related incident occurs, there needs to be a scientific or a technical tracing mechanism implemented in the solution to clearly segregate the cause of the incident is due to hardware and /or network or anything related to the software and its components provided by the Bidder. Performance parameters need to be measured through the tools and dashboards.		
3.5.8. If there are any software components that need to be installed or implemented to manage the service performance, those need to be included in the solution and the bidder needs to clearly explain the use and the behavior of the same. Such tools should not be licensed-based.		
3.5.9. The performance of the solution needs to be tested and demonstrated with automated load testing during the implementation phase of the project. Performance and load test plans need to be submitted along with the associated scripts. These test plans need to cover indicators such as ramp-up, scale-up, scale down, and peak loads.		
3.5.10. Security Requirements need to be adhered to as per the Non-Functional Requirement (NFR) explained in **Annex C**.		
3.6. Mandatory / Minimum Performance Compliances.		
3.6.1. Bidder needs to deliver the features mentioned in the functional requirements (**Annex B**) and technical requirements given		

below. Bidder may suggest a better approach to deliver more value to the solution if there are any.

3.6.1.1. Front end: Performance, usability, and security need to adhere to compliance given by ICTA. The front end needs a security scan and a load test/performance test

3.6.1.1.1. The solution should have a monitoring mechanism to monitor (application health and infrastructure monitoring) across the platform.

3.6.1.1.2. Below specifications in development are recommended:

- Deployment handover to include technical training.
- React is recommended for front-end development
- This should be a responsive web application that is fully usable with mobile device
- maintenance to be easy and effective
- Proposed front-end development and deployment architectures should be recommended by ICTA

3.6.1.2. Back end: Performance and security need to adhere to compliances given by ICTA. It needs a security scan and a load test/performance test.

3.6.1.2.1. Primary services shall include Citizen Service, and Monitoring Service, Reporting service.

A suitable services list should be proposed.

3.6.1.2.2. API management and documentation

API specification document (swagger) should be provided.

API doc should be maintainable with future upgrades and versioning.

3.6.1.3. Testing

3.6.1.3.1. The bidder should submit a quality plan and quality assurance and control criteria.

3.6.1.3.2. Unit Test: Backend minimum 80% unit test coverage. Frontend 60% unit test coverage.

3.6.1.3.3. API test automation 90% integration test coverage (REST Assured). Infrastructure for the automation will be provided by ICTA.

3.6.1.3.4. Cover 8 dimensions of quality management

3.6.1.3.5. Load testing approach and model.

3.6.1.3.6. Stress testing approach and model.

3.6.1.3.7. Endurance testing approach and model.

3.6.1.4. **General specifications:** Entire applications should be implemented in a cloud-native fashion in a virtual environment and comply with the given architecture.

3.6.1.4.1. Open-Source free tools, libraries, and frameworks preferred

3.6.1.4.2. Loosely coupled services

3.6.1.4.3. The API-driven back end is preferred

3.6.1.4.4. Stateless APIs are preferred

3.6.1.4.5. Should run on Lanka Government Cloud (LGC)

3.6.1.4.6. The solution should have High Availability (HA). Bidder should suggest the approach.

3.6.1.4.7. Mobile-first responsive front ends. Need to provide OS and mobile devices front-end platform support.

3.6.1.4.8. Preferred to adhere to 12-factor app (https://12factor.net/)

3.6.1.4.9. The solution should have a Disaster Recovery mechanism. Bidder should suggest the approach.

3.6.1.4.10. Data backup and recovery approach, tools and technologies used for the backup and recovery

3.6.1.5. Implementation guidelines

3.6.1.5.1. Code quality should be enforced both at the IDE level, peer review, and sonar lint level. Static scan reports, Dynamic scan reports, and Profiling reports need to be provided.

3.6.1.5.2. Consistent look and feel across all UIs.

3.6.1.5.3. Bidder can propose the working data model and get approval from ICTA

3.6.1.5.4. Bidder can propose the designer UIs for new features to serve the purpose. ICTA should be able to customize the proposed UI design.

3.6.1.5.5. Semantic versioning for APIs

3.6.1.5.6. Ability to emulate service in the local environment for testing

3.6.1.5.7. Documentation requirements:

- System Requirement Specification
- System Design Document (Architectural Document adhering to 4+1 views model)
- Deployment guidelines
- API specification document
- Test plan and test results
- UAT plan, UAT results
- User manual
- Hardware specification
- Maintenance model with patching and support SLAs
- Configuration details
- Backup strategy and restoration plan
- DR strategy and plan (Including BCP)
- Training plans and materials by user type
- Issue fixing, patch update and code deployment guide

3.7. Testing and Quality Assurance Requirements

3.7.1. Software Process Audit

3.7.1.1. ICTA will be conducting an independent audit process (Software Process Audit - SPA) on the developed applications. ICTA SPA Team will review all the deliverable (Technical and QA) and verify the application based on functional and non-functional aspects in order to certify the application is aligned with the requirement.

3.7.1.2. The bidder should comply with the process/product quality and standards and should be required to implement recommendations provided by the SPA team.

