REQUEST FOR PROPOSAL (RFP)

For

Selection of a Service Provider for Design, Development, Implementation, along with End-to-End Operation, and Maintenance of the Dr. Nandamuri Taraka Rama Rao Vaidya Seva Trust (Dr. NTRVST) Application Suite

Sep 2026

RFP Reference No. – 1.1/APMSIDC/2026-27 Dated: 30/09/2026

Implementing Agency:

ANDHRA PRADESH MEDICAL SERVICES & INFRASTRUCTURE DEVELOPMENT CORPORATION

(Formerly APHMHIDC)

(AN ENTERPRISE OF GOVT. OF A.P.)

2nd Floor, Plot No:09, survey number: 49, IT Park, Mangalagiri,

Guntur District- 522503.

e-mail: aphmhidc@gmail.com & ed.apmsidc16@gmail.com

Ph. No: 8978644900

DISCLAIMER

This Request for Proposal (RFP) for the selection of a Service Provider for Design, Development, Implementation, Operation and Maintenance of the Dr Nandamuri Taraka Ramarao Vaidya Seva (Dr NTRVS) Application Suite for the State of Andhra Pradesh is issued by the Dr Nandamuri Taraka Ramarao Vaidya Seva Trust (hereinafter referred to as "TRUST" or "Dr. NTR VST").

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither the TRUST nor any of its officers, employees, advisers, or consultants accept any liability or responsibility for the accuracy, reasonableness, or completeness of the information contained in the RFP, or for any errors, omissions, or misstatements, negligent or otherwise.

The information contained in this RFP is selective and is subject to updating, expansion, revision, and amendment at the sole discretion of the TRUST. Each party must conduct its own analysis of the information contained in this RFP, correct any inaccuracies therein, and is advised to carry out its own investigation into the proposed project. The TRUST shall not be responsible for any direct or indirect loss or damage arising out of the use of any content of this RFP in any manner whatsoever.

The TRUST shall be the sole and final authority with respect to qualifying a Bidder through this RFP process. The decision of the TRUST in selecting the Service Provider shall be final, and the TRUST reserves the right to reject any or all bids without assigning any reason thereof. The TRUST further reserves the right to negotiate with the selected agency to enhance the value through this project.

The TRUST may terminate the RFP process at any time without assigning any reason, and upon such termination, the TRUST shall not be responsible for any direct or indirect loss or damage arising out of such termination.

TABLE OF CONTENTS

TABLE OF CONTENTS....3
ABBREVIATIONS....8
STRUCTURE OF THE RFP....12
1. About Dr Nandamuri Taraka Ramarao Vaidya Seva Trust....14
1.1 Background....14
1.2 Schemes Administered by the Trust....14
1.3 Current IT Infrastructure....14
2. OBJECTIVES OF THE RFP....16
2.1 Primary Objective....16
2.2 Specific Goals....16
3. BID PROCESS....18
3.1 RFP Issuing Authority....18
3.2 Data Sheet....18
3.3 Bid Submission Instructions....23
3.3.1 Bid Format....23
3.3.2 Technical Bid Contents....23
3.3.3 Financial Bid Contents (Online Only)....23
3.3.4 Validity of Bids....24
3.4 Pre-Bid Conference....24
3.5 Amendment to RFP....24
4. SCOPE OF WORK....25
4.1 Overview....25
4.2 Empanelment Module (Aligned with HEM 2.0)....25
4.2.1 Hospital Registration and Application....25
4.2.2 Empanelment Verification and Approval....26
4.2.3 Hospital Profile Management....26
4.2.4 De-empanelment and Suspension....26
4.2.5 Empanelment Reporting and MIS....27
4.2.6 NABH Accreditation....27
4.3 Transaction Management System (Aligned with TMS 2.0)....27
4.3.1 Beneficiary Registration....27
4.3.2 Pre-Authorization Process....27
4.3.3 Treatment and Discharge....29
4.3.4 Claims Processing....29
4.3.5 Follow-Up Medicine Cases and Chronic OP Treatments....30
4.3.6 Erroneous Claims Management....30
4.3.7 Emergency Registration and Admission....30
4.4 Health Benefit Packages (HBP 2022 Mapping)....30
4.5 Grievance Redressal Module....31
4.5.1 Grievance Registration....31
4.5.2 Grievance Processing....31
4.5.3 Grievance Reporting....31
4.6 Medical Audit Module (Aligned with SAFU)....32
4.6.1 Fraud Detection....32
4.6.2 Medical Audit Management....32
4.6.3 Hospital Audit....33
4.6.4 State Disciplinary Committee (SDC) Management....33
4.6.5 Reporting....33
4.6.6 Field Audit....33
4.6.7 State Disciplinary Committee (SDC) Management....34
4.7 User management Module....34

4.7.1 User and Role Management....34
4.7.2 Master Data Management....35
4.7.3 Configuration Management....35
4.8 Administration, Accounts and Financial Management....35
4.9 Medical Reimbursement Module....39
4.10 Health Camps Management....39
4.11 Field Operations Monitoring....39
4.11.1 Mithra Performance Management....39
4.11.2 Team Leader and District Coordinator Management....40
4.11.3 Field Operations Dashboard....40
4.12 Mobile Applications....40
4.12.1 Citizen Mobile Application....40
4.12.2 Staff Mobile Application....41
4.13 Unified Dashboards and MIS Reporting....42
4.13.1 Operational Dashboards....42
4.13.2 MIS Reports....42
4.13.3 Analytical System....42
4.13.4. Healthcare Analytics & Predictive Analytics....43
4.13.5 Data Sources:....43
4.14 Digital Health Compliance & Interoperability....44
4.14.1. Healthcare FHIR Conversion Engine....44
4.14.2. National Health Claims Exchange (NHCX) Integration....45
4.15 External Integrations....45
4.15.1 National Health Ecosystem Integrations....45
4.15.2 Identity and Authentication Integrations....46
4.15.3 State Government System Integrations....47
4.15.4 Financial Integrations....47
4.15.5 Communication Integrations....47
4.15.6 Geo-Fencing attendance Implementation....47
4.15.7 Enterprise Email System....48
Minimum Requirement for Mail Services....50
4.15.8 Text SMS Notifications....55
4.15.9 WhatsApp Messaging....56
4.16 Digital Sign implementation:....56
4.17 Operations & Maintenance (O&M) — Application and Infrastructure Services....58
4.17.1 Day-to-Day Operations and Application Management....58
4.17.2 Database Management and Administration....59
4.17.3 Patch Management, Security, and Software Upgrades....60
4.17.4 Application Maintenance and Support Services....60
4.17.5 User Management, Access Control, and Administrative Services....61
4.17.6 Functional Changes, Configuration, and Module Enhancements....62
4.17.7 Documentation, Version Control, and Compliance....62
4.17.8 Change Management System and Issue Tracking....63
4.17.9 IT Helpdesk Setup and Operations....63
4.17.10 Training and Capacity Building....63
4.17.11 Audit, Compliance, and Reporting....64
4.17.12 Design, Development, Testing, and Delivery of Requirements During the O&M Phase....64
5. TECHNICAL REQUIREMENTS....65
5.1 Technology Architecture....65
5.1.1 Microservices Architecture....65
5.1.2 Technology Stack....65
5.2 Security Requirements....66
5.2.1 Application Security....66
5.2.2 Data Security....66

5.2.3 Identity and Access Management....66
5.2.4 Audit and Compliance....67
5.2.5 Network Security....67
5.3 Healthcare Standards Compliance....67
5.4 Non-Functional Requirements....67
6. MULTI-SCHEME SUPPORT....69
6.1 Multi-Scheme Platform Requirements....69
7. MANPOWER REQUIREMENTS....71
7.1 Development Phase (6 Months)....71
7.2 O&M Phase (5 Years) - (Onsite at Trust Premises)....73
7.3 Personnel Replacement Policy....76
8. PROJECT TIMELINE AND DELIVERABLES....77
8.1 Overall Project Timeline - Development....77
8.2 Detailed Deliverables....79
8.2.1 Development Phase Deliverables....80
8.2.2 O&M Phase Deliverables....82
8.3 Deliverable Sign-off Process....82
8.4 System Acceptance and Certification....83
8.4.1 Core System Acceptance....83
8.4.2 In the release authorisation (....83
8.4.3 Full System Acceptance and Certification....83
9. ROLES AND RESPONSIBILITIES....84
9.1 Roles and Responsibilities of the Bidder (Service Provider)....84
9.1.1 Design & Development Responsibilities....84
9.1.2 O&M Responsibilities....85
9.1.3 Compliance Responsibilities....86
9.2 Roles and Responsibilities of Dr Nandamuri Taraka Ramarao Vaidya Seva Trust....86
9.3 Governance Structure....86
9.3.1 Project Core Group....86
9.3.2 Project Monitoring Committee (PMC)....86
9.3.3 IT Wing....87
9.3.4 Review Meetings....87
10. ELIGIBILITY CRITERIA....88
10.1 Pre-Qualification (PQ) Criteria....88
11. BID EVALUATION – QCBS METHOD....94
11.1 Evaluation of the Qualification Bid....94
Technical Evaluation:....95
Financial Evaluation:....96
Final Evaluation – QCBS 70:30....97
Tie in Combined Score:....97
12. SERVICE LEVEL AGREEMENT (SLA)....97
12.1 Application Availability and Quality SLA....98
12.2 Incident Resolution SLA (Application)....99
12.3 Requirement, Defect Fix and Enhancement SLA....100
12.4 Delivery Delay Penalties....100
12.5 Key Performance Indicators (KPIs)....101
12.6 Measurement, Exclusions and Cap....102
13. CONTRACT TERMS....102
13.1 General Conditions of Contract....102
13.1.1 Contract Duration....102
13.1.2 Contract Execution....103
13.1.3 Governing Law....103
13.1.4 Termination....103
13.2 Special Conditions of Contract....103
13.2.1 Confidentiality....103

13.2.2 Data Ownership....104
13.2.3 Intellectual Property Rights (IPR)....104
13.2.4 Continuous Service Obligation....104
13.2.5 Exit Management....104
14. FINANCIAL BID STRUCTURE....105
14.1 Financial Bid Components....105
14.2 Payment Schedule - Development Phase....105
14.3 Payment Schedule - O&M Phase....106
14.4 Notes on Financial Bid....106
15. DATA PROTECTION AND INTELLECTUAL PROPERTY RIGHTS....106
15.1 Data Protection Framework....106
15.2 Data Privacy Requirements....106
15.3 Intellectual Property Rights....107
16. ADDITIONAL OPERATIONAL REQUIREMENTS....108
16.1 Helpdesk Services....108
16.2 Training Requirements....108
16.3 Version Control and Code Management....108
17. AS-IS STUDY....109
17.1 AS-IS Assessment....109
17.2 To-Be Process Design....109
17.3 BPR Deliverables by the Trust....109
18. DATA MIGRATION....110
18.1 Scope of Data Migration....110
18.2 Data Migration Activities....110
18.3 Data Integrity Obligations....110
19. MONITORING AND PERFORMANCE REVIEW....111
19.1 Scope of Monitoring....111
19.2 Monitoring Activities of the Service Provider....111
19.3 Performance Review Meetings....111
20. EVENTS OF DEFAULT AND REMEDIES....112
20.1 Events of Default - Service Provider....112
20.2 Notice and Rectification....112
20.3 Penalty Cap....112
20.4 Force Majeure....112
21. Compliance to be maintained....113
21.1 Compliance....113
21.2 Vulnerability Management....113
ANNEXURES....114
Annexure 1: Current Application Architecture (Overview)....114
Annexure 2: Current Database Statistics....115
Annexure 3: Schemes - User Base and Module Coverage....116
Annexure 4: Indicative Workflow Reference Points – (Attachment-1)....117
Annexure 5: Compliance and Standards Reference....118
Annexure 6: Bid Submission Checklist....119
Model Form of Contract Agreement....120
Bid Security (EMD) form....123
Forms....124
Form P#1: Application Form....124
Form P#2: Declaration regarding Clean Track Record....126
Form P#3: Financial Strength Details....127
Form P#4: Details of Local Presence....129
Form P#5: Relevant Project Experience....130
Form P#6: Conflict of Interest....131
Form P#7: Declaration as per GO.Ms.12 Dated 08.05.2015 of ITE&C (Infra) Dept., GoAP. 132
Form T#1 - Understanding of the Project....133

Commercial Forms..... 137
Form C#1- Commercial Proposal Submission Form..... 137
Form C#2- Commercial Form..... 138

ABBREVIATIONS

Abbreviation	Expansion
ABDM	Ayushman Bharat Digital Mission
ABHA	Ayushman Bharat Health Account
AB-PMJAY	Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana
AI	Artificial Intelligence
API	Application Programming Interface
CEO	Chief Executive Officer
CERT-In	Indian Computer Emergency Response Team
CFMS	Comprehensive Financial Management System
CI/CD	Continuous Integration and Continuous Deployment
CSP	Cloud Service Provider
DAMA	Discharge Against Medical Advice
DRG	Diagnosis Related Groups
Dr NTR VST	Dr Nandamuri Taraka Ramarao Vaidya Seva Trust
Dr NTRVS	Dr Nandamuri Taraka Ramarao Vaidya Seva Scheme
HER	Electronic Health Records
EHS	Employees Health Scheme
EMD	Earnest Money Deposit
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation

Abbreviation	Expansion
GIGW	Guidelines for Indian Government Websites
GoAP	Government of Andhra Pradesh
GoI	Government of India
HBP	Health Benefit Package
HEM	Hospital Empanelment Module
HFR	Health Facility Registry
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven International
HPR	Health Professional Registry
HRMS	Human Resource Management System
ICD	International Classification of Diseases
IT	Information Technology
ISMS	Information Security Management System
LAMA	Leave Against Medical Advice
LGD	Local Government Directory
LOINC	Logical Observation Identifiers Names and Codes
MeiTY	Ministry of Electronics and Information Technology
MEDCO	Medical Coordinator

Abbreviation	Expansion
MIS	Management Information System
NHCX	National Health Claim Exchange
NHA	National Health Authority
OTP	One Time Password
PBG	Performance Bank Guarantee
Vaidya Mithra	Pradhan Mantri Arogya Mitra
QCBS	Quality and Cost Based Selection
RTGS	Real Time Gross Settlement
SAFU	Special Anti-Fraud Unit
SDK	Software Development Kit
SHA	State Health Agency
SLA	Service Level Agreement
SMS	Short Message Service
SNOMED-CT	Systematized Nomenclature of Medicine - Clinical Terms
SRS	Software Requirements Specification
TMS	Transaction Management System
TRUST	Dr Nandamuri Taraka Ramarao Vaidya Seva Trust
UAT	User Acceptance Testing
UIDAI	Unique Identification Authority of India

Abbreviation	Expansion
UHC	Universal Health Coverage
VAPT	Vulnerability Assessment and Penetration Testing
WJHS	Working Journalists Health Scheme

STRUCTURE OF THE RFP

This RFP document is organized as follows:

Section	Title	Description
1.	About the Dr Nandamuri Taraka Ramarao Vaidya Seva Trust	Background, schemes, and current IT landscape
2.	Objectives	Primary and specific goals of the project
3.	Bid Process	Timeline, instructions, and key dates
4.	Scope of Work	Detailed functional and technical scope
5.	Technical Requirements	Architecture, security, and compliance
6.	Multi-Scheme Support	Configurable scheme platform requirements
7.	Manpower Requirements	Team structure for development and O&M phases
8.	Project Timeline and Deliverables	Milestones and expected deliverables
9.	Roles and Responsibilities	Bidder and Trust responsibilities
10.	Eligibility Criteria (PQ and TQ)	Pre-qualification and technical qualification
11.	Bid Evaluation	Evaluation methodology
12.	SLA	Service levels, KPIs, and penalty structure
13.	Contract Terms	General and special conditions
14.	Financial Bid Structure	Cost components and payment schedule
15.	Data Protection and Intellectual Property Rights	Data security, confidentiality, and ownership
16.	Additional Operational Requirements	Other Requirements falls under the scope of the bidder
17.	As-Is Study	Study of Legacy system, BPR for enhanced solution
18.	Data Migration	Complete migration of data from the legacy system to the new application

19.	Monitoring and Performance Review	Supervision of the activities of the bidder
20.	Events of Default And Remedies	Guidelines in case of default from Service Provider
21.	Compliance to be Maintained	Technical Compliance to be maintained during contract
22.	Annexures	Supporting Documents
23.	Model Form of Contract Agreement	Model Contract Agreement with SP
24.	Bid Security (EMD) Form	Bid Security Form
25.	Forms	Forms required to submit proving eligibility
26.	Commercial Form	Commercial forms

1. About Dr Nandamuri Taraka Ramarao Vaidya Seva Trust

1.1 Background

The Dr Nandamuri Taraka Ramarao Vaidya Seva Trust (Dr NTR VST) was established by the Government of Andhra Pradesh in February 2007 to function as the focal agency at the State level for implementing cashless health insurance schemes for the citizens of Andhra Pradesh. The Trust is mandated to provide Universal Health Coverage (UHC) and ensure equity of access to quality healthcare for economically and socially vulnerable sections of society.

The flagship scheme under the Trust, is now operated as Dr Nandamuri Taraka Ramarao Vaidya Seva, providing end-to-end cashless treatment coverage up to ₹25,00,000 per family per annum for secondary and tertiary care procedures. The scheme operates on a Unique Public-Private Partnership (PPP) model involving a network of empanelled government and private hospitals across the State.

1.2 Schemes Administered by the Trust

The Dr Nandamuri Taraka Ramarao Vaidya Seva Trust currently administers the following healthcare schemes:

- Dr Nandamuri Taraka Ramarao Vaidya Seva Scheme - Cashless treatment for BPL and eligible citizens of Andhra Pradesh with coverage up to ₹25,00,000 per family per annum.
- Employees Health Scheme (EHS) - Cashless treatment for State Government serving and retired employees along with their eligible family members.
- Working Journalists Health Scheme (WJHS) - Cashless treatment for accredited journalists along with their eligible family members.
- Aarogya Raksha Scheme - Provides health Care benefits coverage to Above Poverty Line (APL) families on a subscription basis, with coverage of ₹2.5 lakh per person per year.
- Medical Reimbursement for Employees and Pensioners - Reimbursement of medical expenses incurred by State Government employees and pensioners at empanelled and non-empanelled hospitals.

1.3 Current IT Infrastructure

The existing IT application suite of the Trust has been in operation since 2007 and is built on legacy technology comprising Java Server Pages (JSP) front-end, JBoss application server, Oracle database, and a Flutter-based mobile application. The current system has approximately 5 TB of across 5,000+ database tables and approximately 300 TB of unstructured (document) data, with an annual incremental growth of approximately 80 TB. The concurrent user base includes approximately 1,50,000 users for Dr Nandamuri Taraka Ramarao Vaidya Seva, 1,00,000 for EHS, and 20,000 each for WJHS, Additionally, the system includes a NIC based mail service provisioned for all Trust users. The overall storage footprint of the mail server for all the 5000+ users (Approx) is estimated to be approximately 5–10 TB.

The legacy architecture presents significant challenges:

(a) It does not support the latest National Health Authority (NHA) guidelines and AB-PMJAY ecosystem components such as HEM 2.0, TMS 2.0, HBP 2022, SAFU, and Grievance Modules.