3.7.1.3.   Acceptance / Rejection of Deliverables: An acceptable client delivery should be 3 - 4 defects without any blocker, critical or major issues. If there are any known issues with the delivery, the vendor should prior inform to ICTA & the SPA team.

3.7.1.4.   Any deliverables may be rejected under the following scenarios, where there is/are;

    3.7.1.4.1.   One blocker issue

    3.7.1.4.2.   Two critical issues

    3.7.1.4.3.   One critical and 4 major issues

    3.7.1.4.4.   Eight major issues

3.7.2. User Acceptance Tests (UAT)

3.7.2.1.   A complete UAT document shall be supplied by the bidder including all positive and negative testing scenarios. The bidder shall also review and resubmit the UAT document including the comments and observations made by the employer.

3.7.2.2.   ICTA team will execute the UAT according to the test plan and end-user scenarios submitted by the bidder. UAT acceptance will be conducted by an internal committee in ICTA.

3.7.2.3.   All test scenarios related to the end-user functionality and technical features need to be included as part of the UAT test scripts, and the ICTA team may carry out additional testing if deemed necessary.

3.7.2.4.   Any issues arising from the UAT would need to be logged and fixed by the bidder and the affected components/parts/sub-systems will be re-tested by ICTA. Iterations of this cycle will be executed until all blockers, critical and major issues have been resolved

3.7.2.5.   Issue categorization (Eg: blocker, critical, major, minor) needs to be defined by the bidder along with ICTA as part of the UAT execution plan.

3.8. Training and Training Material

3.8.1. The bidder shall provide a training plan, considering different users, different functionalities, and the number of days, training approach, required language, etc.

3.8.2. Initial training for the Administrators (10) must be trained by the bidder on the solution administrative functions. This should be conducted onsite with comprehensive hands-on sessions and training materials. This training will be executed right after the solution implementation is completed and just before the live operations start.

3.8.3. Administrators, Organization end-user training, (separate videos and presentations for each user category) shall be prepared and provided by the bidder to be used by the ICTA for the end-user training sessions. Training material for Organization end-user should be in 3 languages (English, Sinhala, and Tamil).

3.8.4. The Bidder should provide both soft and hard copies of all user manuals (e.g. Printed documents). All manuals should be in tri-lingual (Sinhala, Tamil, and English).

3.8.5. FAQs with answers and user guides shall be published by the bidder to Administrators, organizational end-users.

3.8.6. Below mentioned training needs to be provided to the ICTA technical team
   ● Developer training for future change requests
   ● Developer training for change deployment to stage and production
   ● Training for disaster recovery
   ● Training for data backup and restore

3.9. Deployment and Implementation

3.9.1. The deployment guide needs to include the deployment architecture provided by the Bidder. Further, it must include configuration details, performance optimization details, and scale-up / down details, and strategy. The Bidder should provide end to end deployment guide including deployment environment setup and tool stack.

3.10.   Documentation Requirements

3.10.1. The Bidder shall provide all technical documents with adequate information in them mentioned in the compliance sheet. ICTA shall review the documents and may ask for revisions.

3.11.   Data Protection and Security Audit

3.11.1. The system should comply with the data protection act. Details of the act can be found at the below location, https://www.icta.lk/data-protection-legislation-overview/

3.11.2. SLCERT security audit should be performed and fix any vulnerabilities found before go-live

Refer following Annexes which form a part and parcel of the document.

Annex A- Overview of the Current HHIMS System

Annex B - High Level Functional Features

Annex C - Non-Functional Requirements

Annex D - Service Level Agreement for Support and Maintenance

Annex E- High-Level Architecture Diagram - Architectural requirements to be met by the solution

4. Phase-wise Implementation

The scope of work for the bidder spans the complete Software Development Life Cycle from designing, developing, testing, maintaining, and supporting. Bidder shall work closely with ICTA during the software implementation, maintenance, and enhancement phase to ensure successful implementation and operations of the solution.

Iteration I

'Iteration I' is planned to be released in T+ 3 Months (where T = month of signing of contract).

Iteration II

'Iteration II' is planned in T+5 months. The Iteration II shall consist of 'Iteration I' applications and rest of the feature

The table below provides a high-level break-up of the key features which shall be a part of Iteration I and II.

Bidder will evaluate further about the features during the requirement gathering stage and provide more viable approach for the implementation.

Outcome deliverables of Iterations

Iteration I outcomes	Iteration II outcomes
• Establish a cloud-based centralized database to synchronize patient and treatment data from the HHIMS implementations at Kaluthara RDHS.	• Data push and fetch between HHIMS, Open SRP and Cloud HIMS via HAPI FHIR central repository.
• Modify the Personal Health Number (PHN) to comply with National Digital Heath Guideline standards (V2.3)	• Upgrade Appointment and Queue management module of HHIMS.
• Upgrade the registration module to on board and search patients registered in Open SRP & Cloud HIMS SRP and other HHIMS instances.	• Upgrade functionalities for the pharmacy module to integrate and dispense drugs related to the diabetes clinics and to integrate with SWASTHA medical supply management system.
• Upgrade HHIMS to record and operate OPD, Clinic and Inward modules with multiple PHNs from Cloud HIMS, Open SRP and other HHIMS instances.	• Upgrade functionality of Laboratory module of HHIMS including scheduling of investigations and report generation.
• Develop a registration portal for the patients to record demographic details online for pre-registration with HHIMS.	• Upgrade HHIMS Reporting module.

• Develop and upgrade the HHIMS Clinic Module and the notification module for HHIMS as per the requirements from Diabetes compass program. - Record vital signs and point of care tests. - Record consultation notes and diagnosis. - Order drugs and investigations. - Record management plan. - Referral and back-referral management. - Notifications for the HHIMS users.	• Develop APIs to integrate HHIMS with HAPI FHIR server for the Diabetes compass program and SWASTHA. • Develop dashboards for Clinics, OPD and Inwards	
	• A responsive web application features covering the front-end UI of HHIMS.	

4.1 Implementation Schedule

The Bidder will be engaged for 18 months, in which 7 months for the designing, development, implementation, operational acceptance and 12 months for providing support and maintenance.

The Bidder is required to submit the following list of deliverables from this assignment.

4.1.1 Development:

No	Deliverables	Duration
1	Acceptance of the followings; 1. Detailed Project Management Plan 2. Master Test Plan and Performance Test Plan	Commencement Date + 2 weeks
2	Acceptance of the following; 1. Detailed Software Requirements Specification(DSRS) 2. Iteration plan (2 Iterations for deployable and workable solution) 3. Specifications for required hardware 4. Data migration and integration plan 5. Detailed software technical design (DSTD) 6. QA test plan 7. Acceptance criteria for the UAT 8. Prototype using a wireframe tool	Commencement Date + 5 weeks

3	Acceptance of the following; **Iteration I**
	
	    1. Test cases and Test scenarios
	    2. QA Release Notes
	    3. Proper maintenance of source code in GIT
	    4. Successful deployment of staging and production environments.
	    5. Test results
	    6. UAT test cases and successful UAT acceptance
	    7. User / Administration Manual
	    8. Deployment guide
	    9. Data migration
	    10. Production deployment confirmation report
	    11. Production launch Iteration I
		Commencement Date + 12 weeks

4	Acceptance of the following; **Iteration II**
	
	    1. Updated DSRS, and detailed Software Technical Design (DSTD)
	    2. Updated QA Release Notes
	    3. Updated Test cases and test scenarios
	    4. Updated Source code maintenance in GIT
	    5. Successful deployment of staging and production environments((All outcomes of the iteration II)
	    6. Updated Test results
	    7. Updated UAT test cases and successful UAT acceptance
	    8. Updated User / Administration Manual
	    9. Updated Deployment guide
	    10. Updated Production deployment confirmation report for 7 sites
	    11. Data Migration and Integration to other solutions
	    12. Help Desk document for the system
		Commencement Date +20 weeks

5	Acceptance of **Trainings**
	
	    1. User manuals, Training Materials should be given to the users to check against the functionality of the system
	    2. Completion of Training (Admin Training and User Training)
		Commencement Date + 24 weeks

6	Acceptance of the **Operational Acceptance Testing**;
	
	    1. Production launch of the Iteration II
	    2. Iteration II Operational Acceptance
		Commencement Date + 28 weeks

7	Successfully delivering of Maintenance and Software Support up to the acceptable level of ICTA	Operational Acceptance + 12 months

4.1.2 Change Request:

No.	Deliverables	Phase	Duration
1.	1.1. CR Proposal, including effort	Estimation	-
2.	2.1 Updated test plan for the iteration (Functional and Non-functional) 2.2 Updated detailed software technical design (DSTD)) 2.3 Updated test cases and test scenarios (functional and non-functional) 2.4 Proper maintenance of source code in ICTA GitHub 2.5 Updated developer and QA release notes 2.6 Successful deployment of staging and production environments 2.7 Updated test results (functional and non-functional) 2.8 Updated UAT test cases and successful UAT acceptance 2.9 Updated User/Administration manual 2.10 Deployment guide (if applicable) 2.11 Data Migration and Integration(If applicable) 2.12 Production deployment conformation report 2.13 User Training for assignments (if applicable)	Implementation	Agreed duration for the CR

5. Services and Facilities Provided by ICTA

5.1. HHIMS Latest Source code

5.2. Hosting facility (Lanka Government Cloud).

5.3. Web-based access to the ICTA GitHub and Nextcloud system

5.4. Access to Staging/ production environments (Lanka Government Cloud).

5.5. Arrange and facilitate meetings/trainings/ workshops (if required)

6. Review Committees and Review Procedures

The Software Development Bidder is required to work closely with the ICTA Digital Health team and Technology Team.

All versions of deliverables will be reviewed by the Technical Review Committee appointed by ICTA.

7. Minimum Qualifications of Key Professional Staff

The Bidder shall give the team of key professionals with the curriculum vitae and the team organization.