(b) It lacks compliance with Ayushman Bharat Digital Mission (ABDM) milestones M1, M2, M3 and M4.

(c) It is unable to accommodate modern AI/ML-based fraud detection and report digitization capabilities:

(d) the Monolithic Architecture makes enhancements and integrations increasingly difficult.

Accordingly, the Trust has decided to undertake a complete Re-design and Re-development of the application suite on Modern, Scalable, Microservices-based Architecture.

2. OBJECTIVES OF THE RFP

2.1 Primary Objective

The primary objective of this Request for Proposal is to select a competent and experienced Service Provider for Design, Development, Implementation, AI-Enabled Features, Operation, and End-to-End Maintenance of the Dr. Nandamuri Taraka Rama Rao Vaidya Seva Trust (Dr. NTRVST) Application Suite - a modern, scalable, secure, AI-enabled, microservices-based healthcare IT platform to:

- Replace the legacy application with a state-of-the-art technology platform built on open-source, microservices-based architecture.
- Provide end-to-end cashless healthcare services up to ₹25,00,000 for the eligible citizens of Andhra Pradesh across all applicable schemes.
- Achieve full compliance with ABDM (Milestones M1, M2, M3 & M4.)
- Design and development should be In-lines with AB-PMJAY ecosystem components (HEM 2.0, TMS 2.0, HBP 2022, SAFU, Grievance Modules), GIGW guidelines, and CERT-In security standards.
- All the above said components should be updated on continuous basis based on the versions released by the NHA.
- Dynamic workflow management module should be built wherein all the workflows and processes within the application suite can be reconfigured and modified by trust officials with required business conditions and necessary restriction of options in the logins.
- Enable 24x7 high-availability operations with scalability to accommodate 50,000+ concurrent enterprise users and 10 lakh+ concurrent mobile users.
- Integrate seamlessly with national systems including ABDM, PMJAY, NHM, UIDAI, NHCX, payment gateways, RTGS, CFMS, SGSW, Banking's and State Health Department systems.

2.2 Specific Goals

In addition to the primary objective, the new application suite shall achieve the following specific goals:

- Digitize and standardize all clinical and operational workflows in alignment with GOI-mandated healthcare standards (ICD-10/11, SNOMED-CT, LOINC, LGD, FHIR R4).
- Provide unified dashboards, actionable MIS reports, and a configurable analytical ecosystem for decision-makers at all levels.
- Enable citizen centric mobile applications with AI features for health record access, hospital discovery, grievance submission, and real-time hospitalization feedback to improve the transparency.
- Deploy role-based access control, geo fencing, and robust audit trails to minimize fraud and ensure accountability.

- Support multiple healthcare schemes on a single platform with configurable workflows, benefit packages, rates, and payment integration per scheme.
- Ensure data sovereignty and confidentiality with IPR rights vested with the Trust.

3. BID PROCESS

3.1 RFP Issuing Authority

Issuing Authority	Chief Executive Officer, Dr Nandamuri Taraka Rama Rao Vaidya Seva Trust
Address	Dr Nandamuri Taraka Rama Rao Vaidya Seva Trust, Door No. 241, MGM Capital Building, Chinnakakani, Mangalagiri, Guntur District, Andhra Pradesh - 522503
Contact Email	ceoap@ntrvs.ap.gov.in addlceo@ntrvs.ap.gov.in
Contact Phone	9281074744
Website	https://drntrvaidyaseva.ap.gov.in/

3.2 Data Sheet

S. No	Information	Details
1.	Publishing of RFP through eProcurement Portal of GoAP	From 30.09.2026 to 14.10.2026
2.	RFP reference No. & Date	1.1/APMSIDC/2026-27 Dated: 30.09.2026
3.	Prebid meeting-1	05.10.2026 11:00 AM O/o APMSIDC, Mangalagiri, Guntur
4.	Prebid meeting- 2	10.10.2026 11:00 AM O/o APMSIDC, Mangalagiri, Guntur
5.	Last Date and Time of submission of Online bid on eProcurement Portal.	14.10.2026, 03: 00 PM
7.	Bid opening date on eProcurement platform	14.10.2026, 03:01 PM
8.	Bid document fee (Non-Refundable)	Rs. 59,000/-
9.	Bid Validity Period	30 days
10.	Earnest Money Deposit (EMD/ Bid Security)	Rs. 12.50 Lakhs ● The Bidder should submit valid EMD in the form of Bank Guarantee (BG) specific to this

		tender in favour of “Managing Director, Andhra Pradesh Medical Services & Infrastructure Development Corporation (APMSIDC), Government of Andhra Pradesh. ● The scanned copy of BG should be uploaded on AP eProcurement portal. The Original Copy of BG should be submitted to APMSIDC on or before the bid closing date & time. ● Rotational BG is not acceptable. Bidders can also pay EMD through an online payment method. Online payment can be made via NEFT/ Credit/ Debit Card at https://tender.apeprocurement.gov.in
11.	EMD validity Period up to	● 45 days + bid validity.
12.	Contract Period	6 (*Six*) months for Design, Development & Go Live and Operations and Maintenance for the period of 5 (*Five*) Years from the date of Go live as per the milestones. The contract can be extended for a further period of 2 (*Two*) Years on sole discretion of the Trust on same payment, terms and conditions of this RFP.
13.	Implementation cum Performance Bank Guarantee (PBG) Value & Validity Period	1. PBG value: 5% of the total value of the contract in favour of “Chief Executive Officer, Dr NTR Vaidya Seva Trust” from any Nationalized/ Scheduled Bank. 2. PBG validity: 60 days beyond contract period 3. Submission of PBG: Within 10 days from the date of receipt of Notification of Award 4. The EMD of the successful bidder will be returned on submission of PBG.

14.	Contract Signing	Within 7 days from the date of receipt of Notification of Award (NoA).
15.	Bid submission Online	Bidders are requested to submit the bids after issue of minutes of the pre-bid meeting duly considering the changes made if any, during the pre-bid meeting. Bidders are totally responsible for incorporating/complying the changes/amendments issued if any during pre-bid meeting in their bid.
15.	Procedure for Bid Submission	Bids shall be submitted online on https://tender.apeprocurement.gov.in/ platform 1. The participating bidders in the tender should register themselves free of cost on eProcurement platform on the website https://tender.apeprocurement.gov.in/ 2. Bidders can log-in to the eProcurement platform in Secure mode only by signing with the Digital certificates. 3. The bidders who are desirous of participating in eProcurement shall submit their pre-qualification bids, technical bids, financial bids as per the standard formats available at the eProcurement portal. 4. The bidders should scan and upload the respective documents in Pre-Qualification and Technical bid documentation as detailed in the RFP including EMD. The bidders shall sign & affix stamps on all the statements, documents, certificates uploaded by them, owning responsibility for their correctness/authenticity. 5. The rates should be quoted online only

17.	Other conditions	1. After uploading the documents, the copies of the uploaded statements, certificates, documents, original Demand Drafts in respect of Bid Security (except the Price bid/offer/break-up of taxes) are to be submitted by the bidder to the O/o The Managing Director, APMSIDC as and when required. Failure to furnish any of the uploaded documents, certificates, will entitle in rejection of the bid. The APMSIDC shall not hold any risk on account of postal delay. Similarly, if any of the certificates, documents, etc., furnished by the Bidder are found to be false / fabricated / bogus, the bidder will be disqualified, blacklisted, action will be initiated as deemed fit and the Bid Security will be forfeited. 2. APMSIDC will not hold any risk and responsibility regulating non-visibility of the scanned and uploaded documents. 3. The Documents that are uploaded online on eProcurement portal will only be considered for Bid Evaluation. 4. Department users: (i) In the endeavour to bring total automation of processes in eProcurement, the Govt. has issued orders vide G.O.Ms.No. 13 dated 05.07.2006 permitting integration of electronic Payment Gateway of ICICI/HDFC/Axis Banks with eProcurement platform, which provides a facility to participating suppliers / contractors to electronically pay the transaction fee online using their credit

		cards.
18.	Last date/time for receipt of queries from bidders by mail (second pre-bid)	09.10.2026, 03:00 pm
19.	Release of response to pre-bid queries	Will be uploaded in Ap e-procurement
20.	Last date, time (deadline) for submission of bids in response to RFP notice	14.10.2026, 3:00 pm
21.	Date, and time of opening of Pre-Qualification bids received in response to the RFP notice	14.10.2026, 3:01 pm
22.	Penalties	As per RFP
23.	Payment Terms	As per RFP
24.	Conditional and Late bids	Not acceptable and liable for rejection
25.	Date, and time of opening of technical bids received in response to the RFP notice	To be informed to the eligible bidders
25.	Time and Date Technical Presentations by the bidders	To be informed to the eligible bidders
27.	Place, time and date of opening of Financial Proposals received in response to the RFP notice	To be informed to the eligible bidders
28.	Technical Evaluation	QCBS 70:30 Minimum Technical Pass Score of 70 Marks
29	Final Evaluation	Quality-and-Cost Based Selection (QCBS) methodology, wherein the Technical Score and Financial Score shall be assigned the weightages specified in the Tender
30	Contact details of Tender Inviting Authority	Designation: Managing Director, APMSIDC Address: 2nd Floor, PHYCARE Building, Plot No. 9, APIIC IT Park, Survey No. 49, Near Visalandra Printing Press, Autonagar,

		Mangalagiri, Andhra Pradesh - 522503 E-mail id: aphmhidc@gmail.com E-mail Id: ed.apmsidc16@gmail.com Contact No: +91-9121053550
31	Address for all Bid Process Management related activities	The Managing Director, APMSIDC

If your firm is interested in participation, please visit the web site at https://tender.apeprocurement.gov.in. The processing fee is payable only when you indent full copy of the bid document and for participation in tender.

3.3 Bid Submission Instructions

3.3.1 Bid Format

All bids shall be submitted (a) Technical Bid (online & offline) and (b) Financial Bid (online only) as detailed below. Technical bid shall be placed in a single outer sealed envelope super scribed with the RFP reference number and the bidder's name.

3.3.2 Technical Bid Contents

- Covering letter on company letter head duly signed by authorized signatory.
- Bidder profile and company registration documents.
- Evidence of compliance with Pre-Qualification (PQ) criteria.
- Technical proposal addressing all requirements specified in this RFP.
- Proposed technical architecture, solution design, and technology stack.
- Project implementation methodology, duration, and milestones aligned as specified in the RFP.
- Team structure, CVs of all personnel, and resource deployment plan.
- Evidence of compliance with Technical Qualification (TQ) criteria.
- Past project experience certificates and client references.
- Compliance matrix against all functional and technical requirements.

3.3.3 Financial Bid Contents (Online Only)

- Financial bid in the prescribed format (Volume II - Financial Bid).
- Component-wise cost breakup: Development Cost, O&M Cost (Year-wise), Migration Cost, License Costs (if any), and Optional Costs.
- All costs in Indian Rupees (INR), inclusive of applicable taxes.

3.3.4 Validity of Bids

All bids shall remain valid for a period of **30** days from the last date of bid submission. The TIA reserves the right to seek an extension of bid validity, and bidders shall not be entitled to withdraw their bids during this period.

3.4 Pre-Bid Conference

A pre-bid conference shall be organized at the designated venue on the date specified in Section 3.2. Prospective bidders are encouraged to participate to seek clarifications. All queries shall be submitted in writing to the designated email address prior to the pre-bid conference. Responses to all queries shall be published on the e-Procurement website and shall form part of this RFP.

3.5 Amendment to RFP

At any time prior to the deadline for submission of bids, the TRUST may amend the RFP by issuing an addendum. Any addendum shall be published on the e-Procurement website and shall be binding on all bidders. Bidders are requested to regularly check the e-Procurement website for any amendments.

4. SCOPE OF WORK

4.1 Overview

The scope of work encompasses the complete lifecycle of the Dr. NTRVST Application Suite including design, development, testing, deployment, integration, data migration, training, and long-term operation and maintenance. The application suite shall replace the existing legacy system and shall be built as a modern, cloud-native, microservices-based platform aligned with national healthcare IT standards and the AB-PMJAY, ABDM ecosystem.

The scope is divided into the following major phases:

- M1, T1 (Month 1): Project kick-off, AS-IS study, BPR, solution architecture, requirement gathering and SRS approval.
- M2, T2 (Months 2–3): Development, deployment and go-live of the core modules (TMS, Empanelment, HBP).
- M3, T3 (Month 4): Development and incremental go-live of the ancillary modules.
- M4, T4 (Month 5): Mobile apps and external integrations on the live system, with SIT, UAT and VAPT.
- Final Sign-off, T5 (Month 6): UAT closure, CERT-In audit, performance testing, data migration completion and full go-live.
- O&M: 5 years from completion of Final sign-off, extendable by 2 years.

The scope of work is indicative but not exhaustive. The Service Provider shall deliver all the requirements within a stipulated time lines provided by the Trust.

4.2 Empanelment Module (Aligned with HEM 2.0)

The Empanelment Module shall manage the complete lifecycle of hospital empanelment with Dr NTR VST, from initial application through verification, approval, ongoing compliance monitoring, and de-empanelment. The module shall be aligned with the ABPMJAY Hospital Empanelment Module (HEM) 2.0 framework.

4.2.1 Hospital Registration and Application

- Online application portal for hospitals to submit empanelment applications with supporting documents for Different schemes implemented by the Trust as per the mandatory guidelines.
- Integration with Health Facility Registry (HFR) for verification and standardized hospital identification.
- Integration with Health Professional Registry (HPR) for doctor and specialist credential verification.

- Document management for all empanelment-related documents with automated verification workflows.
- Support for Government (deemed empanelled) and private healthcare providers (both for-profit and not-for-profit).
- Specialty-wise and procedure-wise empanelment with infrastructure and manpower requirement validation as per the empanelment guidelines.

4.2.2 Empanelment Verification and Approval

- Field verification workflow with online checklist for infrastructure, manpower, equipment, and IT readiness.
- The System should support and guide the users in the work flow by analysing the documents uploaded whether they are real / fabricated for the purpose.
- The system should allow the video inspection uploads and should guide the Empanelment committee on the suggested lapses and indicate the remarks by analyzing the video.
- Multi-level approval workflow: District level/State level (SHA), and final approval.
- Provider Service Agreement (MoU) generation, digital signing, and management.
- Tripartite agreement management among the Hospital, Trust, and Implementation Support Agency.
- Designation of hospitals for tertiary care packages based on capacity assessment.

4.2.3 Hospital Profile Management

- Comprehensive hospital profile with specialties, procedures, bed capacity, equipment, and contact details.
- Integration with LGD codes for location standardization.
- Geo-tagging and mapping of hospital locations.
- Annual renewal workflow with document re-submission and re-verification with due alerts to the hospitals as well as the district authorities if not uploaded with in time.
- Hospital performance score card accessible to field staff and Trust officials and citizens if required.

4.2.4 De-empanelment and Suspension

- Trigger-based de-empanelment workflow with escalation to Trust for final decision.
- Suspension management with controlled access during the investigation period.
- Due process management ensuring Principles of Natural Justice are followed.
- Claims pending settlement management during de-empanelment proceedings.
- Any other actions which are in use or any other disciplinary action as decided by the Trust should be enabled and made it functional whenever required.

4.2.5 Empanelment Reporting and MIS

- District-wise, specialty-wise, category-wise empanelled hospital reports.
- Renewal status tracking and due renewal alert notifications.
- Hospital audit compliance tracker integrated with the Medical Audit module.

4.2.6 NABH Accreditation

- Should integrate with the NABH to obtain the NABH accredited hospitals list along with details such as NABH Accredited No., FROM and TO date, specialties empanelled for etc.,
- Online application to the hospitals for submission of NABH certificates duly entering their particulars like specialties for which NABH was accredited and the same may be verified against the NABH available data on real time.

4.3 Transaction Management System (Aligned with TMS 2.0)

The Transaction Management System (TMS) module shall manage the complete patient care lifecycle from registration through discharge and final claim settlement. It shall be developed in alignment with the AB-PMJAY TMS 2.0 framework. The system shall integrate with the National Health Claim Exchange (NHCX) for routing claims between providers and payers.

4.3.1 Beneficiary Registration

- Beneficiary identification and verification using Dr NTRVS card/Ayushman ID, ABHA number, or Aadhaar, AB PMJAY, EHS, WJHS, Aarogya Raksha, Amrutha health scheme, Amaravathi Residents card number, etc.
- Aadhaar-based biometric authentication: fingerprint, IRIS, face authentication, or OTP.
- Exception process for non-Aadhaar authentication with Medical Superintendent (MS)/MEDCO/DC approval with due approval flow.
- New-born baby registration linked to mother's beneficiary record.
- Registration cancellation workflow with reason capture.
- Patient status classification: Inpatient (IPD) and Outpatient (OPD).
- Patient attendant details capture with consent documentation.
- Communication address capture and verification against scheme eligibility.
- Wallet balance display and benefit utilization tracking at registration stage.
- Referral from one Empanelled hospital to other and maintain the history of events hospital wise till discharge along with reason for referring with the consent of the patient.

4.3.2 Pre-Authorization Process

- Pre-authorization initiation by MEDCO/Vaidya Mithra upon patient registration and initial evaluation.

- Medical information capture: general findings, personal history, family history.
- Admission information: authentication consent, admission date, type (planned/emergency), FIR details for medico-legal cases.
- Diagnosis entry with ICD-10/ICD-11 coded diagnosis, aligned with SNOMED-CT terminology.
- Treatment plan: specialty selection, procedure selection from HBP 2022 mapped packages, stratification, ICHI codes, number of days/units.
- Support for single procedure, multiple procedure (with multiple procedure pricing guidelines: 1st highest at 100%, 2nd at 50%, 3rd and subsequent at 25%) or any other policies as defined by the Trust, procedures with stratification, procedures with implants, cyclic procedures, and Standard Treatment Guideline (STG)-based procedures as defined by the Trust.
- Investigation document upload and care team details (treating doctor with HPR registration).
- Across the entire application wherever image capture or upload functionality is required shall contain predefined embedded data such as Geo coordinates, date time stamp etc.
- eRUPI voucher generation for eligible cashless diagnostic tests at outside labs.
- Finance section: package amount, stratification cost, incentive calculation, and total payable amount display.
- Pre-authorization submission from the Hospital with due authorization of the MEDCO of the Hospital through Aadhaar based authentication or Digital sign based along with SSO authentication process for login.
- Verification work flow with Executive verification of all mandatory documents social/ Medical
- Preauthorization Processing Doctors – Pre-auth Panel Doctors (PPD - Specialists) --> Preauthorization Trust Doctors at the Trust end.
- The flow should be flexible in such a way that the procedure/specialty wise fixed flows can be implemented on a go.
- Auto-approval for designated auto-approved procedures as defined by the Trust.
- PPD/PTD workflow: Approve, Query, or Reject with documented reasons.
- *Pre-authorization resubmission*: modify existing procedures or add new procedures with reasons for resubmission.
- *Pre-authorization enhancement*: add new procedures or change stratification/duration for existing procedures (enhancement documents mandatory).
- Pre-authorization cancellation workflow with reason documentation.
- Patient Liability case management (where patient bears additional cost).
- Hybrid case management (where cost is shared between Trust and Insurance).