7.1. Development Team Key Professionals

#	Key Professional Staff & Assign Marks	Academic & Professional Qualifications (25%)	Work Experience in the domain Experience in the PROPOS ED ROLE (Yrs.) (25%)	Adequacy for the assignment) Specific Qualifications/ Requirements (50%)
a)	Project Manager	-Degree in ICT relevant field or Business Management	10	Enterprise Application, Experience -5 years of experience
b)	Technical Lead	- BSc in ICT/ Computer Science or equivalent	5	Enterprise Application Development with PHP related Framework - 5 years of experience
c)	Senior Software Engineer	- BSc in ICT/ Computer Science or equivalent	5	Enterprise Application Development with PHP related Framework - 3 years of experience
d)	UI/UX Engineer	-BSc in ICT/ Computer Science or equivalent	5	Enterprise Application Development, Wire framing, Prototyping- 3 years of experience
e)	Business Analyst	- BSc in ICT/Computer Science or equivalent	5	Experience in Enterprise applications, Government related projects, - 3 years of experience
f)	Quality Assurance Lead	-BSc in ICT/ Computer Science or equivalent	5	Enterprise Application Quality Assurance, Automated Testing - 3 years of experience
g)	Quality Assurance Engineer	-BSc in ICT/ Computer Science or equivalent	3	Enterprise Application Quality Assurance, Automated Testing- 2 years of experience

7.2. Support & Maintenance Team

#	Key Professional Staff & Assign Marks	Academic & Professional Qualifications (25%)	Work Experience in the domain Experience in the PROPOSED ROLE (Yrs.) (25%)	Adequacy for the assignment) Specific Qualifications/ Requirements (50%)
f)	Quality Assurance Lead	-BSc in ICT/ Computer Science or equivalent	5	Enterprise Application Quality Assurance, Automated Testing - 3 years of experience
g)	Quality Assurance Engineer	-BSc in ICT/ Computer Science or equivalent	3	Enterprise Application Quality Assurance, Automated Testing- 2 years of experience

Annex – A

Overview of the Current HHIMS System

Hospital Health Information Management System (HHIMS) is an element of health informatics that focuses mainly on the administrative and patient care needs of the hospitals. It is a comprehensive, integrated information system designed to manage all aspects of health information of a hospital's operation, such as medical, administrative and audit. It mainly consists of a patient data management module, a queue management module, a drug management module and a laboratory information system module etc. This system also facilitates the generation of various real time public health reports and statistics as requested by various parties. Main purpose of the system is to generate and maintain a free electronic Medical Record (EMR) for the citizens of Sri Lanka.

HHIMS is currently hosted on local servers located at each hospital and running as a standalone system and data sharing amongst the hospitals is difficult which a mandatory requirement in the future is.

Figure 1: System Overview

Technology used in HHIMS:

Technology Stack - PHP 5.6, MySQL 5.7 Framework Code Igniter 2
 LAMP Stack

HHIMS Existing Features:

Module	Modular description
Comprehensive Electronic Medical Record (EMR)	• All required medical/ clinical related information, such as presenting complain, Systemic review, past medical and surgical history, medical examinations, diagnoses, treatment and management, nursing notes, test results, and medication histories etc., necessary for clinical staff (consultants, doctors, nurses, and other health care providers) to carry out their clinical operations
Patient Registration	• This module manage all patient registration related activities.

	• Generating Patient Identification Number -PIN (temporary or permanent) as per the Hospital requirement, capturing demographic data, financial and insurance data will be managed by this module.
Out Patient Department Module	• The Out-patient module support the workflow of Out-patient department. • Out-patient department specific drugs management and examination templates to be created. • Ability to add Internal Referrals and External Referrals to clinics.
Clinic Module	• The Clinic module supports the requirements for different clinics. Main clinics which operate at hospitals are ENT, Dental, Orthopedic, Eye, Rheumatology, Endocrine, Medical, Pediatric, Surgical, Gynecology and Obstetrics, Dermatology and Cardiology. • Clinic specific drugs management and examination templates to be created. • Ability to record diagnosis, recording management plan, and Consultant, senior registrar and medical officer to manage clinical records. • Ability to add Internal Referrals and External Referrals to clinics. • Clinic specific requirements to be gathered at the time of creating the detailed requirements. • Include clinical diagrams to be integrated with HHIMS so Doctors can use those during diagnosis. • Ability to send the routine surgery list to the theatre module.
Inpatient management module	• All inpatient related activities pre-admission, admission, transfer, discharge activities managed by this module. It seamlessly integrate with patient administration, bed management, EHR, LIS, RIS.
Pharmacy Management	• The pharmacy management system manage the hospital pharmacy workflow from prescription reception, medication preparation, error checking to dispensing. • It has the capability to adopt separate workflow for OPD, IPD, OTC and controlled drugs.
Appointment management module	• This module manage all hospital related schedules/ appointments including doctor's appointment scheduling, consultants appointment scheduling.
Hospital order and stock management	• The Order and stock Management module address the order inquire, order requests of all clinical goods. This maintain the store, sub stores, ward stores and floor stores etc. The authorize users have capability to visualize transfer items seamlessly between the stores. • Orders can be placed form any ancillary department by any user in the hospital, depending on the authority level assigned to the employer.