- DRG (Diagnosis Related Groups) form capture: drug details, diagnostic details, implant details, and consumables for drug utilization analysis.

4.3.3 Treatment and Discharge

- Under-treatment monitoring dashboard for Vaidya Mithra/MEDCO and Trust staff.
- Daily update provision for patient condition and treatment progress.
- Discharge types: Normal Discharge, LAMA (Leave Against Medical Advice), DAMA (Discharge Against Medical Advice), Death.
- Normal discharge: discharge stage, surgery date, discharge date, post-surgery photo with Vaidya Mithra/doctor, discharge summary, feedback form, and Post-Op medicine provision.
- LAMA discharge: LAMA stage (before/during/after surgery), surgery date, LAMA date, in-treatment photo, and medicine provision.
- DAMA discharge: DAMA stage, discharge date, surgery date, in-treatment photo, feedback form, etc.
- Death: death stage (before/during/after surgery), death date, death certificate, clinical note/death summary, and mortality audit report.
- Biometric patient verification at discharge (fingerprint/face auth); exception process with discharge consent form upload.
- Beneficiary satisfaction form generation, download, and upload workflow.
- Auto grievance escalation based on the feedback submitted in the Satisfactory form.
- Daily feedback form to be enabled during hospitalization and based on the input given, the auto grievance mechanism to be put in place and ensure this should not be shown to Hospital and other field teams to ensure hassle free treatment to the patients.

4.3.4 Claims Processing

- Claim initiation by MEDCO after patient discharge with finance section review.
- Amount claimed as per hospital bill vs. approved package amount reconciliation.
- Supporting document upload: hospital bill number, date, hospital bill, post-operative investigations, detailed discharge summary, detailed ICPs, and treatment details.
- Claim submission with preview and validation before final submission.
- Claims query management: query raised by Trust, response by hospital within defined TAT.
- Claim rejection and arbitration process for disputed rejections.
- Claims settlement workflow: Trust approval, payment advice generation.
- RTGS/CFMS payment integration for direct bank transfer to empanelled hospitals.

- Claims submission within due duration of discharge as per scheme guidelines; relaxation provision for public hospitals as per Trust decision.
- Claims settlement within defined period of receipt of all required documents by Trust.

4.3.5 Follow-Up Medicine Cases and Chronic OP Treatments

- Follow-up registration for discharged patients requiring post-procedure medication for the identified procedure list.
- Chronic outpatient treatment management for listed conditions under defined schemes.
- Repeat authorization workflow for cyclic treatments (e.g., dialysis, chemotherapy).
- After 10-day post-discharge medicine tracking and hospital compliance monitoring.

4.3.6 Erroneous Claims Management

- Identification and flagging of erroneous claims through automated validation rules.
- Erroneous claim correction workflow with dual authorization.
- Recovery management for overpaid claims.
- Audit trail for all erroneous claim corrections with defined workflows.

4.3.7 Emergency Registration and Admission

- Emergency telephonic pre-authorization through dedicated round-the-clock helpline.
- Post-hoc documentation and authorization regularization workflow.
- Emergency case tracking dashboard for TRUST officials.

4.4 Health Benefit Packages (HBP 2022 Mapping)

The Procedures Module shall manage the complete lifecycle of Health Benefit Packages (HBP) and ensure real-time data sharing with the PMJAY ecosystem.

- All the existing packages should be mapped with the PMJAY's HBP 2022/latest version package with package codes, names, specialties, rates, and inclusions.
- Package component definition: diagnosis, doctor and nursing charges, pre-hospitalization investigations, bed charges, consumables, medicines, food, post-surgery investigation, and post-surgery medicines.
- Stratification management within packages.
- Implant price management and caps as per scheme guidelines.
- Multiple procedure pricing guideline implementation.
- Package rate customization for different schemes to be provided to the department.
- Real-time sharing of HBP data with PMJAY/NHA as per mandated documentation requirements.
- Integration with ICD-10/ICD-11 for diagnosis codes and SNOMED-CT for clinical terminologies.

- ICHI (International Classification of Health Interventions) code mapping.
- Standard Treatment Guidelines (STG) management and questionnaire configuration per procedure.
- Package auto-revision workflow with version control and effective date management.
- Audit trail for all package changes with due authentication through Aadhaar based/ Digital sign based at each level
- Provide a detailed pricing screen as per the HBP guidelines and ensure the department can able to review and revises the rates based on the policy with due approval flow which can be considered as a Pricing module.

4.5 Grievance Redressal Module

The Grievance Redressal Module shall provide a comprehensive platform for patients, hospitals, and staff to raise, track, and resolve grievances related to scheme operations.

4.5.1 Grievance Registration

- Multi-channel grievance submission: web portal, mobile app, call centre, and direct submission.
- Auto grievance raising provision based on the daily feedback form by the Patients or from On-bed visit details from the Vaidya Mithra on daily basis.
- Grievance categories: denial of treatment, delay in authorization, excess charges, Vaidya Mithra/MEDCO misconduct, hospital misconduct, quality of care, Death case, and others.
- Beneficiary grievance registration linked to Dr NTRVS card no./AB PMJAY ID/ABHA ID.
- Whistle blower grievance registration module
- Staff grievance registration for operational issues.
- Acknowledgement generation with unique grievance reference number.

4.5.2 Grievance Processing

- Automatic routing to concerned department/district based on grievance category and location.
- Multi-level escalation: District level to State level to CEO as per defined TAT.
- Investigation workflow with evidence collection and document management.
- Grievance committee management with hearing scheduling and digital proceedings.
- Trust/ISA compliance with Grievance Redressal Committee orders.
- Auto-escalation for unresolved grievances beyond defined TAT.
- Ensure all the cases which are unresolved beyond SLA to be reported by default to the Disciplinary committee with due alerts to the Officers concerned.

4.5.3 Grievance Reporting

- Weekly grievance summary reports to Trust.
- Pending, resolved, and escalated grievance dashboards.
- Category-wise, district-wise, and hospital-wise grievance analysis.

4.6 Medical Audit Module (Aligned with SAFU)

The Medical Audit module shall implement a robust framework for detecting, investigating, and preventing fraudulent activities, aligned with the AB-PMJAY SAFU (State Anti-Fraud Unit) framework.

4.6.1 Fraud Detection

- Outlier detection for claims data with configurable fraud trigger alerts.
- Real-time monitoring of fraud trigger parameters including: duplicate registration, duplicate pre-authorization, unusual procedure combinations, outlier hospitalization duration, outlier claim amounts, mismatched diagnosis and procedure codes, repeated use of same diagnostic report images across different cases.
- Real time alert to Pre-auth executives/doctors on the duplication of document duly alerting them with previous cases where the same document has been used.
- Document validation by cross-checking and detecting alterations in HD charts, OT notes, prescriptions, and related claim documents.
- Biometric matching data at IP and Discharge, Biometric cycles for Dialysis, Radiation and chemotherapy.
- On-bed photographic evidence verification against hospital admission records.
- Automated sharing of fraud alerts and trigger data with Dr NTRVST in real time.

4.6.2 Medical Audit Management

- Medical audit scheduling for min 5% of total hospitalized cases per empanelled hospital per quarter. The percentage of cases may vary (only increase) based on the needs of the Trust/ISA.
- The default audit cases should be retrieved based on the Audit parameters predefined in the system to identify the set percentage of cases. These should be defined by the Trust based on the Age, Gender, Procedure, seasonal disease wise or any other parameters.
- Mandatory audit of all the death cases.
- On-site audit workflow for MBBS/Specialist auditors with digital audit forms.
- Audit checklist covering: completeness of medical records, patient history and current illness documentation, operation reports, patient progress notes from admission to discharge, pathology and radiology reports, compliance with Standard Treatment Guidelines (STG) where issued.
- Audit report generation within 24 hours of audit completion.
- Weekly medical and hospital audit summary reports.
- Action taken report tracking on audit observations.

4.6.3 Hospital Audit

- Hospital audit conducted in conjunction with medical audit visit.

- Hospital audit checklist: operational helpdesk, scheme signage, Vaidya Mithra availability, IT infrastructure status, MoU compliance.
- Performance scorecard generation for each hospital.
- Auto assignment of doctors to the inspections of hospitals, if necessary instead of manually picking of doctors by the concerned wing staff/officers.

4.6.4 State Disciplinary Committee (SDC) Management

- All the audit cases, grievances, pre-auth level issues will be escalated to the SDC for appropriate action.
- Case registration for disciplinary action following proven fraud.
- Investigation timeline management (not more than 15 days for a case).
- Penalty and recovery workflow: de-empanelment, financial recovery, blacklisting.
- Natural justice compliance tracking: show cause notice issuance, response management, hearing records.
- Appealing work flow to the appellate authority after SDC action with required flow for raising a request, verification by appellate authority and approval scheduling of cases for weekly or fortnight meetings

4.6.5 Reporting

- Daily, weekly, and monthly fraud alert reports to Trust.
- Investigation status tracker dashboard.
- Financial impact analysis of detected fraud cases.

4.6.6 Field Audit

- Automated Auditor Assignment: The system must feature an auto-assignment algorithm to randomly allocate MBBS/Specialist doctors to specific hospital inspections, strictly preventing the manual selection/picking of auditors by concerned wing staff.
- Digital Audit Workflows: On-site audit workflows for auditors must be facilitated via digital audit forms (accessible via mobile/tablet).
- Medical Audit Checklist: Mandatory digital checklists covering: completeness of medical records, patient history, current illness documentation, operation reports, patient progress notes (admission to discharge), pathology/radiology reports, and compliance with issued STGs.
- Hospital Operations Checklist: Conducted in conjunction with the medical audit, this checklist must cover: operational helpdesk status, scheme signage, Vaidya Mithra availability, IT infrastructure status, and general MoU compliance.

Reporting & Analytics:

- Mandatory audit report generation within 24 hours of audit completion.
- Automated generation of weekly medical and hospital audit summary reports.

- Performance scorecard generation for each empanelled hospital based on audit findings.
- Tracking of Action Taken Reports (ATR) on all audit observations.

4.6.7 State Disciplinary Committee (SDC) Management

- **Centralized Escalation**: All unresolved grievances, pre-authorization level disputes, un-cleared field audit cases, and confirmed fraud cases shall be automatically escalated to the SDC module for appropriate disciplinary action.
- **Notice & Communication Framework**: The system must provide a communication framework allowing the SDC to digitally serve Show Cause Notices directly to hospitals seeking explanations. The system must track the entire communication thread—from notice issuance to hospital response and hearing records—until a final level of resolution is reached (Natural Justice compliance tracking).
- **SLA & Timeline Management:** Automated tracking of case investigation timelines, strictly enforcing a maximum limit of 15 days per case.
- **Penalty & Recovery Workflow**: Integrated digital workflows for executing disciplinary outcomes, including de-empanelment processing, financial recovery tracking, and hospital blacklisting.
- **Appellate Workflow:** A dedicated workflow for hospitals to appeal to the Appellate Authority following an SDC action. This must include raising a request, verification by the appellate authority, and automated scheduling of cases for weekly or fortnightly appellate meetings.

4.7 User management Module

4.7.1 User and Role Management

- Central user management with Role-Based Access Control (RBAC) for all application modules.
- Role definition: Vaidya Mithra/Mithra, MEDCO, Hospital Administrator, Medical Superintendent, District Coordinator, Trust Officials (various levels), CEO, Secretary, IT Admin, Audit Staff, Finance Staff, and others as defined by Trust.
- User creation, modification, deactivation, and deletion workflows with approval.
- Multi-level approval for new user creation.
- User mapping to hospitals, districts, and schemes.
- Automated account provisioning based on HR system integration.
- Session management: idle timeout, concurrent session controls.

4.7.2 Master Data Management

- Centralized master data management: LGD codes (State, District, Mandal, Village/Ward), hospital masters, specialty masters, procedure masters, drug masters, ICD codes, SNOMED codes, LOINC codes, scheme masters, benefit package masters.
- Master data creation, modification, enable/disable workflows with audit trail.
- Version control for all master data changes.
- Import/export capability for bulk master data management.

4.7.3 Configuration Management

- Scheme-wise configuration management: benefit limits, eligible beneficiary categories, procedures, rates, and workflows.
- Workflow configuration: TAT settings, escalation rules, auto-approval rules, query response windows.
- Notification configuration: SMS templates, email templates, WhatsApp message templates.
- Geo-fencing configuration for document upload location verification.

4.8 Administration, Accounts and Financial Management

HRMS and Payroll

- Bidders should study the existing recruitment and payroll models available in the existing system
- Development and implementation of a centralized, role-based HRMS platform covering end-to-end employee lifecycle management for Regular, Contract, Outsourcing, and Consultant categories.
- Creation of a digital employee master with unique Employee ID mapped to cadre, designation, department, service type, pay scale, and reporting hierarchy.
- Comprehensive employee profile module capturing personal details, Aadhaar (masked), contact details, social category, gender, disability status, educational qualifications, certifications, skills, experience, and complete service history with secure document repository.
- Digital Service Register with storage of appointment orders, pay fixation statements, increments, promotions, transfers, disciplinary proceedings, leave accounts, and retirement benefits data.
- Role-based access control for Employee, Reporting Officer, HOD, HR, Finance, and Competent Authority with configurable permissions.
- Vacancy requisition module enabling departments to raise post requirements with justification, service type, pay scale, roster category, and budget availability, routed

through HR and Finance for concurrence and approval by the competent authority.

- Vacancy notification generation with reservation roster as per AP Government norms, eligibility criteria, qualifications, experience, and automated publication to applicant portal.
- Online application submission for notified posts with scrutiny module for HR covering document verification, eligibility checks, rejection with reasons, and configurable shortlisting criteria.
- Interview management including panel constitution with approval workflow, interview scheduling, panel login for marks entry, remarks, automated merit list generation, and approval by Head of Organization.
- Offer management with salary structure finalization by HR and Finance, automated offer letter generation, appointment order issuance, digital joining report, and employee login activation from day one.
- Transfer and posting management with request initiation, approval workflow, relieving and joining tracking, and service record updates.
- Employee Self-Service portal for profile viewing, document downloads, leave balances, pay slips, service register extracts, and submission of requests for leave, advances, transfers, and grievances.
- Leave management compliant with AP Leave Rules covering EL, HPL, CL, CCL, ML, PL, Special Leave, LOP with automated leave credit, online application, multi-level approval workflow, leave encashment calculations, and leave analytics dashboards.
- Half-day permissions and short leave module integrated with attendance and approval workflow with automatic HR intimation after HOD approval.
- Attendance management integrated with biometric and Face Recognition System (FRS) devices with real-time capture, geo-tagging for field staff, late/early tracking, shift configuration, and attendance regularization workflow with full audit trail.
- Department-wise monthly attendance certification by HOD with recommendation workflow for salary processing.
- Grievance redressal system with confidential submission, category tagging including harassment and service matters, defined escalation matrix, SLA tracking, and resolution monitoring.
- · Dashboards for management showing sanctioned vs filled posts, roster status, leave utilization, attendance compliance, payroll expenditure, and department-wise HR analytics.

Payroll Scope

- Configuration of pay structures as per AP Government and contract norms including pay scales, DA, HRA, TA, special allowances, and increment automation.
- Monthly payroll processing with automated integration of attendance, leave, pay revisions,

advances, recoveries, and arrears.

- HOD salary recommendation workflow followed by HR verification and Finance approval prior to payment processing.
- Salary advance request module with approval workflow, loan sanction, disbursement, EMI recovery, and pre-closure facility.
- Statutory deductions configuration for PF, ESI, PT, IT, NPS with automated calculation and statutory report generation.
- Generation of digital pay slips, salary registers, bank advice files for e-payments, and audit-compliant payroll reports.
- Support for multiple employee categories with separate pay rules and consolidated financial reporting.

HRMS Monitoring

- Secure mobile application for employees with OTP/biometric login.
- Employee features include profile viewing, leave balance, leave application, permission requests, attendance marking through FRS/geo-tagging, pay slip download, grievance submission, and real-time notifications for orders, transfers, and salary credit.
- HOD and HR mobile dashboard for leave approvals, attendance monitoring, vacancy approvals, interview panel mark entry, and salary recommendation approvals.
- Push notifications for workflow actions, approvals, and alerts.

Other Modules:

- Store Management, Asset Management and Change management system, etc. with defined work flows and approval functionalities as desired by the Trust.

Claims payment processing:

- Hospital payment processing workflow with RTGS/CFMS integration after the approval of CEO
- Fund flow management: central fund to state fund, state to district, district to hospital.
- Payment advice generation with detailed claim breakdown.
- Financial reconciliation between claim amounts, approved amounts, and paid amounts.
- Integration with CFMS based on the approval of the CEO on FIFO basis based on the availability of the funds. And FIFO based queue should be maintained even if the funds are not available in the PD account and process whenever the funds are available
- At any point of time the department can able to see the list of cases which are already shared to CFMS and which are in the queue - Hospital wise, Procedure wise, category wise, district wise, etc. For ready report submission to the authorities.

Other payments, Procurement and Vendor Management:

- All the payment other than claims/ follow ups/Health camps/erroneous which are getting routed through Operations department of the Trust should be processed through a Government structure of administrative sanction.
- Vendor masters, Account masters, Heads, Subheads, Works, Employees, etc.
- Initiation of Vendor payment, workflow for Administration sanction with proper heads and sub heads
- Generation of administrative sanction to accounts wing.
- Payment approval workflow in the Accounts section for the vendor payments within accounts department
- Timely TDS payments of hospitals, vendors. Etc
- Income tax payments with required integration with the department portals
- PF and ESI payments initiation with approval flow and monthly generation of the same through Payroll module
- Form 16 and other documents generation in the respective hospitals/vendors/employees logins.
- Payroll integration for field staff incentive calculation and payment.
- Vaidya Mithra/Mithra incentive management: calculation, approval, and payment workflow.
- Financial reporting: daily, weekly, monthly, quarterly, and annual financial MIS.
- Budget and fund management: scheme-wise budget allocation, utilization tracking, and variance reporting.
- Integration with CFMS (Comprehensive Financial Management System) for GoAP financial systems.
- Tax deduction management (TDS) with statutory compliance.
- Integration with State Government payment gateway for citizen-facing transactions.
- Annual accounts and audit support module.
- All Transactional related to Bank integrations with in the functionality of the Trust.

4.9 Medical Reimbursement Module

The Medical Reimbursement Module shall manage the end-to-end process of medical expense reimbursement for State Government employees and pensioners who avail treatment at non-empanelled hospitals or in situations where cashless treatment was not available.

- Reimbursement application submission by employee/pensioner with supporting documents (bills, prescriptions, discharge summary, reports).
- Both online and offline reimbursement modules should be made available.

- Online submission by the Employee/pensioner through EHS or any other Finance department application with due integration should be made available
- Status update to the Employee/ Pensioner on real time for desired level as confirmed by the department
- Eligibility verification against employee/pensioner database.
- Treatment verification and expense claim scrutiny workflow.
- Multi-level approval: DDO/HoD, District Medical Officer, Head Office.
- Applicable rate verification against GoAP-approved rates.
- Reimbursement status tracking for applicants.
- Rejection with reasons and appeal management.
- MIS reports: pending claims, settled claims, amounts by category, grade, district.
- Integration with EHS module to cross-check if cashless treatment was available.