Patient queue management module	• The queue management system manage patient queues in the OPD, Clinics and any patient gathering areas automatically. • At the registration (when a patient encounter is created) the patient will be issued a number which is generated automatically by the system indicating the consultation room to go, doctor and the queue number. • The display at the consultation room indicates the queue number which is being catered by the system when the patient encounter is created. • The LED or LCD screen in the patient's waiting areas will display the consultation rooms and queue numbers which are catering currently as a summery. • At the pharmacy, Laboratory, radiology etc. a patient token number is generated at the time, of the encounter creation and it will be displayed at the relevant counter.
Alerts and Notification / Dashboards	• This module integrates with all the other modules and have capability to generate notifications, alerts, and messages as per the pre-determined trigger points which will be decided by the hospital.
User Management Module	• The User Management module has functionalities to manage "user role" and authentication processes management required for the smooth uninterrupted function of HIMS.
RIS/PACS	• The Radiology Information System (RIS) and Picture Archiving and Communication System (PACS) has capability to manage hospital specific radiology workflow and report authorization process. • It integrates with all relevant modules to automate the RIS workflow. The RIS come with radiology modality request, scheduling capability.
Laboratory Information System	• This system manage and automate all laboratory activities and related workflows from patient registration to report issue. • The system facilitate report generation leading to improved clinical outcomes and increased efficiency. • The system have capability to integrate with all the lab instrument at the hospital. The system have capability to manage all satellite laboratories using a central location.
Integration, and interoperability	• Lab equipment integration (HL7, ASTM or equipment specific) • Integration with Radiology modalities (DICOM) • Medical database ICD-10, ICPC V2.0 • The system complies with HL7 latest version.
Reports Module	• The system reporting module to supports hospital specific reporting.
Internal Chat Module	• The internal chat module operates as an internal communicator to send inter ward communications. • Ability to send messages to users within the hospital When a message is sent via the chat module, it displayed as a pop up and remain visible until the recipient views the information and closes it.

Annex – B

High-Level Functional Features

Bidder should study the HHIMS business process and should carry out requirement study to identify new functionalities and features to be implemented in HHIMS in relation to Diabetes Compass Project. The below are the high-level functional features that provide understanding about the requirements.

Bidder should conduct end to end requirement gathering and come up with the Detailed Software Requirement Specification and obtain the approval from ICTA before implementing.

#	Component	Description	Task
1	Developments and Integrations	Design, development, and implementation of an extended and integrated version of HHMIS that features a diabetes and hypertension module.	a) Establish a cloud-based centralized database to synchronize patient and treatment data from the HHIMS implementations at Kaluthara RDHS.
			b) Modify the Personal Health Number (PHN) to comply with National Digital Heath Guideline standards (V2.3)
			c) Upgrade the registration module to on board and search patients registered in Open SRP & Cloud HIMS SRP and other HHIMS instances.
			d) Upgrade HHIMS to record and operate OPD, Clinic and Inward modules with multiple PHNs from Cloud HIMS, Open SRP and other HHIMS instances.
			e) Develop a registration portal for the patients to record demographic details online for pre-registration with HHIMS.
			f) Develop and upgrade the HHIMS Clinic Module and the notification module for HHIMS as per the requirements from Diabetes compass program. - Record vital signs and point of care tests. - Record consultation notes and diagnosis. - Order drugs and investigations. - Record management plan. - Referral and back-referral management. - Notifications for the HHIMS users. - Develop dashboards for Clincs, OPD and Inwards
			g) Data push and fetch between HHIMS, Open SRP and Cloud HIMS via HAPI FHIR central repository.
			h) Upgrade Appointment and Queue management module of HHIMS.
			i) Upgrade functionalities for the pharmacy module to integrate and dispense drugs related to the diabetes clinics and to integrate with SWASTHA medical supply management system.

			j)	Upgrade functionality of Laboratory module of HHIMS including scheduling of investigations and report generation.
			k)	Upgrade HHIMS Reporting module.
			l)	Develop APIs to integrate HHIMS with HAPI FHIR server for the Diabetes compass program and SWASTHA.
			j)	A responsive web application features covering the front-end UI of HHIMS.
2	HHIMS Deployment	HHIMS Deployment for selected Kaluthara district hospitals.		
3	Data Migration	HHIMS data migration for the upgraded version (Diabetes Compass Project).		

Annex – C

Non-Functional Requirements

1. SECURITY

1.1   The Bidder should provide what methodologies /standards are used for security testing and development.

1.2   The Bidder should provide information if any third-party assessments involved for security such as vulnerability testing of actual code and application

1.3   The Bidder should provide information if any automated tools are used for internal testing.

1.4   The Bidder should provide the patch strategy and use of any patch development tools

1.6   The proposed solution should be able to adhere to functionalities as per scope of work.

1.7   Audit logs recording user activities, exceptions and information security events must be generated and store for a defined period of time for future investigation and monitoring purpose.

1.8   The Bidder should provide their DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan) to the ICTA

1.10   The Bidder should adhere to the Data Protection Act when handling personal and organizational data.

1.12   The Bidder should provide documentation that explains the design for achieving each of the security requirements. The design should clearly specify whether the support comes from custom software, third party software, or the platform.

1.13   The Bidder should provide secure configuration guidelines that describe all security related configuration options and suggestions for the overall security of the software. The guideline shall include dependencies on the supporting platform, including the operating system, web server, and application server. The default configuration of the software shall be secure.

1.14   The Bidder should validate, and encoding each input to the application, whether from users, file systems, databases, directories, or external systems. The default rule

shall be that all input is invalid unless it matches a detailed specification of what is allowed. Specifically, the application shall not be susceptible to injection, overflow, tampering, or other corrupt input attacks.

1.15 The Bidder should state in what way authentication credentials and session identifiers would be protected all over their lifecycle. Requirements for all correlated functions, including forgotten passwords, changing passwords, remembering passwords, logout, and multiple logins, will be included.

1.16 The Bidder should disclose all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

1.17 The Bidder should use a source code control system that authenticates and logs the team member associated with all changes to the software model and all related configuration files and build files.

1.18 The Bidder will be responsible for verifying that all members of the software development team have been trained in secure programming methods.

1.19 User authentication and authorization

All applications should be able to access via ICTA's common infrastructure/application itself and independently via the respective department's website if required. Any authorization requirements should be implemented within the specific web application.

However, the solution should have the provision to integrate with the ICTA's proposed Identity Management solution in the future.

An administrative application needs to be developed wherever applicable.

Wherever applicable internal small applications need to be developed to capture and store relevant data.

1.21 Confidentiality and Integrity

All developed web applications should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message-level security standards. (i.e.: HTTPS, WS-Security) including point-to-point encryption (P2PE)

1.22 Authentication

The web application should be able to verify the users.

1.23 Authorization

The web application should be able to verify that allowed users have access to resources.

1.24 Non-repudiation

All Web applications should ensure non-repudiation by having standard audit trails and provisions to have WS-Security using digital signatures.

1.25 OWASP Guidelines

All web applications should ensure that the OWASP guidelines for security are followed when designing, developing, and deploying the web application.

1.26 Data Protection

- Develop an application in line with ith Personal Data protection Act
- Data should be encrypted according to the ISO Standards.

1.27 The Bidder should provide an SSL certificate and it should be an extended validated (EV) SSL certificate with a trusted brand.

2. AUDIT FACILITIES

Wherever applicable, an audit trail of all activities must be maintained. On service or operation being initiated, the system should log the event, creating a basic 'audit log entry. It should not be possible for the operation to be executed without the log entry being made.

The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are -

- Data Capture & Maintenance
- Creation of an entry/item
- Modification an item
- Deletion
- Control (or status change)
- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval

- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing some attributes may be considered mandatory, and they should not be turned off.

3. BACKUP AND CONTINGENCY PLANNING

The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff -

- Equipment failure
- Physical / natural Disaster
- Messaging or communication facilities.
- Changes in operations and policy
- Sudden absence of key personnel
- Breach in Security

Automatic Backups daily, weekly, *and* monthly should be taken. All the backup procedures and backups need to be tested regularly for restoration.

4. PERFORMANCE TESTING

Please find the below index as a guide to determine the benchmark values for the Application under the test.

Following the performance, criteria are provided as a guideline only. If the actual performance is falling below the stipulated figures, the Bidder is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the client. The bandwidth is assumed at 1mbps (shared) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 5 milliseconds
Screen Navigation: screen-to-screen	< 3 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 2 seconds
Screen grid – 25 rows, 10 columns	<3 seconds

Report preview – (all reports) – initial page view (if asynchronous)	< 40 seconds in most instances. It is understood that complicated/large volume reports may require a longer period
Simple inquiry – single table, 5 fields, 3 conditions – without screen rendering	< 4 seconds for 100,000 rows
Complex inquiry – multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 6 seconds for 100,000 rows
Server-side validations/computations	< 10 milliseconds
Client-side validations/computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept.) – max duration	4 hours

4.1 Performance Test Process Outputs

- Performance Test Scripts
- Performance Test Results

5. USABILITY

The web application should be extremely usable, even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user-friendly interface. The web application should be internationalized and localized if needed. The web application should be responsive where it should be viewable on any computing device.

6. INTEROPERABILITY

The web application should be able to view in standard compatible web browsers.

7. AVAILABILITY

The web application should be performed as follows,

- 99.99% available unless the web application is designed with expected downtime for activities such as database upgrades and backups.
- Hence to have high availability, the web application must have low downtime and low recovery time.

8. ROBUSTNESS

The web application should be able to handle error conditions gracefully, without failure. This includes tolerance of invalid data, software defects, and unexpected operating conditions.