4.10 Health Camps Management

- Health camp scheduling, planning, and logistics management.
- Camp registration with location (LGD codes), date, type of camp, and target beneficiaries.
- PHC/NWH camp management for initial patient registration.
- Camp attendance and beneficiary registration tracking.
- Camp outcome reporting: number of patients screened, diagnosed, referred for hospitalization.
- Integration with beneficiary registration module for direct referral of detected cases.
- Health camp calendar and notifications for staff and beneficiaries.
- Post-camp analysis and MIS reports.

4.11 Field Operations Monitoring

This module shall enable real-time monitoring and performance management of the Trust's field workforce, including Mithras, Team Leaders, District Coordinators, and other field staff.

4.11.1 Mithra Performance Management

- Mithra attendance and shift management (24x7 shift-based operations at hospitals).
- Case-wise performance tracking per Mithra (registrations, pre-authorizations, discharges assisted).
- Hospital-wise and district-wise Mithra deployment tracking.
- Geo-fencing-based attendance and duty verification.
- Mithra incentive calculation based on performance metrics.

4.11.2 Team Leader and District Coordinator Management

- Hospital group assignment for Team Leaders with escalation matrix.
- District Coordinator performance dashboard with district-level KPIs.

- Visit record management with geo-tagged check-ins.
- Issue escalation from field to district to state level.

4.11.3 Field Operations Dashboard

- Real-time dashboard showing: active cases per hospital, pending pre-authorizations, TAT compliance, discharge pendency, and claims pendency.
- Alerts for hospitals with no Mithra on duty.
- Alert for pre-authorizations exceeding defined TAT.
- District-wise performance heatmap.

4.12 Mobile Applications

4.12.1 Citizen Mobile Application

The Citizen Mobile App shall be available on Android and iOS platforms, designed to be user-friendly and accessible to citizens with varying levels of digital literacy. The app shall be available in English and Telugu.

- All the Card holders should be provided with logins
- Users can able to login using Dr NTRVST/Ayushman ID/ABHA number or mobile number with OTP.
- Users can able to change the details like phone no., profile photo, address etc with due Aadhaar based authentication through OTP.
- Electronic Health Record (EHR) access: view personal health records, past treatment history, and uploaded reports - fully ABDM compliant.
- Hospital discovery: search nearby empanelled hospitals by specialty, procedure, location (GPS-based), rating, and availability.
- Appointment booking at empanelled hospitals.
- Real-time hospitalization status tracking during active treatment.
- Daily feedback submission during hospitalization (including diet, care quality, and staff behaviour).
- Grievance submission with photo/video attachment capability.
- Scheme information, benefit package details, and eligibility check.
- Notification engine: dietary advice, post-discharge medication reminders, scheme policy updates, health camps nearby, and government health alerts.
- Integration with teleconsultation service providers (optional/future integration).
- Integration with diagnostic test partners for basic health parameter monitoring (optional/future integration).
- ABDM milestone compliance: ABHA creation, health record linking (M1, M2, M3, M4).

- Accessibility features: text size adjustment, screen reader support, WCAG 2.0 compliance.

4.12.2 Staff Mobile Application

The Service Provider has to develop a Mobile application for field staff, MEDCOs, Mithras, DCs and other officials in addition to Citizen Mobile app, to deliver their regular duties and responsibilities especially on field and empanelled hospitals. The functionalities developed in the web portal should be developed in such a way to communicate with the Mobile app for exchange of data and attachments like uploading the documents and photos (On-bed, Discharge, OT, ICU/Ventilator photo, etc.).

The Staff Mobile App shall support role-based access for all Trust field and office staff including Mithras, MEDCOs, Team Leaders, District Coordinators, Trust Officers, and Executives including CEO and Principal Secretaries.

- Role-based dashboard with relevant KPIs and alerts for each role.
- Mithra: patient registration support, pre-authorization initiation, discharge assistance, on-bed photo capture with geo-tag.
- MEDCO: pre-authorization submission, claim initiation, document upload with Geo coordinates capturing for Discharge photos, on bed photos, discharge photos etc.,.
- District Coordinator and Team Lead: district/hospital performance dashboard, case escalation management.
- Trust Officials: real-time scheme performance dashboard, daily/weekly MIS reports.
- CEO/Secretary: executive summary dashboard with key scheme metrics, financial summaries, and alerts.
- Push notification for escalations, alerts, and approvals requiring action.
- Offline mode capability for basic data entry with sync when connectivity is restored.
- Secure authentication with OTP and biometric unlock.
- Geo-fencing and geo-tagging for field activity verification.

4.13 Unified Dashboards and MIS Reporting

4.13.1 Operational Dashboards

- Real-time operational dashboard: registrations, pre-authorizations (pending, approved, rejected), discharges, claims (initiated, paid, rejected), and amount paid - per scheme, per district, per hospital.
- TAT compliance dashboard for pre-authorization, claims, and grievance resolution.
- Hospital performance dashboard: case volumes, claim volumes, rejection rates, fraud alerts.
- Field staff performance dashboard: Mithra-wise, Team Leader-wise, District Coordinator-wise.

- Interactive reporting through AI Copilot with conversational analytics, drill-down, and report generation capabilities.

4.13.2 MIS Reports

Comprehensive MIS reports shall be available in Excel, PDF, and PowerPoint formats with the following dimensions at minimum:

- Scheme-wise: Dr Nandamuri Taraka Ramarao Vaidya Seva, EHS, WJHS, Aarogya Raksha, etc.
- Time period: daily, weekly, fortnightly, monthly, quarterly, annual, and custom date range.
- Dimensions: age, gender, community/sub-community, district, constituency, mandal, SGSW.
- Clinical dimensions: specialty-wise, procedure-wise, diagnosis-wise, hospital category-wise.
- Transaction dimensions: pre-auth initiated date, pre-auth approved date, claim initiated date, claim approved date, surgery updated date, discharge date, claim paid date.
- Graphical representation options: bar charts, pie charts, heat maps, trend lines, and custom visualizations.

4.13.3 Analytical System

- Centralized data warehouse integrating all modules and schemes.
- OLAP layer with star and snowflake schema support.
- Highly interactive dashboards accessible via web browser without additional software installation.
- Self-service analytics with drag-and-drop interface and minimal SQL knowledge requirement.
- Statistical and predictive modeling for fraud detection, utilization patterns, and health outcome analysis.
- Automated data integration with configurable collection frequency.
- Data integration with external data sources: census data, demographics, and disease burden data.
- Information delivery via scheduled email/SMS reports.
- Support for comparative analysis: MoM, QoQ, YoY, and custom period comparison.
- Exception reporting and color-coded exception thresholds.
- Map-based spatial analysis for geographic health access visualization.
- Text based and command based query builder for generating instant summary on desired analytics with excel, word, slide based generation features.
- Able to drag and drop the fields required to execute and fetch data sets.
- Fixed Parameter based analytics and alerts from the reporting duly implementing BI to identify with the lapses deviating the policy.

4.13.4. Healthcare Analytics & Predictive Analytics

- The Bidder shall provide an integrated Healthcare Analytics and Predictive Analytics platform capable of generating operational, clinical, financial, utilization, fraud, and performance analytics through configurable dashboards and reports.
- The solution shall provide real-time dashboards covering hospital performance, claim processing, disease trends, beneficiary demographics, audit status, fraud investigations, financial utilization, claim rejection patterns, fraud recovery, and key performance indicators.
- The solution shall support configurable predictive analytics models to identify high-risk hospitals, high-risk providers, abnormal claim behaviour, emerging fraud trends, seasonal disease patterns, resource utilization, future claim volumes, and financial risk projections.
- The analytics platform shall support drill-down analysis, geographical visualization, configurable dashboards, ad hoc reporting, role-based access, scheduled report generation, and export in standard formats.
- The solution shall support configurable Key Performance Indicators (KPIs) to measure the effectiveness of medical audits, fraud detection activities, claim adjudication efficiency, hospital performance, and overall scheme governance.

4.13.5 Data Sources:

Data Sources for the proposed Analytical and Reporting System will primarily consist of the existing transactional system at Dr. NTR VST with the scope of incorporating external data from other sources as identified during the requirements analysis discussions and also as proposed by the vendor based on their understanding of the Healthcare Insurance and operations domain. Primary sources of data for the Dr. NTR VST Analytical System is from the Dr. NTR Vaidya Seva Application suite.

Following are the indicative functional areas that would be used for developing the Analytical Solution for all the schemes and programs implementing by the Dr NTRVST:

i) Patient Registration
ii) Empanelment & Hospital Data Management
iii) Change/ addition of MEDCOs, Doctors, Nursing staff, Paramedical staff, etc.
iv) Pre-Authorization
v) Discharge
vi) On bed verifications by Field staff
vii) Feedback of the Patient
viii) Enhancements
ix) Claims Submission & Processing
x) Erroneous claims
xi) Treatment & Discharge

xii) Follow-ups Claims
xiii) Chronic OP treatments
xiv) Health Checkup
xv) Grievances
xvi) Flags
xvii) Disciplinary actions
xviii) Appellate cases
xix) Audit
xx) Payments
xxi) IVRS call Outcomes
xxii) KPI Parameters of the Trust, Individuals working in the Trust
xxiii) Application Logs
xxiv) Database Logs
xxv) API Logs
xxvi) Aadhaar enabled authentication transaction logs for biometric, IRIS, OTP, Face-auth (Device wise, Hospital Wise, User wise, District wise etc)

4.14 Digital Health Compliance & Interoperability

4.14.1. Healthcare FHIR Conversion Engine

- The Bidder shall provide a Healthcare Interoperability Engine capable of converting extracted clinical information into HL7 FHIR-compliant healthcare resources.
- The solution shall transform structured healthcare information into standard FHIR resources including, but not limited to, Patient, Practitioner, Encounter, Observation, Condition, Procedure, Medication, Diagnostic Report, Imaging Study, Document Reference, Claim, Coverage, Organization, and Care Plan.
- The solution shall expose secure API interfaces supporting JSON and XML formats for seamless interoperability with Hospital Information Systems (HIS), Electronic Medical Record (EMR) systems, Electronic Health Record (EHR) systems, ABDM ecosystem components, Trust applications, Insurance systems, and other authorized healthcare platforms.
- The solution shall be extensible to accommodate future revisions of FHIR standards and national healthcare interoperability frameworks.

4.14.2. National Health Claims Exchange (NHCX) Integration

- The Bidder shall provide integration with the National Health Claims Exchange (NHCX) framework to enable secure, standardized, and interoperable electronic exchange of healthcare claims information.
- The solution shall support electronic exchange of pre-authorizations, claim submissions, supporting medical documents, adjudication responses, payment advice, claim settlement information, investigation outcomes, fraud alerts, and other claim-related transactions through NHCX-compliant APIs.
- The solution shall ensure interoperability with National Health Authority (NHA), Ayushman Bharat Digital Mission (ABDM), Third Party Administrators (TPAs), Trust systems, Hospital Information Systems, and other authorized healthcare stakeholders.
- The Bidder shall ensure compliance with all prevailing NHCX specifications, API standards, security requirements, and future enhancements notified by the Government of India.

4.15 External Integrations

4.15.1 National Health Ecosystem Integrations

- ABDM (Ayushman Bharat Digital Mission): ABHA creation, health record linking, consent manager, HIE-CM integration - M1, M2, M3, M4 milestone compliance.
- ABPMJAY/NHA: HEM, TMS, HBP 2022, SAFU, Grievance module data sharing with NHCX routing.
- National Health Mission (NHM): integration for beneficiary data and health program coordination.
- Integration with RTGS for Core dashboard and other data sets for direct access to the HCM office for any sort of analysis out of the schemes outcome
- Integration with Hospitals HMIS System.
- Integration of Application and database logs to the Trust for real time assessment and monitoring of system performance, threats, unwanted hits, etc. to alert the department for immediate action.
- Integration with State or National bodies specific to Specialty and Procedures based data exchange with NCDIR, National Cancer registry (NCRP), Blindness Control Program, Thalassemia, ADIP Scheme - cochlear cases, etc.
- State Health departments - Integration with State Health departments like CMHFW, DSH, DME, Sanjeevani, Aids Control and other programs based on the necessity.
- Integration with SGSW department for proper data exchange pertaining to Beneficiaries data along with family mapping.
- Provide a centralized API Management UI with interactive API development and management capabilities supporting both REST, SOAP services etc., along with a real-

time dashboard for monitoring live APIs, data synchronization status, API performance, usage analytics, and error reporting.

- The above requirements are indicative but not exhaustive. Further, the scope of requirement shall be extend based on the Trust requirement. The Service Provider should deliver all the requirements without any financial implications on the Trust.

4.15.2 Identity and Authentication Integrations

- UIDAI: Aadhaar authentication (biometric, OTP, face auth) using AUA/KUA/Sub-AUA framework as per UIDAI guidelines.
- ABPMJAY - BIS data integration with ABPMJAY
- ABDM: ABHA identification based in Aadhaar
- Digi Locker: for document verification and sharing.
- Biometric devices (fingerprint scanners, IRIS scanners) for Aadhaar authentication at hospitals.
- Digital signature for document authentication.
- eRUPI voucher system integration.
- The platform establishes a secure, real-time integration between the Hospital Management Information System (HMIS) of empanelled hospitals and the Trust. Through this integration, hospitals can electronically submit pre-authorization requests and claims, accompanied by the complete set of supporting clinical and administrative records required under the Standard Operating Procedure (SOP) of each treatment package. These records include, but are not limited to:
    - Clinical photographs
    - Inpatient (IP) notes and progress sheets
    - Laboratory investigation reports
    - Radiology reports together with the associated images
    - Discharge summary
    - Prescriptions
    - Pharmacy bills and medication records
    - Any other package-specific documentation mandated by the SOP
- All data exchange is designed to be ABDM-compliant (M1–M4), NHCX-enabled, and fully auditable, thereby supporting both efficient claim processing and the strengthened oversight functions of the State Anti-Fraud Unit (SAFU).

4.15.3 State Government System Integrations

- CFMS (Comprehensive Financial Management System): fund flow, payment processing, and financial reconciliation.
- SGSW (Swarna Grama/ Swarna Ward): beneficiary verification and enrolment support.
- APSDC integration with state IT infrastructure.
- Andhra Pradesh State Health Department systems: HMIS, LMIS, NHM portal.
- RTGS: For Core dash board
- Health department: HMFW/DSH/DH whenever required for implementing various state or central health initiative programs.

4.15.4 Financial Integrations

- RTGS/NEFT payment gateway for direct hospital payments.
- CFMS integration for budget and vendor ID generation
- Payment gateway for Hospital payments by Trust and along for citizen-facing payments (co-payments where applicable).

4.15.5 Communication Integrations

- SMS gateway integration for OTP, notifications, and alerts.
- Email gateway for system notifications and reports.
- WhatsApp Business API for beneficiary notifications.
- IVRS (Interactive Voice Response System) integration for beneficiary feedback and outbound call automation.
- National Call Centre linkage (AB-PMJAY National Helpline 14555) integration.
- FRS integration for employees' salaries.

4.15.6 Geo-Fencing attendance Implementation

- Implement Geo-fencing technology for document upload location verification to ensure pre-authorization and claim documents are captured from within designated hospital premises.
- Geo-fencing for field staff attendance verification (Mithras, Team Leaders, District Coordinators). FRS should have the provision for Offline attendance.
- Geo-tagged photographs of patients for IP, daily on-bed verification, discharge, and OT/ICU documentation using FRS wherever possible.
- Geo-fencing violation alerts to District Coordinator and Trust officials in real time.

4.15.7 Enterprise Email System

4.15.7.1 Existing Email and Authentication Setup - Replacement of NIC mail Setup

1. The Trust currently operates a NIC-based enterprise mail service for Trust users.
2. Email IDs are provisioned for all Trust users and select operational roles and are used as the primary channel for official communication within the Dr NTRVS ecosystem.
3. The overall storage footprint of the mail server for approximately 200 users is estimated to be in the range of 20 TB.

4. User accounts currently exist for Trust staff to ensure that scheme-related communication is routed only through authenticated users of the Trust ecosystem.
5. The existing legacy mail platform and its integration mechanisms do not fully align with the proposed cloud-native, microservices-based architecture and SDC hosted environment envisaged under this RFP.

4.15.7.2 Enterprise Email and SSO Solution

1. The Service Provider shall design, provision, configure, and operationalize a MietY certified enterprise email and identity platform to replace the existing NIC mail solution.
2. The new solution shall be hosted on a MeitY-empanelled environment (same or securely integrated with the environment hosting the Dr NTRVS Application Suite), as approved by the Trust.
3. The solution shall function as the Trust-wide enterprise email, identity, and SSO backbone for all applications covered under this RFP, with email IDs acting as the primary digital identity for users.
4. The Service Provider shall perform end-to-end migration from the existing NIC email system, including mailbox data (approximately 18–20 TB overall), user accounts, distribution lists, and role-based groups, ensuring integrity and non-repudiation of migrated data.
5. Migration shall be carried out with minimal downtime and clearly defined cut-over planning, including pre-migration data assessment, pilot migration, user acceptance, and final switchover.
6. The bidder shall provide detailed migration tools, methodologies, rollback procedures, and post-migration verification reports as part of the implementation plan.

4.15.7.3 SSO and Identity Integration Requirements

1. The new system shall support Single Sign-On (SSO) for all Trust applications (including the Dr NTRVST Application, EHS, WJHS, Medical Reimbursement, Mobile Apps and any future modules) using secure, industry-standard protocols such as SAML 2.0 and/or OAuth 2.0 / OpenID Connect, together with Digital Signature Certificate (DSC) and Aadhaar eSign integration compliant with the IT Act, 2000 and CCA guidelines, enabling Class 3 DSC (FIPS 140-2 USB token) based login and signing of approvals, claims, payment files and orders, with real-time certificate validation (CRL/OCSP), trusted time-stamping, browser-independent and bulk signing, and a complete, non-repudiable audit trail of all login and signing events.

2. User authentication to all major applications shall be routed through the CSP-supported identity and email platform, ensuring that only authenticated users with valid official email IDs can access the systems.
3. The solution shall support Multi-Factor Authentication (MFA) for sensitive roles and transactions, and configurable conditional access policies (e.g., device, location, risk-based).
4. The email and identity platform shall integrate with the User and Role Management module, so that application roles and email identities remain synchronized throughout the user lifecycle except the Citizen Mobile app.
5. All user creation, modification, and deactivation workflows shall ensure that application access is automatically aligned with email account status and assigned roles.

4.15.7.4 User Coverage and Mailbox Categories

1. The enterprise email and identity platform shall cover, at a minimum, the following categories of users:
    a. Trust Head Office users (CEO, senior officials, functional wings, IT team, finance, audit, SAFU, etc.)
    b. Trust/ Implementation Support Agency users (where applicable)
    c. District-level users (District Coordinators, Managers, Associates, auditors, finance personnel, grievance officers)
    d. Empanelled hospital users including MEDCOs, hospital administrators, preauthorization doctors, billing staff
    e. Field functionaries including Vaidya Mithras / Mithras, field coordinators, audit teams, and other field staff.
2. The Service Provider shall design and implement a role-based mailbox provisioning model with at least two tiers:
    a. Enterprise-grade mailboxes for Trust, district coordinators, district managers/associates, and other identified key roles, with higher mailbox storage limits, advanced collaboration features, archival and e-discovery support, and extended retention as per Trust policy.
    b. Standard / limited mailboxes for users such as MEDCOs in empanelled hospitals, Vaidya Mithras / Mithras, and other field staff, with optimized storage, essential mail features, and policy-driven restrictions, while ensuring authenticated communication.
3. The bidder shall be responsible for creating and configuring email IDs for all existing and new users as per the finalized user matrix and HR/administrative records.