- Failure Detection
    - Once deployed, there should be appropriate tools to discover anomalies and failures of the system
- Fault Tolerance
    - Web application developer should anticipate exceptional conditions and develop the system to cope with them. The web application must be able to use reversion to fall back to a safe mode, meaning, the application should continue its intended functions, possibly at a reduced level, rather than falling completely.

9. MAINTAINABILITY

The code of web application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements, or adaption.

10. COMPLIANCE TO STANDARDS

The code of web applications should be standardized by following web standards like W3C and ECMA – European Computer Manufacturers Association, to save time, augment the extensibility of the code, increase web traffic and improve the accessibly and load time of your application.

11. REUSABILITY

The web application should be able to use existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design and documentation.

12. API MANAGEMENT

13.1. API Standards and Best Practices

API standards and best practices should adhere in the code.

13.2 API Documentation
- Swagger documentation should be provided.

13.3. API Security

The web application should be used appropriate API security protocol mentioned below.
- Basic API authentication
    - Basic authentication should never be used without TLS (formally known as SSL) encryption as user name and password combination can be easily decoded otherwise.
- OAuth1.0a
    - Uses cryptographic signature value that combines the token secret, nonce, and other request based information. Can be safely used without SSL.
    - Recommend for sensitive data applications
- OAuth2
    - No need to use cryptographic algorithms to create, generate and validate signatures as all the encryption is handled by TLS.
    - Recommend for less sensitive data applications
- JWT (JSON Web Tokens)
- Keycloak security of FHIR server

13. SCALABILITY
The web application should be both scalable and resilient. A well-designed application should be able to scale seamlessly as demand increases and decreases. It should be resilient enough to withstand the loss of one or more hardware resources.

14. LEGAL AND LICENSING
The web application should comply with the national law.

15. EXTENSIBILITY
The web application should be designed and developed in a way that it can cater to future business needs.

16. TESTABILITY

The web application should be designed and developed in a way that testability is high, meaning, the ease of testing a piece of code or functionality, or a provision added in software so that test plans and scripts can be systematically executed. In simple terms, the software should be tested easily with the most famous 5 testing categories,

- Unit test
- Integration test
- System test
- Safety test
- Experience test

Refer Aden (2016)'s view on semantic testing for more information.

The web application should be working according to the given criteria in the latest version and 5 versions before in web browsers such as Mozilla Firefox, Google Chrome, Opera, and Apple Safari and the latest version and 2 versions before in Internet Explorer.

17. NOTES

- The Bidder can propose similar standards/requirements for the above-mentioned standards/requirements with the approval of the ICTA Technology Team.
- The design documents should be based on the 4+1 architecture model or the template provided by ICTA.
- Bidder should sign a non-disclosure agreement with respect to HHIMS source code and data provided by the ICTA.

Annex – D

Service Level Agreement for Support and Maintenance Services

(i) **Introduction**

The aim of this agreement is to provide a basis for close co-operation between the Client and the Bidder for support and maintenance services to be provided by the Bidder, thereby ensuring a timely and efficient support service is available. The objectives of this agreement are detailed in Section 1.1.

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

(ii) **Objectives of Service Level Agreements**

1. To create an environment conducive to a co-operative relationship between Client, Bidder and Client's representatives (government organizations) to ensure the effective support of all end users.
2. To document the responsibilities of all parties taking part in the Agreement.
3. To define the commencement of the agreement, its initial term and the provision for reviews.
4. To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
5. To institute a formal system of objective service level monitoring, ensuring that reviews of the agreement is based on factual data.
6. To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
7. To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.
8. The Bidder should adhere to the non-functional requirements that are stated in (Annex C) to maintain high availability and business continuity.
9. To design a business continuity plan with client in terms of disaster recovery, maintain system back-ups and related roles and responsibilities of both parties.

(iii) **Service Level Monitoring**

The success of Service Level Agreements (SLA) depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

Service factors must be meaningful, measurable and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both Client and Bidder. In the event of a discrepancy between actual and targeted service levels both Client

and Bidder are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Service level monitoring will be performed by Client. Reports will be produced as and when required and forwarded to the Bidder.

(iv) Principal Period of Support (PPS) Requirements

The Bidder must provide support and maintenance services during Support Levels mentioned below;

PPS category	Support hours		Applicability
PPS1	From	To	For the internal department administration system/ external integrations, API exposed to external departments.
	08:00 a.m.	06:00 p.m.	
	Monday to Friday (excluding Public Holidays)		
PPS2	From	To	Online services offered via portal/ external integrations related to smooth operation of the online services
	08:00 a.m.	10:00 p.m.	
	All days in the week (including Public and Mercantile Holidays)		

(v) On-Call Services Requirements

Bidder MUST make at least ONE qualified personnel available to the Client by telephone and email for the reporting and resolution of non-conformities or other issues, defects or problems. Dedicated telephone numbers and emails should be available for reporting issues. Client will nominate the personnel who are authorized to report non-conformities or other problems with the system from the departments. Reporting of non-conformities includes requests by the Client to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial telephone response times for the individual priority ratings. All times indicated represent telephone response time during specified Support Levels. The indicated telephone response time represents the maximum delay between a fault/request being reported and a Bidder's representative contacting the Client by telephone. The purpose of this telephone contact is to notify the Client of the receipt of the fault/request and provide the Client with details of the proposed action to be taken in respect of the particular fault/request.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
PPS1	10 minutes within Support Hours	20 minutes within Support Hours	20 minutes within Support Hours	45 minutes within Support Hours
PPS2	20 minutes within Support Hours	45 minutes within Support Hours	1 hour within Support Hours	2 hours within Support Hours