4. Naming conventions, domain policies, and group structures (e.g., hospital-wise, district-wise, scheme-wise groups and distribution lists) shall be implemented as approved by the Trust.
5. The system shall support scalable onboarding of additional users and roles over the contract period without service disruption.

Minimum Requirement for Mail Services

<u>For CEO and other HODs/ Officers of the Trust i.e., requiring high storage and advanced collaboration</u>

User Capacity

- The solution shall support no minimum or maximum seat limit.
- The solution shall support unlimited users for large-scale departmental and enterprise deployments.

Core Email & Applications

- The solution shall provide secure, enterprise-grade business email services.
- The solution shall support custom domain-based, ad-free professional email.
- The solution shall include integrated applications:
    - Online word processing
    - Online spreadsheets
    - Online presentations
- All applications shall be accessible via web and mobile (Android & iOS).
- The solution shall support access across devices (desktop, web, mobile).
- The solution shall support both online and offline modes.

Storage & Data Management

- The solution shall provide minimum 1 TB pooled cloud storage per user.
- The solution shall support shared drives/shared storage, ensuring organizational ownership of data instead of individual users.
- The solution shall support storage of emails, documents, and attachments.

Security & Identity Management

- The solution shall support Single Sign-On (SSO) and integration with Active Directory / Identity Providers.
- The solution shall support automated user provisioning and de-provisioning.
- The solution shall provide 2-Step Verification (2SV) and push-based authentication.
- The solution shall provide Security Health monitoring and reporting.
- The solution shall support Advanced Endpoint Management (mobile and desktop devices).
- The solution shall provide a centralized admin console for complete control and policy

enforcement.

Email Security

- The solution shall support:
    - Spam protection
    - Malware and virus protection
    - Anti-phishing and advanced anti-phishing protection
    - Anti-spoofing protection
    - Attachment protection
    - Safe links and external image protection
    - Protection against unauthenticated emails
- The solution shall support:
    - Email log search and message tracing
    - Custom email filtering and routing
    - Email quarantine and administrative actions

Communication & Collaboration

- The solution shall support:
    - Real-time team messaging (chat) with threaded rooms and guest access
    - Direct messaging and group chats
    - Native desktop client
    - Native mobile applications (Android and iOS)
- The solution shall support document sharing and collaboration.

Enterprise Search

- The solution shall provide advanced enterprise search capabilities across:
    - Emails
    - Documents
    - Chats
    - Entire organizational domain

AI / Generative AI Features

- The solution shall include built-in Generative AI capabilities:
    - Smart reply and email drafting assistance
    - AI assistant integrated within email interface
    - Smart replies in chat
    - Voice message transcription (web and mobile)
    - Live captions during meetings
    - AI-powered content/video creation
    - Grounded research features (upload sources, summaries, Q&A, audio overviews)

Calendar & Scheduling

- The solution shall provide integrated calendar services with:
    - Resource booking (meeting rooms, etc.)
    - To-do lists / reminders
    - Sync with mobile devices
    - Team/shared calendars

Groups & Directory

- The solution shall support:
    - Business groups and mailing lists
    - Admin-managed groups
    - Search and discovery of groups

Support & Integration

- The OEM shall provide 24/7 support via phone, email, and online channels.
- The solution shall support integration with third-party archival and compliance tools, if required.

Compliance & Certifications (Mandatory)

The solution shall comply with the following:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy Information Management)
- SOC 2 and SOC 3 reports

Service Level Agreement (SLA)

- The solution shall provide a minimum 99.9% uptime guarantee.

<u>For Field staff (Vaidya Mithras)/ MEDCOs etc</u>

User Capacity

- The solution must support no minimum or maximum user limit, enabling unlimited users for large-scale departmental deployment.

Core Applications

- The solution must provide an integrated suite including:
    - Business Email
    - Calendar
    - Online Word Processing
    - Online Spreadsheets
    - Online Presentations
- All applications must be accessible via web and mobile devices.

Storage

- The solution must provide minimum 10 GB cloud storage per user for email, documents, and photos.
- Storage should be sufficient for mobile-first communication and essential document access.
- Must support secure cloud-based file storage per user.

Accessibility & Usability

- Must support access across devices (desktop, mobile, and tablet).
- Must support both online and offline working modes.

Identity & Access Management

- Must be compatible with Microsoft Active Directory and integrate with identity management systems.
- Must support Single Sign-On (SSO).
- Must support secure login with 2-step verification and push notifications.
- Must provide a centralized administrative console.

Device Management (MDM / Endpoint Security)

- Must include built-in Mobile Device Management (MDM) / Endpoint Management.
- Must support Android, iOS, and Windows 10 devices.
- Must support:
    - Remote device wipe
    - Passcode enforcement
    - Application management
- Must support both BYOD and government-issued devices.

Email & Communication

- Must provide secure, professional email with **custom domain support**.
- Must support instant messaging/chat for team coordination.

Email Security

The solution must support:

- Spam protection
- Malware and virus protection
- Anti-phishing protection
- Anti-spoofing protection
- Advanced threat protection (phishing & malware)
- Attachment protection
- Safe links and external image protection
- Protection against unauthenticated emails
- Message tracing through email log search

- Custom mail filtering and routing
- Email quarantine management

Threat Protection

- Must include ransomware detection.
- Must provide warning mechanisms for external sharing to prevent data leakage.

Collaboration

- Must provide native applications for Android and iOS.
- Must support document creation and presentations.
- Must allow collaboration with external participants.

Chat & Communication

- Must support direct messaging.
- Must support creation of chat rooms/groups.
- Must provide a native desktop client.

AI / Generative AI Features

- Must include built-in Generative AI capabilities.
- Must support smart replies in chat.
- Must support voice message transcription on web and mobile.
- Must support live captions during meetings.
- Must support grounded research features including:
    - Uploading documents/sources
    - Summarization
    - Audio overviews
    - Q&A

Calendar & Scheduling

- Must support resource booking (e.g., meeting rooms).
- Must include reminders/to-do functionality.
- Must sync calendars across mobile and tablet devices.
- Must support team/shared calendars.

Groups & Administration

- Must support business groups.
- Must support admin-managed groups.

Compliance Logging & Audit

- Must provide access to logs for tracking email and document activity.
- Must support Drive/file activity logs for auditing access and usage.

Support & Implementation

- OEM must provide 24/7 support via phone, email, and online channels.

Compliance & Certifications

The OEM must comply with:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy Management)
- SOC 2 and SOC 3 reports

Service Level Agreement (SLA)

- The solution must provide a minimum uptime SLA of 99.5%.

4.15.8 Text SMS Notifications

SMS (Short Message Service) is a reliable and widely accessible communication method, allowing Dr NTR VST to reach stakeholders quickly and directly on their mobile phones. It does not require internet access/smart phone, making it an ideal option for reaching a broad audience, including those in rural or low-connectivity areas. SMS can be used to send important alerts, reminders, or updates about ongoing programs, deadlines, and other mission-related activities. Its simplicity and high open rate make it an essential tool for effective communication.

Bidder conditions for the Text SMS:

- The bidder shall provide end-to-end SMS services, including transactional messages, OTPs, alerts, and emergency notifications for the TRUST, as per the requirements defined by the TRUST.
- The bidder shall strictly comply with all applicable regulations issued by the Telecom Regulatory Authority of India, DoT, and DLT platforms. All messaging shall follow Government policies, including data protection and communication guidelines.
- The Trust shall register all Sender IDs (Headers) and templates on the DLT platform. The bidder shall assist in DLT registration, scrubbing, and template management.
- SMS shall be routed through reliable and compliant telecom routes, as per the conditions specified in the relevant section. The bidder shall ensure high throughput and low latency delivery. Real-time delivery status shall be provided.
- Delivery is subject to telecom operator networks; however, the bidder shall ensure best-effort delivery.
- A standard SMS shall be limited to:
    - 160 characters for GSM (7-bit) encoding (English)
    - 70 characters for Unicode (UCS-2) (regional languages)
- Concatenated SMS shall follow:
    - GSM: 153 characters per part
    - Unicode: 67 characters per part

4.15.9 WhatsApp Messaging

WhatsApp Messaging provides Dr NTR VST with an efficient and interactive communication channel for connecting with stakeholders. It allows for the exchange of real-time information, including text, images, videos, and documents, making it a versatile tool for outreach. WhatsApp's widespread usage ensures accessibility, even for beneficiaries in remote areas. The platform also supports the WhatsApp Chatbot for two-way communication, enabling beneficiaries to ask questions or seek system enabled clarifications instantly. Its ease of use, coupled with multimedia support, makes WhatsApp an effective tool for engaging and keeping beneficiaries informed.

For this service, the bidder should integrate with the "MANA MITHRA" WhatsApp service of Government of Andhra Pradesh

4.16 Digital Sign implementation:

Digital Sign will be used by the Head of the departments and other officials of the Trust including the District level heads to sign on Notices to Hospitals, Administrative sanctions, Payment orders, internal UO notes, proceedings generated through Application suite. Doctors to approve specific cases or for all cases in addition to the Aadhaar authentication for each case.

Specifications:

- The solution should support document signing from web and mobile platforms, allowing users to sign documents from anywhere and at any time.
- The solution should enable users to sign data using both cryptographic tokens.
- The solution should be compatible with all latest browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Edge, Safari, etc., including mobile operating systems.
- The signing solution should not have any 3rd party dependencies such as Java Applet, ActiveX, etc., to ensure wider adoption in multiple environments.
- The system should allow the use of cryptographic token for signing within the application workflow whenever digital signing is required.
- The signing solution should provide easy interfaces, APIs, and web services for real-time document signing.
- The solution should facilitate signing of multiple documents in bulk or at a single go.
- Co-signing should be supported, allowing multiple users to digitally sign a single document.
- The solution should also support signing of multiple pages within the same document.
- The solution should support full long-term validity (LTV) and signed documents should be LTV enabled with timestamping. It can be verified any time and a signed copy will always have a green tick in the acrobat reader.

- The architecture of the signing solution must be scalable and flexible to accommodate modular expansion as per future requirements.
- The signing solution should support encryption of all or part of requests and responses.
- The service should ensure that the hash data exchanged for signing between the system should be encrypted and secure.
- The bidder & the OEM should provide operation support and maintenance services for the solution for the period of Five (5) Years.
- All the proposed solutions shall comply with all existing and future Information Security Guidelines for Digital Signature Certificates and should adhere to the Controller of Certifying Authorities (CCA) Guidelines issued by the Government of India.
- The signing solution shall accept all digital certificates issued by licensed Certifying Authorities (CAs) under the purview of CCA in India.
- The Signing Solution Provider should be a Licensed Certifying Authority (CA) under Controller of Certifying Authorities (CCA), India for the last 10 Years.
- The Signing Solution Provider should be a Licensed Digital Signature and eSign Service Provider (ESP) under Controller of Certifying Authorities (CCA), India.
- The CA should be a Signing Solution Provider of DSC based signing solution, Authentication solution and e-Sign Solution.
- If the bidder is a reseller, they must submit the Manufacturer's Authorization Form (MAF) issued by the Signing Solution Provider for all the offered products / items specified in the tender. The MAF must authorize the bidder to submit the bid including Signing Solution Provider support till end of the project.
- The Signing Solution Provider should have a valid CMMI Level 5 Certificate issued from the CMMI Institute of India.
- The Signing Solution Provider must have executed at least Ten (5) projects of similar nature i.e. Signing Solution to any Government Entity or PSU in India.
- The Signing Solution Provider should not have been blacklisted / debarred by any Government Entity or PSU in India during the submission of tender.
- The Signing Solution Provider should have ISO 20000, 27001, 9001, 27018 certifications.

4.17 Operations & Maintenance (O&M) — Application and Infrastructure Services

- The Service Provider shall be responsible for end-to-end Operations and Maintenance (O&M) of all applications, databases and related services deployed as part of this engagement. The scope encompasses all activities necessary to ensure continuous, secure, and operation of the system across all internal and external user locations on a 24×7 basis, in strict adherence to the Service Level Agreements (SLAs) and contractual

obligations agreed upon with Dr NTRVST. The Service Provider shall perform all additional activities reasonably required to ensure the effective operation, maintenance, and support of the application suite.

4.17.1 Day-to-Day Operations and Application Management

The Service Provider shall perform the following activities as part of routine operations and application management:

A. Core Operational Responsibilities

i. Responsible for the day-to-day operations and maintenance of the application on a 24×7 basis as per the functional requirements, SLA parameters, and contractual agreement across all internal and external user locations.

ii. Maintenance of applications by duly undertaking and implementing all changes logged by department users. All changes to the application as suggested by the Trust's department shall be handled within the defined timelines.

iii. Analysis of open change requests; prioritization and implementation of all business-critical changes post receipt of formal approval from the Trust.

iv. Monitoring of daily batch jobs running on the servers, ensuring timely execution, exception handling, and escalation in case of failures.

v. Migration of all current functionality to new or enhanced versions during any future upgrades, modifications, or enhancements, ensuring zero data loss and minimal downtime.

vi. Monitoring the availability and performance of services and applications; troubleshooting and resolving bottlenecks using industry-standard techniques; ensuring effective capacity planning; and proactively alerting the Trust regarding new hardware or software requirements.

vii. Addressing all functionality, availability, and performance issues, including implementation of system change requests within agreed SLA timelines.

viii. Addressing all errors, bugs, and gaps in the functionality of existing applications in a timely and systematic manner.

ix. Adherence to ITIL v3 / ITSM related guidelines for all operations and maintenance activities.

B. Application Lifecycle and Performance Management

i. Tuning of applications, databases, third-party software, and all other solution components to optimize overall performance.

ii. Performing changes, bug fixes, error resolutions, and enhancements incidental to the proper and complete functioning of the application.

iii. Application code changes necessitated by patches to licensed software or third-party components used in the solution.

iv. Migration of all current functionality to new or enhanced versions during future upgrades, modifications, or enhancements.

v. Monitoring of application health and load on the application and database layers; carrying out tuning and code changes for optimal performance.

vi. Maintaining version control and configuration information for all application software and system documentation; updating and maintaining all project-related documents.

vii. Ensuring uninterrupted availability of the complete system at the end-user point, meeting all functional, non-functional, technical, and security requirements.

viii. Maintaining version control and configuration information of the application throughout the contract period.

4.17.2 Database Management and Administration

The Service Provider shall manage and administer all databases forming part of the solution, covering the full spectrum of database operations as detailed below:

i. Undertake management of databases to facilitate smooth functioning and optimum utilization, including regular database backup, periodical testing of backup data, database administration, archival management, configuration review and tuning, database security management, maintenance of necessary documentation, and management of database schema, disk space, user roles, and storage allocations.

ii. Management of database upgrades or patch upgrades as and when required, ensuring minimal downtime and zero data loss.

iii. Regular backups for all databases in accordance with the approved backup and archive policies; conducting recovery operations whenever required with appropriate permissions from the Trust.

iv. Monitoring and enhancement of the performance of scheduled backups; scheduling regular testing of backups; and ensuring adherence to defined data retention policies.

v. Performing regular internal audits of applications, data, and user access for optimal performance and security compliance.

4.17.3 Patch Management, Security, and Software Upgrades

The Service Provider shall be responsible for all patch management and security update activities, as described below:

i. Performing patch management, testing, and installation of software upgrades issued by the OEM or Service Providers from time to time.
ii. Installation of application-level upgrades, database-level upgrades, and security patch updates with documented testing and rollback procedures.
iii. Any changes to application code required due to patches applied to licensed software components.
iv. In the event any software component reaches end-of-life, the Service Provider shall proactively inform the Trust in advance, assist in determining specifications, and provide technical support to facilitate fresh procurement by the Trust.

4.17.4 Application Maintenance and Support Services

Application maintenance and support services shall be provided under two broad categories:

(a) Routine Managed Support, and

(b) Change Request-Based Support.

A. Support and Maintenance Activities

Support requests shall broadly include, but are not limited to, the following:

- Bug fixing and defect resolution
- Code optimization and performance tuning
- Data validation and data correction
- Report tuning and backend data services including report generation
- Enhancements and modifications requiring up to 3 man-days of effort
- Code version control and configuration management
- User training and end-user support
- Project management, impact analysis, root cause analysis, and monthly support review presentations
- Changes to workflow and approval processes
- Development work required as per Vulnerability Assessment and Penetration Testing (VAPT) findings

B. Bug Fixing / Defect Resolution

Fixing of bugs already identified prior to commencement of the contract, as well as those identified during the contract period. A list of already identified bugs shall be shared with the Service Provider at the time of contract commencement.

C. Enhancement and Modification

Enhancement, modification of the existing application code and any other new developments as per the functional requirements, updated business rules, regulatory mandates, or other directives as and when issued by the Trust.

4.17.5 User Management, Access Control, and Administrative Services

The Service Provider shall provide comprehensive user management and administrative support services covering the following:

i. Maintenance of user IDs — additions, modifications, and deactivation — and maintenance of associated user access logs.
ii. User ID and group management services to ensure proper role-based access control.
iii. Maintaining and enforcing access controls to protect and limit application access to authorized end-users only.
iv. Administrative support for user registration, creation and maintenance of user profiles, granting of user access and authorization, ongoing password support, and providing administrative support for directory and email servers.
v. Creation of additional users and maintenance of user logs as required during the contract period.
vi. Addition of new roles for accessing existing services as directed by the Trust.
vii. Audit trail maintenance: maintaining historical records of all transactions and activities effected, with sufficient detail to track the activity of all users and log the same on a real-time basis.
viii. Configuration of new rules and any other configurable data entities in the system as required by the Trust.

4.17.6 Functional Changes, Configuration, and Module Enhancements

The Service Provider shall implement all routine functional changes and configuration updates directed by the Trust, including but not limited to the following:

i. Introduction of new forms, new workflows, or modifications to existing workflows for existing services.
ii. Addition or modification of validations in e-forms.
iii. Modifications to forms, including addition of new fields, removal of fields, modification of approval levels, changes in processing logic and approval logic, and addition of attachment requirements.
iv. Configuration changes to improve performance and operational efficiency of the system.

v. Creation of new report formats and configuration of reports as per user requirements.
vi. Extension of Trust services via the Trust portal to other government departments.
vii. Addition of new interfaces with existing banks or new banking entities.
viii. Changes to the application or development of new application modules for strategic control and monitoring by the Trust or its appointed body.
ix. Release management for interim releases of the application.
x. The Service Provider shall provide support to the Trust and such agencies designated by the Trust for the implementation of integration and interfacing requirements, including making available all data and industry-standard interfaces.
xi. Various report creations on user requests.
xii. All GUI changes as directed by the Trust.

4.17.7 Documentation, Version Control, and Compliance

The Service Provider shall ensure systematic maintenance of all documentation and compliance records throughout the contract period as detailed below:

i. Maintaining user manuals and constantly updating help manuals in line with changing functionalities of the application.
ii. Maintaining version control and configuration information for all application software, infrastructure components, and system documentation.
iii. Updating and maintaining all project documents including design documents, test records, deployment notes, and operational runbooks.
iv. Submission of a Quarterly Report covering all changes performed in the system and resolution of malfunctions during the preceding quarter.
v. Application logs shall be maintained and shared with the Trust on a regular basis as mutually agreed.
vi. Sharing application and database server log reports and network settings with the Trust on tapes or equivalent digital medium on a regular basis.

4.17.8 Change Management System and Issue Tracking

The Service Provider shall deploy and operate a robust request tracking system to manage all service requests from department users:

i. Deploying a request tracking tool for receiving change/service requests and issues from department users and enabling status checks for each raised request or issue.
ii. Defining Standard Operating Procedures (SOPs) with call prioritization guidelines, problem severity codes, and escalation procedures, in consultation with the Trust.

iii. Tracking and routing all service requests; assigning a severity level to each ticket as per the defined SOPs.

iv. The Service Provider shall develop and implement all the Change/Service Requests provided by the Trust without any additional cost during entire Agreement period.

4.17.9 IT Helpdesk Setup and Operations

The Service Provider shall establish and operate a fully functional IT Helpdesk to provide support for all users of the Trust's application ecosystem.

4.17.10 Training and Capacity Building

The Service Provider shall provide structured training and knowledge transfer services throughout the contract period as and when required:

i. Training to Trust officials and other users on new modules developed during the course of the project period, ensuring self-sufficiency in day-to-day operation.

ii. End-user support in case of technical difficulties in the use of the software, including answering procedural questions and providing recovery and backup information.

iii. Updating and maintaining user manuals and help documentation as per changing functionalities of the application on an ongoing basis.

4.17.11 Audit, Compliance, and Reporting

The Service Provider shall ensure compliance with all audit and reporting obligations as detailed below:

i. Undertaking regular internal audits of the applications, data, and user access for optimal performance and security compliance.

ii. Maintaining an Audit Trail: historical records of all transactions effected, with sufficient detail to track the activity of all users; logs shall be maintained and available on a real-time basis.

iii. Application logs shall be maintained and shared with the Trust on a regular basis.

iv. Sharing application and database server log reports and network settings with the Trust on tapes or equivalent digital medium on a regular basis.

v. Submitting a Quarterly Report on all changes performed in the system and resolution of malfunctions carried out during the preceding quarter.

vi. Supporting the Trust and its designated agencies for integration and project implementation activities; making available all data and industry-standard

interfaces and integration touch points for interoperability with the Trust's suite of applications.

4.17.12 Design, Development, Testing, and Delivery of Requirements During the O&M Phase

The Service Provider shall be responsible for the design, development, testing, and delivery of all requirements during the Operations & Maintenance (O&M) phase, including any new or additional requirements identified by the Trust from time to time. The Service Provider shall implement and deliver such requirements without any financial implications or additional cost to the Trust.

No Change Request (CR) process shall be applicable under this Tender during the Operations & Maintenance (O&M) phase. All enhancements, modifications, new requirements, and other deliverables identified by the Trust during the O&M phase shall be executed by the Service Provider as part of its contractual obligations, without any additional cost, payment and compensation.

5. TECHNICAL REQUIREMENTS

5.1 Technology Architecture

5.1.1 Microservices Architecture

The application suite shall be designed and developed on a microservices-based architecture where each functional domain (empanelment, TMS, HBP, grievance, fraud management, Change Management System, accounts, etc.) is implemented as an independently deployable, loosely-coupled microservice. Key requirements:

- Each microservice shall have its own data store and API boundary.
- Asynchronous communication between microservices using event-driven messaging.
- API gateway for all external-facing API endpoints.

5.1.2 Technology Stack

The Bidder shall propose a modern, open-source-preferring technology stack. The following are indicative requirements:

- Backend: Node.js/Python
- Frontend: React.js/Angular
- Mobile: Native Android/Kotlin and Swift

- Database: CSP Native fully managed database services supporting relational, NoSQL, and globally distributed horizontally scalable databases with strong consistency, automatic scaling, high availability, and integrated backup and disaster recovery.
- Messaging: CSP Native fully managed, scalable event streaming and messaging service supporting publish-subscribe architecture.
- API Management: CSP Native API management platform for secure API publishing, lifecycle management, traffic control, and analytics.
- CI/CD: CSP Native continuous integration and continuous deployment services with automated build, test, and release pipelines.
- Monitoring: CSP Native observability suite providing real-time monitoring, logging, alerting, and performance insights.
- Identity Management: CSP Native identity and access management service enabling fine-grained access control, role-based policies, and user identity governance.

Note: All licenses required for this project i.e. software, Hardware, ATS/AMC, SSL Certificates, Call Centre equipment's and any other subscriptions required to procure, these should be procured in the name of Trust. The cost of the all software's and hardware equipment shall be borne by the Service Provider.

5.2 Security Requirements

5.2.1 Application Security

- CERT-In empanelled agency security audit before every production deployment (new go-live, major changes, new modules).
- VAPT (Vulnerability Assessment and Penetration Testing) every 6 months or after major changes.
- OWASP Top 10 vulnerability compliance.
- Secure Software Development Life Cycle (SSDLC) with code reviews and automated security scanning in CI/CD pipeline.
- Input validation, output encoding, and SQL injection prevention.
- CSRF protection, XSS prevention, and clickjacking protection.
- Security headers implementation (HSTS, CSP, X-Frame-Options).
- It is the responsibility of the service provider to submit the all types of Security Audit Certificates to the Trust by annually or as decided by the Trust.
- The IS Audit and other Audits should be complete as per the requirement of the Trust.
- The Service Provider shall bear all the cost to obtain Security Audit Certificates from the CERT-In empanelled Agencies.

5.2.2 Data Security

- End-to-end encryption for all data in transit (TLS 1.2+).
- Encryption at rest for all sensitive data (AES-256 or equivalent).
- Data masking for PII in non-production environments.
- Database-level access control with principle of least privilege.
- Row-level security for multi-tenant scheme data.

5.2.3 Identity and Access Management

- Multi-factor authentication (MFA) for all Trust officials and critical roles.
- Aadhaar-based authentication integration for hospital-side users.
- Role-Based Access Control (RBAC) with granular permissions.
- JWS token authentication for all API endpoints.
- Account lockout after configurable failed login attempts.
- Password complexity enforcement and expiry policy.
- Single Sign-On (SSO) capability with LDAP/Active Directory integration.
- Idle session timeout and forced re-authentication for sensitive operations.

5.2.4 Audit and Compliance

- Comprehensive audit trail for all user actions, data changes, login events, and API calls.
- Immutable audit logs with timestamp, user ID, IP address, and action details.
- Audit logs retained for a minimum of 7 Years.
- Auto-escalation of unauthorized access attempts to designated security officers.
- ISO 27001 certification for the application suite during the agreement period.
- Compliance with NHA Health Data Management Policy, HIPAA, DPDP act, GDPR principles, and Andhra Pradesh Legislature Portal Privacy Policy. GIGW (Guidelines for Indian Government Websites) compliance for all web portals.

5.2.5 Network Security

- DDoS protection for all internet-facing services.
- Web Application Firewall (WAF) deployment.
- Application and database in separate network layers with restricted port access.
- Software-defined Security (SDS) implementation.
- Network segmentation with VPC isolation for different environments.

5.3 Healthcare Standards Compliance

- ICD-10 and ICD-11 coding for all diagnoses, procedures, and mortality codes.
- SNOMED-CT and India Extension Codes for clinical terminologies.
- LOINC codes for all laboratory and diagnostic investigations.
- ICHI (International Classification of Health Interventions) for procedure codes.
- LGD (Local Government Directory) codes for all location references.

- FHIR Release 4 for all clinical data exchange APIs.
- HL7 standards for inter-system messaging where applicable.
- ABDM ABHA Number standards for patient identification.
- NrCES Claims Profile specifications for claims-related APIs.
- EHR Standards 2016 notified by MoHFW for Electronic Health Records.

5.4 Non-Functional Requirements

Parameter	Requirement
Application Uptime	99.9% (24x7x365), excluding planned maintenance windows
Response Time	Web pages: < 3 seconds; API responses: < 2 seconds; Reports: < 10 seconds
Concurrent Users (Enterprise)	1,50,000 concurrent users - Dr NTRVS 1,00,000 concurrent users - EHS 20,000 concurrent users - WJHS
Concurrent Users (Mobile)	10 lakh+ concurrent users for Mobile apps of Dr NTRVS/EHS/WJHS citizen apps
Language Support	English and Telugu; extensible to other regional languages
Accessibility	WCAG 2.0 Level AA compliance; screen reader support
Browser Compatibility	Latest 2 versions of Chrome, Firefox, Edge, Safari
Mobile Platform Support	Android 14+; iOS 23+
Data Retention	All transaction data: minimum 10 Years; Audit logs: minimum 7 Years
Backup Frequency	Daily incremental; Weekly full backup; tested quarterly
Scalability	Horizontal and vertical auto-scaling based on load
Code Quality	SonarQube or equivalent quality gates; < 3% code duplication
API Standards	RESTful APIs with Open API 3.0 specification; FHIR R4 for clinical data

6. MULTI-SCHEME SUPPORT

The Dr. NTRVS Application Suite shall be designed as a multi-scheme platform capable of managing multiple healthcare schemes administered by the Trust on a single technology platform, with scheme-specific configurable workflows, benefit packages, eligibility rules, and financial parameters. The following schemes shall be supported:

Scheme Name	Target Beneficiaries
Dr Nandamuri Taraka Rama Rao Vaidya Seva	BPL and eligible citizens of Andhra Pradesh
Employees Health Scheme (EHS)	State Government serving Employees, Retired employees, and eligible family members
Working Journalists Health Scheme (WJHS)	Accredited Working Journalists and eligible family members
Medical Reimbursement	State Government employees and pensioners for treatment at non-empanelled facilities
Aarogya Raksha	APL and eligible family members of Andhra Pradesh
Amrutha Health Scheme	Orphans

Additional Development:

Any additional development related to Schemes, Modules, workflows, user roles, access provisioning, or configurations required shall be carried out by the selected bidder without any additional financial implication to the Trust during the entire contract period.

6.1 Multi-Scheme Platform Requirements

- Configurable scheme parameters: benefit limit per family per year, eligible beneficiary categories, co-payment rules, package rates, and eligible procedures.
- Scheme-specific enrolment and eligibility verification workflows.
- Scheme-specific hospital network (different hospitals may be empanelled for different schemes).
- Scheme-specific document requirements for pre-authorization and claims.

- Scheme-specific payment terms and settlement timelines.
- Scheme-specific reporting and MIS.
- Single beneficiary may be covered under multiple schemes; deduplication and benefit coordination rules shall be configurable.
- Scheme-specific payment gateway integration with corresponding bank accounts and CFMS codes.
- All security, audit, and compliance standards shall be equally applicable to all schemes.

7. MANPOWER REQUIREMENTS

7.1 Development Phase (6 Months)

The Bidder shall deploy complete team in the Trust office for entire development phase along with dedicated Clinical Domain Team during the Development Phase comprising:

S.No	Position (No. of Resources)	Minimum Qualification	Minimum Experience
1	Project Manager (01)	BE/B. Tech/MBA + PMP/Prince2 Certification/ MCA/ M. Tech/ Relevant Degree	10+ Years IT/Health Administration; 6+ Years in Public Healthcare; Project Management
2	Solutions Architect (01)	BE/B. Tech/MCA/ M. Tech	10+ Years IT; 6+ Years in Public Healthcare; Solution Architecture and Building Scalable Solutions
3	Health care Domain Experts (03)	Degree with Healthcare background preferred	1) Chief Medical Officer / Clinical Domain Lead (1)- MBBS/MD, 10+ Years in Health PMJAY/ State Health Schemes, knowledge with Experience in Healthcare IT platforms 2) Claims Adjudication and Medical Audit: a) Desk Audit (1)- MBBS/BHMS/BAMS/BDS, 5+ Years b) Field Audit (1)- MBBS/BHMS/BAMS/BDS
4	Database Lead / Developer (02)	BE/B. Tech/MCA/M. Tech	8+ Years; PostgreSQL/ Oracle/ MySQL; Cloud Database Modelling and Performance tuning
5	Database Administrator	BE/B.	6+ Years; PostgreSQL/ Oracle/

	(01)	Tech/MCA/M. Tech	MySQL; Cloud Database Administration and Maintenance
6	Sr. Data Analyst (01)	Masters/Bachelor degree in Computer Science/Statistics/ Mathematics/Economics/Data Science	10+ Experience in Data Analytics with minimum experience in Health insurance domain/Health care domain.
7	Mobile App Developer (01)	BE/B. Tech/MCA/M. Tech	3+ Years; Native Android / Kotlin Development & SWIFT IOS Development
8	Senior Developers - Backend (04)	BE/B. Tech/MCA/M. Tech	5+ Years; Node.js/Python; Microservices; API Development
9	Senior Developer - Frontend (04)	BE/B. Tech/MCA/M. Tech	5+ Years; React/Angular; UI/UX implementation
10	Junior Developers (08)	BE/B. Tech/MCA/M. Tech	3+ Years; Relevant Development Stack
11	QA / Testing Lead (01)	BE/B. Tech/MCA/M. Tech	5+ Years; Automation testing, Performance Testing, VAPT support
12	QA Engineers (03)	BE/B. Tech/MCA/M. Tech	3+ Years; Automation Testing, performance Testing, VAPT support, load testing

13	Business Analyst (02)	BE/B. Tech/MCA/M. Tech (CS)	5+ Years; Healthcare IT; Requirement Analysis, SRS Preparation, UAT coordination
14	Cyber Security Engineer (01)	BE/B. Tech/MCA/M. Tech	3+ Years experience in Cyber Security
15	Cyber Security AI-ML Graduates (01)	BE/B. Tech Cyber Security with AI/ML	Experience in Cyber Security with AI/ML
16	UI and UX designer (01)	BE/B. Tech/MCA/M. Tech	3+ Years experience in UI and UX.
17	Technical Support Engineer (01)	BE/B. Tech/ MCA/ M. Tech / any other relevant degree	3+ Years experience in the similar field

Note: All the above team including the Project Manager should be available in Dr. NTR Vaidya Seva Trust premises during the design, development, Testing, implementation phase.

7.2 O&M Phase (5 Years) - (Onsite at Trust Premises)

During the O&M phase, the Bidder shall deploy the entire team in Trust office premises. This team shall be responsible for day-to-day operations, support, additional developments, enhancements, and maintenance of the entire application suite. The Service Provider shall ensure continuity of the key personnel involved in the design, development, implementation, and deployment of the solution during the subsequent Operations and Maintenance (O&M) phase. Any replacement or change of such key personnel shall be subject to prior approval of the Trust and shall be supported by a comprehensive knowledge-transfer and handover process to ensure that there is no loss of project knowledge or adverse impact on service delivery.

S.No	Position (No. of Resources)	Minimum Qualification	Minimum Experience

1	Project Manager (01)	BE/B. Tech/MBA+ PMP/Prince2 Certification/ MCA/ M. Tech/ MBA -AI OR IT/ Relevant Degree	10+ Years IT/Health Administration; 6+ Years in Public Healthcare; Project Management
2	Health care Domain Experts (03)	Degree with Healthcare background preferred	1. Chief Medical Officer / Clinical Domain Lead (1)- MBBS/MD, 10+ Years in Health PMJAY/ State Health Schemes, knowledge with Experience in Healthcare IT platforms 2. Claims Adjudication and Medical Audit: • Desk Audit (1)- MBBS/BHMS/BAMS/BDS, 5+ Years • Field Audit (1)- MBBS/BHMS/BAMS/BDS
3	Database Lead / Developer (02)	BE/B. Tech/MCA/M. Tech	8+ Years; PostgreSQL/ Oracle/ MySQL; Cloud Database Modelling and Performance tuning
4	Database Administrator (01)	BE/B. Tech/MCA/M. Tech	6+ Years; PostgreSQL/ Oracle/ MySQL; Cloud Database Administration and Maintenance
5	Sr. Data Analyst (01)	Masters/Bachelor degree in Computer Science/Statistics/ Mathematics/Economics/Data Science	10+ Experience in Data Analytics with minimum experience in Health insurance domain/Health care domain.

6	Mobile App Developer (01)	BE/B. Tech/MCA/M. Tech	3+ Years; Native Android / Kotlin Development & SWIFT IOS Development
7	Senior Developers - Backend (02)	BE/B. Tech/MCA/M. Tech	5+ Years; Node.js/Python; Microservices; API Development
8	Senior Developer - Frontend (02)	BE/B. Tech/MCA/M. Tech	5+ Years; React/Angular; UI/UX implementation
9	Junior Developers (04)	BE/B. Tech/MCA/M. Tech	3+ Years; Relevant Development Stack
10	QA / Testing Lead (01)	BE/B. Tech/MCA/M. Tech	5+ Years; Automation testing, Performance Testing, VAPT support
11	QA Engineers (01)	BE/B. Tech/MCA/M. Tech	3+ Years; Automation Testing, performance Testing, VAPT support, load testing
12	Business Analyst (01)	BE/B. Tech/MCA/MBA/ M. Tech (CS)	5+ Years; Healthcare IT; Requirement Analysis, SRS Preparation, UAT coordination
13	Cyber Security Engineer (01)	BE/B. Tech/MCA/M. Tech	3+ Years experience in Cyber Security
14	Cyber Security AI-ML Graduates (01)	BE/B. Tech Cyber Security with AI/ML	Experience in Cyber Security with AI/ML
15	UI and UX designer (01)	BE/B. Tech/MCA/M.	3+ Years experience in UI and UX.

		Tech	
16	Technical Support Engineer (01)	BE/B. Tech/ MCA/ M. Tech / any other relevant degree	3+ Years experience in the similar field

Note: The total O&M team members shall be physically present at the Trust office premises on all Trust working days during Development Milestones (M1–Final Sign Off, T1–T5; 6 Months) & O&M Phase. A minimum of 2 critical resources shall be available in the Trust Office on Saturdays, Sundays, and public holidays for critical support. The Team shall be available 24x7 for on call support.

7.3 Personnel Replacement Policy

- All key personnel shall be assigned for a minimum period of 12 months without replacement.
- Any replacement of key personnel requires prior written approval from the Trust with at least 30 days' notice.
- Replacement personnel must have equivalent or higher qualifications and experience.
- A minimum 30-day handover/knowledge transfer period is mandatory before any key personnel departure.

8. PROJECT TIMELINE AND DELIVERABLES

- Bidder should enter the Agreement with the Trust duly submitting the Bid security and other relevant documents in original within 7 working days from the date of issue of Work order.
- Bidder should assign and depute the Manpower as mentioned below for Development phase within 15 days from the date of enter into agreement with the Trust
- The minestrone starts from the 16th day from the date of entry into agreement with the Trust.