Table-1: Response Priority

Note:

Fatal   - Total system inoperability
Impaired   - Partial system inoperability
Business Critical   - Unable to perform core business functions
Non-Business Critical   - Able to perform limited core business functions

Bidder notification can occur outside Support Level time, and thus the response may occur after the next Support Level begins. Furthermore, "Time to Arrive On-Site (specified in above table) starts from Support Level starting time and "Time to Resolve the Problem" is Support Level time starting from the actual time of arrival on site.

(vi) Problem Resolution and Penalties

If faults are not corrected within the time limits specified in the Table-2, the Client shall be entitled to a penalty payment for each hour that the Bidder fails to resolve the fault.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
PPS1	1 Hour LKR 10,000.00 per hour	1.5 Hours LKR 7,500.00 per hour	1.5 Hours LKR 7,500.00 per hour	3 Hours LKR 5,000.00 per hour
PPS2	1.5 Hour LKR 7,500.00 per hour	3 Hours LKR 5,000.00 per hour	3 Hours LKR 5,000.00 per hour	4 Hours LKR 4,000.00 per hour

Table-2: Resolution Time and Penalties

"At the beginning of maintenance period Bidder and Client will mutually identify and agree on "Business Critical and Non-Business Critical" functionality/tools classification to apply SLA terms"

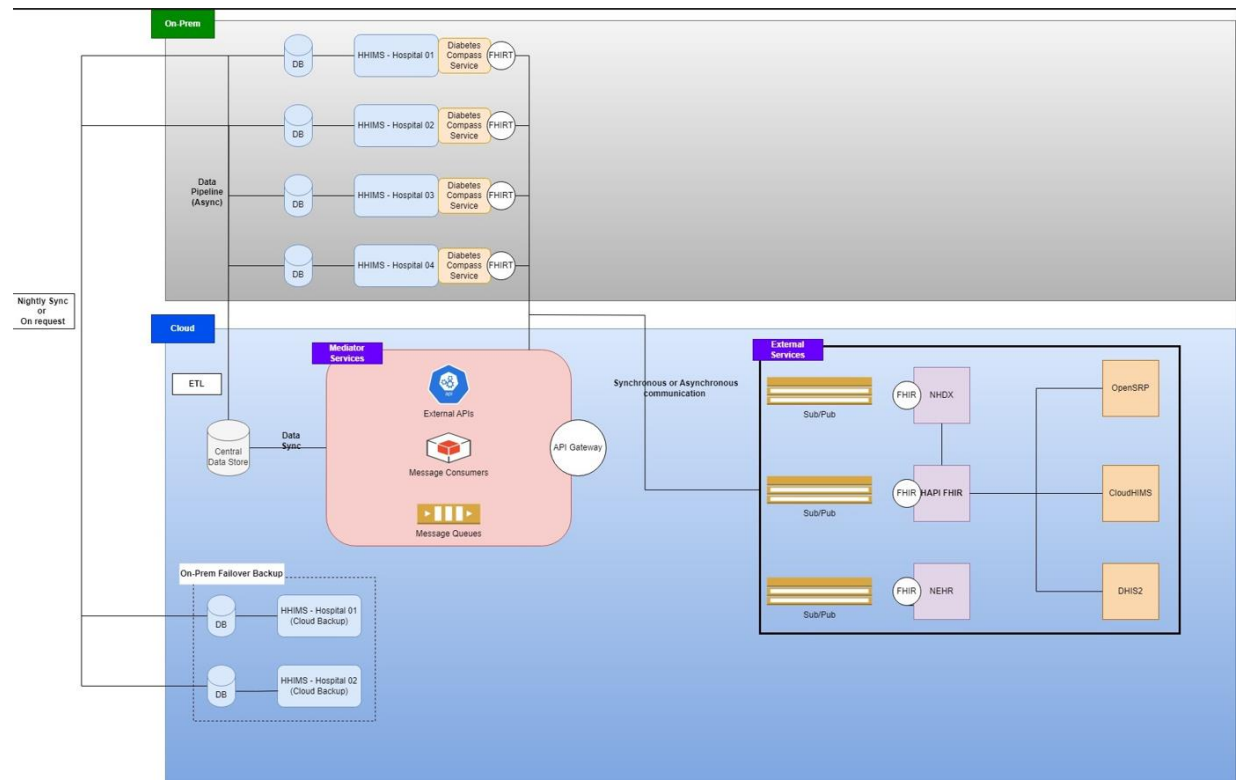# Annex – E

High Level Architecture - Architectural requirements to be met by the solution

Figure 2: High-Level Architecture Diagram