8.1 Overall Project Timeline - Development

Milestone	Activity	Duration	Key Deliverables
M1	**Project Kick-off, AS-IS Study, BPR, Solution Architecture, Requirement Gathering**	**T1 (Month 1)**	• Kick-off report; Project Charter & Governance structure • AS-IS Assessment Report and To-Be Process Design • BPR report • System Requirement Specification (SRS) — approval gate for development start • High-Level Design (HLD) and Solution Architecture Document
M2	**Core Module Development, Deployment & Go-Live (TMS, Empanelment, HBP); Architecture Finalisation**	**T2(Months 2–3)**	*Continuous process: develop, deploy, and take core modules live within Months 2–3. Development starts only after SRS approval by the Trust.* • Final SRS (if residual updates), HLD & LLD, API documentation • Unit test reports and development builds • Core modules (TMS, Empanelment, HBP) developed, deployed, and gone live in production • Architecture finalisation aligned to live core landscape • Interim UAT sign-off for core modules prior to / at go-live • Production cutover plan, hypercare start,

Milestone	Activity	Duration	Key Deliverables
			and core-module go-live report
M3	**Ancillary Module Development & Incremental Go-Live (Grievance, SAFU, Accounts, HRMS, MIS)**	**T3 (Month 4)**	*Release of ancillary modules into the live environment as a continuous rollout.* • Ancillary modules developed, integrated, and deployed to production • Integrated builds; integration and security scan reports • Comparison reports of agent recommendations vs human decisions • Incremental go-live of Grievance, SAFU, Accounts, HRMS, and MIS on the live core
M4	**Mobile App Development and External Integrations on Live System**	**T4 (Month 5)**	• Mobile apps (Android/iOS) developed, tested, and released • External integrations and integration test reports • Event-driven orchestration and human task queues on the live estate • Full System Integration Testing (SIT) and User Acceptance Testing (UAT) • Security testing (VAPT) against the live + staging landscape
FINAL SIGN-OFF	**UAT Closure, CERT-In Audit, Performance Testing, Data Migration Completion & Full Go-Live**	**T 5 (Month 6)**	*Everything is live by end of month 5: remaining cutovers closed, audits complete, full production estate certified.* • UAT sign-off for remaining scope; training completion reports • CERT-In audit certificate and VAPT closure • Performance test report • Complete data migration & reconciliation; data migration report • Production deployment of any residual modules / integrations

Milestone	Activity	Duration	Key Deliverables
			• Controlled activation of approved low-risk agentic features (if not already live in M4) • Go-Live readiness certificate and full Go-Live report • Exit criteria sign-off for Development Phase — entire solution live
O&M	**Operations, Maintenance, and Enhancements (on the live system)**	**T6 (5 Years + 2 Years (extendable))**	*Steady-state operations of the fully live platform from FINAL SIGN-OFF onwards.* • Ad hoc Changes in the existing modules. • Monthly operational reports • Quarterly performance reviews • Enhancement releases and hypercare-to-steady-state transition

8.2 Detailed Deliverables

Deliverables follow a continuous build–deploy–go-live model. Core modules (TMS, Empanelment, HBP) are developed and taken live in Months 2–3 (M2). Subsequent modules and features are released onto that live base. The complete solution is live by the end of FINAL SIGN-OFF. Development of application code starts only from the date of SRS approval by the Trust.

- M1 (T1 Month 1): Inception, AS-IS / To-Be, BPR, SRS, HLD, architecture and governance. No production go-live.
- M2 (T2 Months 2–3): Core modules (TMS, Empanelment, HBP) developed, deployed and gone live.
- M3 (T3 Month 4): Ancillary modules built and incrementally released onto the live core.
- M4 (T4 Month 5): Mobile apps and external integrations released onto the live estate; SIT / UAT / VAPT.
- Final Sign-Off (T5 Month 6): Full-estate UAT close, CERT-In, performance testing, complete migration and residual cutover. Entire solution live. Development-phase exit.
- O&M (T6 5 years + 2 years extendable): Operations, maintenance and enhancements on the live system.

8.2.1 Development Phase Deliverables

A. Foundation artefacts (M1 — T1 Month 1)

- Project Inception Report and Project Plan with detailed milestones aligned to continuous go-live (core live in M2; full estate live by FINAL SIGN-OFF).
- Project Charter and Governance structure.
- AS-IS Study Report and Gap Analysis Report.
- To-Be Process Design.
- Business Process Re-engineering (BPR) Report.
- Software Requirements Specification (SRS) for all modules — Trust approval is the gate for start of development.
- High-Level Design (HLD) including architecture, integration design and security design.
- Solution Architecture Document.
- Security design and threat model document (baseline; updated before each production release).
- Kick-off report.

B. Core modules — develop, deploy and go live (M2 — T2 Months 2–3)
These artefacts cover TMS, Empanelment and HBP. Production go-live of the core is an M2 deliverable and is not deferred to FINAL SIGN-OFF.

- Low-Level Design (LLD) for core modules.
- Database design document for the core schema (entity-relationship diagrams, data dictionary), versioned for subsequent module increments.
- API design specification document (Open API 3.0) for core services.
- Unit test cases and unit test execution reports for core modules.
- Integration test cases and integration test execution reports for core interfaces.
- Interim UAT plan, test cases and interim UAT sign-off for core modules.
- Core-module security scan / pre-production VAPT findings and closure note.
- Core data-migration plan (as applicable), migration scripts and post-migration validation report for the core cutover.
- Deployment guide and operations runbook for the core production estate.
- Role-wise user manuals for core functions (web) in English and Telugu, sufficient for core go-live.
- Training materials and completion report for core-user groups required at M2 go-live.
- Source code repository with version history for the core release (handed over to the Trust).

- Core production deployment package and Core Go-Live Report (TMS, Empanelment, HBP live).
- Hypercare commencement note and P1/P2 support roster for the live core.

C. Ancillary modules — incremental live release (M3 — T3 Month 4)

- LLD, unit test cases and unit test execution reports for Grievance, SAFU, Accounts, HRMS and MIS.
- Updated database design, data dictionary and API specifications (Open API 3.0) for ancillary services.
- Integrated builds and integration test execution reports against the live core.
- Security scan reports for ancillary releases.
- Comparison reports of agent recommendations versus human decisions (where agentic assist is in scope).
- Incremental production deployment of ancillary modules onto the live core.
- Updated user manuals and quick reference guides for newly live modules (English and Telugu).
- Ancillary incremental go-live note and updated operations manual.

D. Mobile, integrations and agentic features on the live estate (M4- T4 Month 5)

- Mobile applications (Android and iOS) with store-ready builds, integration test reports and production release.
- External integration specifications, test reports and live cutover of approved interfaces.
- Event-driven orchestration design and human task-queue configuration on the live estate.
- Controlled production activation packs for Claim Co-Agent, Grievance Triage and Executive Intelligence (approved low-risk features only).
- Full System Integration Testing (SIT) report across core, ancillary, mobile and integrations.
- UAT plan, test cases and in-phase UAT reports for M4 scope.
- Security testing (VAPT) report against staging and the live landscape, with remediation tracker.
- Updated source repository, release notes and operations manual for M4 production releases.

E. Full-estate closure and complete go-live (FINAL SIGN-OFF — T5 Month 6)

By the end of FINAL SIGN-OFF the entire solution is live. FINAL SIGN-OFF closes residual scope, certifies the estate and exits the Development Phase.

- Consolidated UAT plan (residual and regression), test cases and UAT sign-off reports covering the full solution.
- Performance / load test plan and results report confirming response-time and concurrency benchmarks.

- CERT-In empanelled-agency security audit certificate obtained before declaration of complete go-live.
- Complete data migration plan (if not already executed in increments), final migration scripts, reconciliation and post-migration validation report.
- Production deployment of any residual modules or integrations.
- Controlled activation record of any remaining approved low-risk agentic features.
- Deployment guide and operations manual — final Development-Phase edition.
- User manuals for all roles (web and mobile) in English and Telugu — complete set.
- Training materials: presentations, e-learning videos and quick reference guides.
- Training completion reports for all designated user groups.
- Source code repository with full version history handed over to the Trust.
- Go-Live readiness certificate and complete Go-Live Report for the full estate.
- Exit criteria sign-off for the Development Phase.

8.2.2 O&M Phase Deliverables

O&M applies to the fully live platform from completion of FINAL SIGN-OFF for five years, extendable by two years (T6, milestone 0&M).

- Monthly operational report: uptime, incidents, resolutions, pending issues and change requests.
- Quarterly performance review presentation.
- Quarterly VAPT report and action-taken report.
- Annual CERT-In security audit certificate.
- Release notes for every production deployment.
- Updated source code repository after every release.
- Updated user manuals and training materials after every feature release (English and Telugu as applicable).
- Annual application health assessment report.

8.3 Deliverable Sign-off Process

Sign-off is milestone-wise and aligns with incremental go-live. Core go-live in M2 and full-estate go-live require their own formal sign-off. Incremental M3 and M4 production releases require sign-off of the deliverables listed for that window.

- Each deliverable shall be submitted to the Trust for review.
- Trust shall review and provide written feedback within 10 working days of submission.
- Bidder shall address all feedback within 5 working days and resubmit.

- Final sign-off shall be provided in writing by the designated Trust official.
- All sign-off documents shall be stored in electronic format on cloud.
- No milestone payment shall be released without formal sign-off on the corresponding deliverables for that milestone (including M2 core go-live and FINAL SIGN-OFF complete go-live).
- There shall be no partial sign-off or acceptance of a milestone. Incremental module releases in M3 and M4 are complete milestones in their own right; they are not partial acceptance of final sign off.
- Production go-live of a module set (core in M2; ancillary in M3; mobile / integrations / agentic in M4; residual / full estate) shall not proceed without the Trust's written authorisation for that release.

8.4 System Acceptance and Certification

Acceptance is staged to match continuous go-live, with two formal acceptance events plus in-phase release authorisations.

8.4.1 Core System Acceptance

The Trust shall grant Core System Acceptance upon satisfactory completion of the following for TMS, Empanelment and HBP (T2, end of milestone M2):

- All M2 deliverables submitted and approved.
- Interim UAT completed with sign-off from designated Trust representatives for core modules.
- Agreed core performance and security gates met for the core release.
- Applicable core data migration completed with validation sign-off.
- Training completed for designated core-user groups.
- Core Go-Live Report accepted and core production authorised.

8.4.2 In the release authorisation (

Each incremental production release onto the live estate requires (T3, T4 & milestones M3, M4):

- Deliverables for that window submitted and approved.
- Relevant UAT / SIT sign-off for the release scope.
- Security scan or VAPT findings for the release closed or risk-accepted in writing by the Trust.
- Updated runbooks and user documentation for the newly live scope.

8.4.3 Full System Acceptance and Certification

Formal full-system acceptance shall be granted by the Trust upon satisfactory completion of the following. This is the Development-Phase exit. The entire solution shall be live.

- All Development-Phase deliverables (milestone M1 through FINAL SIGN-OFF) submitted and approved.
- User Acceptance Testing completed with sign-off from designated Trust representatives for the full solution.
- Performance testing confirming response-time and concurrency benchmarks are met.
- CERT-In empanelled agency security audit certificate obtained.
- Data migration completed with validation and reconciliation sign-off.
- Training completed for all designated user groups.
- Go-Live readiness certificate and complete Go-Live Report accepted.
- Exit criteria for the Development Phase signed off. O&M obligations commence on the live estate.

9. ROLES AND RESPONSIBILITIES

9.1 Roles and Responsibilities of the Bidder (Service Provider)

9.1.1 Design & Development Responsibilities

- Should deploy complete team in Trust office.
- Conduct detailed AS-IS study and BPR in close coordination with Trust officials and current vendors.
- Obtain the requirements from the concerned Head of the Departments for design, development and deployment of the requirements.
- Submit SRS documents for each requirement for approval.
- Perform end-to-end design, development, testing, and deployment of the complete application suite.
- Develop and maintain all integration layers with national and state systems.
- Perform complete data migration from the legacy system including structured (5 TB) and unstructured (300 TB) data across 5,000+ tables from existing service provider to Trust desired location.
- Migration of Data Centre and Disaster Recovery Centres from Existing Service Provider to the Trust desired location.
- Conduct Knowledge Transfer from the existing vendor to ensure no data or functionality loss.
- Perform comprehensive testing: unit, integration, system, performance, security, and UAT.
- Security scan or VAPT closure before each production release in M2–M4, and a CERT-In certificate before full go-live (end of final sign off milestone) and annually thereafter.

- The service provider shall audit the application from a CERT-In empanelled agency and submit the Security audit certificates to the Trust by-annually or as per the requirement of the Trust.
- The cost of all the Security Audits, IS audits and all other audits shall be borne by the Service Provider.
- Train all designated user categories including Trust staff, hospital staff, and field staff.
- Implement CI/CD pipeline and version control from day one.
- Design and implement cloud-native applications with built-in high availability, security, scalability, and observability to ensure production readiness from the outset.
- Bear the cost of required software and DB licenses if any subject to Trust decision on need/utilization.
- Should provide SLAs monitoring tools before go-live of the application.

9.1.2 O&M Responsibilities

- Deploy entire O&M team at Trust premises throughout the O&M phase.
- Ensure 24x7 technical support including Saturdays, Sundays, and public holidays.
- Resolve all incidents within defined SLA timeframes.
- Execute all approved requirements within given timelines by the Trust.
- Perform proactive monitoring of application health, database performance, and cloud infrastructure.
- Perform regular database backup, testing, and recovery procedures.
- Implement all security patches and vulnerability fixes on highest priority.
- Conduct quarterly VAPT and implement all remediation actions.
- Perform all third-party audits, statutory audits, and Trust-commissioned reviews.
- Submit all prescribed reports (monthly, quarterly, annual) to Trust in a timely manner.
- Maintain all project documentation in up-to-date state.
- Provide training for all newly developed features.
- Alert Trust in advance of any software reaching End-of-Life.
- Ensure request and response time in all application modules does not exceed SLAs.
- Submit SRS document for the requirements for approval of the Trust.
- Obtain the requirements from the concerned Head of the Departments for design, development and deployment of the requirements.
- Develop the requirements, workflows, Modules as per the requirement of the Trust.
- Submit security audit certificate before every production deployment from the Trust identified CERT-In agency.
- The service provider shall audit the applications from a CERT-In empanelled agency and submit the Security audit certificates to the Trust by-annually or as and when required.

- The cost of all the Security Audits, IS audits and all other audits shall be borne by the Service Provider.
- Bear the cost of required software/DB/AI/ML tool licenses subject to Trust decision on need/utilization.

9.1.3 Compliance Responsibilities

- Fix all vulnerabilities identified by CERT-In, Trust, or any authorized body on highest priority.
- Ensure ABDM (M1, M2, M3, M4) compliance is maintained throughout the contract period.
- Ensure data privacy compliance as per applicable laws and regulations.
- Implement and maintain all security controls as per NHA Health Data Management Policy.

9.2 Roles and Responsibilities of Dr Nandamuri Taraka Ramarao Vaidya Seva Trust

- Appoint a designated Nodal point for the project duly appointing a Nodal officer.
- Provide access to all relevant documentation, current system data, and current vendor for knowledge transfer.
- Provide all required domain inputs (clinical protocols, scheme rules, operational workflows) through designated domain experts.
- Provide timely approvals, sign-offs, and feedback within defined turnaround times.
- Facilitate access to all stakeholders including field staff, hospital staff, and beneficiaries for UAT and training.
- Ensure availability of adequate office space and infrastructure at Trust premises for the development and O&M teams.
- Coordinate with State and Central Government agencies for API access and integrations.
- Organize and facilitate training sessions for all user categories.
- Conduct fortnightly review meetings for the first 3 months and monthly review meetings thereafter.
- Have the right to call for additional review meetings as required.
- Provide written approval for all requirements before implementation.
- Maintain the final decision authority on all project-related matters.
- Processing of payments to the Service provider based on the payment terms.

9.3 Governance Structure

9.3.1 Project Core Group

Headed by CEO, Dr NTR VST, the Project Core Group shall meet fortnightly to review day-to-day project progress. It shall include Trust Project Officers, ITE&C Department representatives, Service Provider Project Manager, and Nodal officer will act as a Convenor.

9.3.2 Project Monitoring Committee (PMC)

Chaired by the CEO, Dr NTR VST, and comprising HoDs of key departments, the Project e-Governance Mission Team (PeMT) shall monitor overall project implementation progress based on inputs from the Project Core Group.

9.3.3 IT Wing

The IT wing shall independently monitor SLA compliance, prepare periodic performance reports, make recommendations on payments and penalties, and assist in exit management.

9.3.4 Review Meetings

- Fortnightly reviews for the during M1 and M2 (T1–T2), up to core go-live of the development phase.
- Monthly reviews thereafter during development and O&M phases.
- Trust has the right to call additional reviews as required.
- All meeting minutes shall be documented and shared with all parties by the Trust.

10. ELIGIBILITY CRITERIA

10.1 Pre-Qualification (PQ) Criteria

Bidders must fulfil all of the following PQ criteria to be eligible to submit a Technical Bid. Bidders failing to meet any single PQ criterion shall be disqualified.

Sl.	Criteria	Supporting Documents Required
1	The Bidder shall be a company registered under Companies Act 1956/2013 in India.	Certificate of Incorporation, MOA, AOA
2	The Bidder shall be in existence for **at least 10 Years** as on the date of submission of bid.	Certificate of Incorporation; Annual Reports
3	The Bidder shall have an average annual turnover of INR **100 Crores** or above from IT/ITES services during the **last 3 financial Years (FY 2023-24, 2024-25, 2025-26).**	Audited financial statements for last 3 Years; CA certificate.
4	The bidder shall have minimum one project completed in **digital Health IT application service worth of Rs.30 Cr** during the period **FY 2023-24, 2024-25, 2025-26**. **Or Two projects each with at least 15 Cr**. **Or Three projects each with at least 10 Cr** during the period **FY 2023-24, 2024-25, 2025-26**.	Work order/Work satisfaction/ Client certificate
5	The Bidder shall have a **minimum of 3 Years of Experience in digital Health IT application service** with any Government Organisation/PSU in India.	Work order/Work satisfaction/ Client certificate
6	The Bidder shall have a positive **net worth as of the last audited financial year 2025-26**.	Audited Balance Sheet; CA certificate
7	Mobile Application Development Experience: At least **one mobile application deployed and live at scale (minimum 5 lakh users)** to any Central/State Government body or PSU in India.	Work order/Work satisfaction/ Client certificate
8	The Bidder **shall not be under any insolvency proceedings,** winding up, or similar legal proceedings.	Self-declaration on company letterhead
9	The Bidder shall have a minimum of **100 full-time IT/ITES professionals on its rolls in India** (As on tender published date).	Certificate from HR/MD; EPF returns
10	The Bidder **shall not have been blacklisted or debarred** by any Central/State Government body or PSU in India in During the last 10 years.	Self-declaration on company letterhead
11	The Bidders company must be: **a.** The bidder must be CMMI Level 5 **b.** ISO 27001:2013 certified for Information Security Management.	Along with CMMI level 5 Certificate and all other certificates must be valid.

	c. ISO 9001:2015 (Quality Management) **d.** ISO 20000 (ITSM).	
12	**Insurance Transaction Management / HMIS Experience:** • **Insurance Transaction Management Experience** The Bidder shall have experience in implementing and operating an Insurance Transaction Management System for Central/State Government Department, PSU, private/public insurance organisation, or multiple or large chain of hospitals in India. The implemented system shall cover at least four (4) of the following functional areas: Hospital Empanelment, Pre-authorisation Management, Claims Management, Grievance Management, Claims Settlement/Accounts, Audit & Disciplinary Committee Workflow, and Dashboards & Reporting. • **HMIS Experience:** The Bidder shall have experience in implementing and operating at least one (1) live HMIS/Health Scheme Platform serving 500 or more active health facilities, with OPD, IPD, Laboratory Integration, Radiology Integration, Pharmacy Inventory Management, Discharge Management, and Payment Management as part of the platform. The platform shall support a seamless end-to-end digital workflow and integration across these modules, enabling information and transactions to flow electronically from one module to another without requiring duplicate data entry.	Work order and completion / go-live / client certificate listing modules and facility.
13	**Data Platform Experience:** The Bidder shall have successfully implemented and/or operated at least one (1) production-grade data platform for a Central/State Government Department, PSU, private/public insurance organisation, or hospital in India, handling both structured and unstructured data, and meeting all of the following minimum requirements: (i) supporting at least 10,000 concurrent users; (ii) managing at least 500 GB of structured data generated per year; and (iii) managing at least 80 TB of unstructured data, including images, PDFs, clinical photographs,	Client certificate stating concurrent users, annual structured volume and unstructured volume. *Self-certified figures shall not be accepted.*

	medical reports, and other healthcare-related documents.	

10.2 Technical Qualification (TQ) Criteria

Bidders meeting the PQ criteria shall be evaluated on the following Technical Qualification criteria. Minimum qualifying score for technical evaluation shall be 70 out of 100 marks.

Sl.	Criteria	Max Marks	Evidence Required
1	Value of the Project : The bidder must have been providing digital health services, i.e. Application Development and/or SaaS services, to Central and/or State Government organizations in India as of the bid calling date. Out of these, at least one engagement must be with a State Health Authority/ National Health Authority/Ministry of health delivering , during the last three financial Years (FY 2023–24, 2024–25, and 2025–26). Eligibility with 1 Project worth of 30 Cr- 10 Marks Eligibility with 2 Projects worth of 15 Cr- 8 Marks Eligibility with 3 Projects worth of 10 Cr- 6 Marks	**10**	Work Satisfactory/Completion certificates from client; Work order/agreement copy
2	e-Governance / Government IT Experience: The bidder must have successfully executed a minimum of three (3) e-Governance projects i.e. Application Development and/or SaaS services for Central and/or State Government organizations in India during the last three financial Years (FY 2023–24, 2024–25, and 2025–26). <= 2 Projects – 0 Marks 3-5 Projects – 4 Marks 6-7 Projects – 6 Marks 8-9 Projects – 8 Marks >= 10 projects – 10 Marks	**10**	Work order/Work satisfaction/ Client certificate
3	ABDM/PMJAY Ecosystem Experience: The bidder must have experience in developing and/or integrating applications with the Ayushman Bharat Digital Mission (ABDM), covering M1, M2, M3 implementation.	**05**	M1- M3: Work order/Work satisfaction/ Client certificate.
4	Mobile Application Development Experience: The bidder must have successfully deployed at least one (1) mobile application at scale, with a minimum of 5 lakh users, for Central and/or State Government organizations in	**05**	Work order/Work satisfaction/ Client certificate/App store links/deployment evidence; Client certificate

	India during the last three financial Years (FY 2023–24, 2024–25, and 2025–26). 1 application - 3 marks >1 application - 5 marks		
5	Experience in Working for Epidemics & Disasters: The bidder must have successfully provided IT services, including Application Development and/or SaaS services, to Central and/or State Government organizations in India for managing epidemics and/or natural disasters.	**05**	Client certificate; Architecture document
6	Team Strength and Key Personnel Qualifications: Curriculum Vitae (CVs) of key personnel demonstrating compliance with the requirements specified in the Tender.	**10**	CVs with certificates; Offer letters/appointment letters/PF returns
7	Medical Audit Expertise	**05**	CVs with certificates; Degree copies; Experience certificates from SHA/NHA; with PF returns/appointment letters.
	Insurance Transaction Management / HMIS Experience The Bidder must have successfully implemented and operated at least one (1) Insurance Transaction Management System / HMIS for a Central/State Government Department, PSU, private/public insurance organisation, or hospital in India, covering the specified functional areas and meeting the prescribed HMIS requirements, during the last three financial years (FY 2023–24, 2024–25, and 2025–26).	**10**	Work order and completion / go-live / client certificate listing modules and facility.
	Data Platform Experience: The Bidder must have successfully implemented and/or operated at least one (1) production-grade data platform for a Central/State Government Department, PSU, private/public insurance organisation, or hospital in India, handling both structured and unstructured data and supporting at least 10,000 concurrent users, 500 GB of structured data generated per year, and 80 TB of unstructured data, during the last three financial years (FY 2023–24, 2024–25, and 2025–26).	**10**	Client certificate stating concurrent users, annual structured volume and unstructured volume.
8	**Proposed Solution Quality & POC Demonstration (30 marks)** The technical proposal shall be evaluated on quality, including overall architecture design, module coverage, integration approach and security architecture. The proposed solution	**30**	Technical Proposal Document

	must be fully developed, operational and demonstrable (not conceptual). It shall include edge-optimised facial recognition capable of offline execution, ensuring low-latency authentication without persistent cloud connectivity. It shall also support real-time capture and conversion of doctor–patient conversations in English, Telugu and Hindi, with direct real-time mapping into FHIR-compliant structured data through a managed healthcare-standard API, without third-party orchestration or custom data-shaping middleware. **Approach & Methodology Evaluation (15 marks):** Understanding of the Trust's workflow, objectives and requirements, healthcare ecosystem, implementation strategy, execution methodology, project governance, risk-mitigation approach, resource-deployment plan, delivery timelines, quality-assurance framework, and overall capability to deliver the proposed solution. **Technology & Solution Architecture (15 marks):** Proposed technology stack, solution architecture, scalability, security, performance, interoperability, integration capabilities, compliance with applicable standards, innovation, maintainability, and future scalability of the proposed solution.		

Note:

1. Weightage will be QCBS 70:30 and the 70 marks absolute cut-off.

2. The Technical Score shall be calculated out of 100 Marks. Only Bidders securing a minimum Technical Score of 70 Marks shall be considered technically qualified for Financial Evaluation.

3. The evaluation shall be based only on the criteria and documentary evidence specified in this RFP.

4. The same project shall not be counted more than once under the same evaluation criterion.

5. Where a project satisfies multiple independent technical evaluation criteria, the project may be considered under each such criterion only where the relevant scope and documentary evidence independently demonstrate compliance with that criterion.

6. The Trust may seek clarification regarding documents submitted by the Bidder; however, such clarification shall not be used to introduce new experience, materially modify the submitted proposal or cure a material omission.

7. The Bidder shall demonstrate the proposed solution based on the requirements identified by the Trust. The proposed solution shall be fully developed, operational and demonstrable for the specified workflows and shall not be merely conceptual.

8.The demonstration may include, but shall not be limited to, the following core workflows:

i. Beneficiary registration and verification;

ii. Hospital/Provider empanelment and management;

iii. Pre-authorisation workflow;

iv. Claims submission, processing and adjudication workflow;

v. Medical audit workflow;

vi. Rule-based fraud/risk identification and workflow;

vii. Grievance management;

viii. Package/rate and master-data management;

ix. Dashboards and management reporting;

x. API and system integration;

xi. Role-based access control and user management; and

xii. Audit trail and transaction history.

11. BID EVALUATION – QCBS METHOD

- The bids shall be evaluated using the Quality and Cost Based Selection (QCBS) methodology with a weightage of 70% for Technical Evaluation and 30% for Financial Evaluation.
- The evaluation shall be carried out in the following stages.

11.1 Evaluation of the Qualification Bid

- The Qualification Bids shall first be evaluated for responsiveness to the Tender Documents and fulfilment of the Pre-Qualification criteria based on the following parameters:

a) The Bid is complete in all respects and submitted in the prescribed formats.

b) It contains no material alterations, conditions, deviations or omissions which materially affect the requirements of the RFP.

c) All documents required as specified in the Tender Documents and submitted by the Bidder are appropriate and valid.

d) All undertakings required under this Tender Document are in the prescribed format and unconditional.

e) Based on the review of the documents, the TIA concludes that the Bidder fulfils the minimum qualification criteria specified under .

f) The Bidder has submitted the required documentary evidence in support of the qualification criteria.

Only Bidders meeting the requirements of above shall be considered for Technical Evaluation.

Technical Evaluation:

- The Technical Proposals of the technically responsive and PQ-qualified Bidders shall be evaluated against the Technical Qualification criteria specified above.
- The Technical Proposal shall be evaluated for a maximum of 100 Marks.
- Only Bidders obtaining a minimum Technical Score of 70 Marks shall be considered technically qualified and shall proceed to Financial Evaluation.
- The Technical Evaluation shall be based only on the criteria, weightages, documentary evidence and methodology specified in this RFP.

Technical Evaluation Principles:

- The following principles shall apply during Technical Evaluation:

a) The evaluation shall be carried out strictly in accordance with the criteria and weightages specified above.

b) No new evaluation criterion or additional scoring parameter shall be introduced after opening of the bids.

c) Documentary evidence submitted by the Bidder shall form the basis for evaluation of past experience and eligibility.

d) The same project shall not be counted more than once under the same evaluation criterion.

e) Where clarification is sought, the clarification shall be limited to information already contained in the submitted bid or documentary evidence and shall not result in a material modification of the bid.

f) All Bidders shortlisted for POC/demonstration shall be evaluated against the same POC protocol, use cases and evaluation methodology.

Financial Evaluation:

- Only those Bidders who obtain a minimum Technical Score of 70 Marks shall be considered for Financial Evaluation.
- The Financial Bids shall be examined for:

a) Completeness of the Financial Bid;

b) Compliance with the prescribed Financial Bid format;

c) Arithmetic correctness;

d) Consistency between the Financial Bid and the requirements of the RFP;

e) Applicability and treatment of taxes as specified in the Financial Bid;

f) Any material conditionality, deviation or qualification affecting the commercial validity of the bid; and

g) Any other requirement specified under specific section – Financial Bid Structure.

- A Financial Bid containing a material condition, qualification, deviation or unquantifiable financial implication may be considered non-responsive.

Evaluated Financial Bid:

- The Evaluated Financial Bid (EFB) shall be the total financial amount considered for comparison of Bidders in accordance with the Financial Bid structure specified in the Tender.
- For the purpose of financial comparison, all Bidders shall be evaluated on a uniform basis. Applicable taxes shall be treated in accordance with the Financial Bid instructions specified in the Tender

Financial Score:

- The Financial Score shall be calculated using the following formula:
- Financial Score (FS) = (Lowest Evaluated Financial Bid / Bidder's Evaluated Financial Bid) × 100
- The Bidder quoting the lowest Evaluated Financial Bid shall be assigned a Financial Score of 100.
- The Financial Score of other technically qualified Bidders shall be calculated proportionately using the above formula.

Final Evaluation – QCBS 70:30

- The final evaluation shall be carried out using the following formula:
- Combined Score = (Technical Score × 70%) + =(Financial Score × 30%)

  Where:

- Technical Score = Score obtained by the Bidder in Technical Evaluation out of 100.
- Financial Score = Score obtained by the Bidder in Financial Evaluation out of 100.
- The Bidder obtaining the highest Combined Score shall be considered for award of the contract, subject to fulfilment of all other requirements, conditions and provisions of this RFP.

Tie in Combined Score:

- In the event that two or more Bidders obtain the same Combined Score, the following order shall be followed:

  a) The Bidder obtaining the higher Technical Score shall be ranked higher.

b) If the Technical Scores are also identical, the Bidder having the lower Evaluated Financial Bid shall be ranked higher.

c) If the tie still remains unresolved, the matter shall be dealt with in accordance with the applicable procurement rules/guidelines and the decision of the competent authority.

12. SERVICE LEVEL AGREEMENT (SLA)

This SLA covers Application Development, production application behaviour attributable to the application layer, and Operations & Maintenance of the application. Availability and performance metrics below apply only to defects, regressions, misconfiguration of the application, failed releases, or O&M lapses by the Service Provider.

12.1 Application Availability and Quality SLA

Measured on the production application during the agreed business window, excluding scheduled maintenance approved by the Trust and excluding infrastructure-caused events.

Metric	Target SLA	Penalty Zone	Penalty
Application service availability (application-layer; production)	99.5% per month	99.0% – 99.5%	1% of Quarterly invoice
Application service availability (application-layer; production)	99.5% per month	< 99.0%	2% of Quarterly invoice per 0.1% shortfall below 99.0%
Page response time (application processing, P95, excluding network/infra latency)	< 3 seconds	> 3 seconds attributable to application code or queries	Warning; repeat breach in consecutive months = 3% of Quarterly invoice
API response time (application processing, P95, excluding network/infra latency)	< 2 seconds	> 2 seconds attributable to application code or queries	Warning; repeat breach in consecutive months = 3% of Quarterly invoice
Mobile app crash	< 0.1% of sessions	> 0.1%	3% of Quarterly invoice

Metric	Target SLA	Penalty Zone	Penalty
rate (application defect, not device/OS/store)			
Failed production release / rollback caused by application defect	Zero unplanned rollback per month	Each unplanned rollback	1% of Quarterly invoice per incident
Critical functional defect escaping to production	Zero open P1 functional defects beyond resolution SLA	Each P1 functional defect breaching resolution SLA	As mentioned in the Tender

12.2 Incident Resolution SLA (Application)

Clock starts from logging in the Service Provider's ticketing tool (or Trust-notified channel) for incidents whose root cause is the application, a release, data handled by the application, or O&M process. Infrastructure-only incidents are logged, triaged and handed to the infrastructure owner; they do not accrue application resolution penalty.

Severity	Description	Resolution Time	Penalty for Breach
Critical (P1)	Production application down or unusable for all users due to application defect, bad release or data corruption introduced by the application	4 hours	2% of quarterly invoice per hour of delay
High (P2)	Major module / workflow down; significant business impact; > 50% of affected user group unable to complete a core transaction due to application defect	8 hours	2% of quarterly invoice per hour of delay

Severity	Description	Resolution Time	Penalty for Breach
Medium (P3)	Module or feature degraded; moderate business impact; workaround may exist	2 working days	1% of quarterly invoice per working day of delay
Low (P4)	Minor application issue; minimal business impact; workaround available	5 working days	Warning notice; repeat breach in the same quarter = 1% of quarterly invoice per working day of delay

12.3 Requirement, Defect Fix and Enhancement SLA

Applies during Development (post-SRS approval) and O&M. Effort bands are estimated by the Service Provider and confirmed by the Trust. Timelines exclude Trust review/approval wait time.

Change / Request Type	Delivery Timeline	Notes
Critical-path production bug (< 0.5 man-days)	Within 8 working hours of confirmation	Hotfix on the live application; included in O&M
Minor bug fix (0.5 – 3 man-days)	Within 3 working days	Included in O&M scope
Support / small enhancement (up to 3 man-days)	Within 5 working days	Included in O&M scope
Small enhancement (3 – 10 man-days)	Within 10 working days	Included in O&M scope; requires Trust confirmation of scope
Medium enhancement (10 – 30 man-days)	As decided by the Trust in writing	Requires SRS / design approval; scheduled into a release
New module / large enhancement (> 30 man-days)	As decided by the Trust in writing	Separate SOW with Trust approval; not part of standard O&M effort band

12.4 Delivery Delay Penalties

- For deliverables delay beyond the scheduled end of T1 to T5 for the corresponding Milestone M1 to Final Sign Off of the Development Phase attributable solely to the Service Provider, a penalty of 0.5% of the implementation-phase contract value per day of delay shall be levied.

The maximum cumulative penalty for implementation-phase delays shall be capped at 10% of the implementation-phase contract value.

- For delays in requirement / enhancement / defect-fix deliverables during O&M attributable solely to the Service Provider, a penalty of 0.5% of the quarterly invoice per day of delay for each such item shall be levied. The maximum cumulative penalty for O&M-phase requirement delays shall be capped at 20% of the quarterly invoice amount.
- Delay attributable to pending Trust inputs, infrastructure unavailability, third-party systems outside the Service Provider's control, or approved change in scope shall not attract penalty, provided the Service Provider has notified the delay in writing with evidence.

12.5 Key Performance Indicators (KPIs)

The following application development and maintenance KPIs shall be tracked monthly and reviewed in governance meetings. Persistent failure (below target for two consecutive quarters) shall constitute an Event of Default.

Sl.	KPI	Target	Penalty for Breach
1	Application-layer service availability	>= 99.5% per month	As mentioned in the Tender
2	P1 application incident resolution within SLA	100%	2% of quarterly invoice per hour per P1 incident beyond SLA
3	P2 application incident resolution within SLA	>= 95%	2% of quarterly invoice per hour per P2 incident beyond SLA
4	On-time delivery of Trust-approved requirements / enhancements	>= 90% within agreed timeline	1% of quarterly invoice per day per delayed requirement (O&M); as mentioned in the Tender for Development milestones
5	Critical application / dependency security patch in Service Provider's code or libraries	Within 48 hours of confirmed applicability (or next agreed release if Trust so directs)	2% of quarterly invoice per day of delay
6	CERT-In audit certificate before complete go-live (FINAL SIGN-	100% compliance	Production release of the affected application scope

Sl.	KPI	Target	Penalty for Breach
	OFF) and annually thereafter, or as required by the Trust for a major application release		blocked until certificate obtained. Related milestone / O&M payments withheld until obtained.
7	Monthly operational report (application uptime as measured, incidents, releases, pending CRs, team attendance)	By 5th working day of the following month	Warning; repeat breach in consecutive months = 0.1% of quarterly invoice
8	Agreed on-site / dedicated application O&M team strength	As specified in the RFP manpower schedule during O&M	1% of quarterly invoice per resource shortfall per day
9	SLA monitoring dashboard for application KPIs in the Tender.	Available before core go-live (M2) and complete before full go-live (FINAL SIGN-OFF)	Related payments withheld until the monitoring tool is delivered and accepted
10	Release quality — defects found in production within 7 days of an application release	<= 2 P1/P2 defects per major release	1% of quarterly invoice per excess P1/P2 production defect
11	UAT defect closure before a planned production release	100% of P1 and P2 UAT defects closed or waived in writing by the Trust	Release shall not proceed; delay treated in the Tender if attributable to the Service Provider

12.6 Measurement, Exclusions and Cap

- Final target SLA values shall be baseline-calibrated and mutually agreed after core go-live (M2), using one calendar month of production application telemetry. Until that baseline is signed, the targets in this section apply.
- Measurement is monthly and reviewed in the monthly governance meeting. Application telemetry, APM, logs and the ticketing tool of the Service Provider (accessible to the Trust) are the system of record.
- Excluded from application availability and response-time measurement: Trust-approved planned maintenance; infrastructure / network / identity-provider / third-party outages; force

majeure; defects in Trust-supplied data or upstream systems; user-side device or connectivity issues.

- The Service Provider shall still log, notify and provide application-side workarounds during excluded events.
- Penalties under this section are subject to the overall Penalty Cap in the RFP.
- The maximum total penalty in any given quarter shall be limited to 20% of the quarterly invoice amount for that period.

13. CONTRACT TERMS

13.1 General Conditions of Contract

13.1.1 Contract Duration

- The contract shall be for a total period of 6 months (Development Phase) + 5 Years (O&M Phase), commencing from the date of contract execution.
- The O&M phase may be extended by up to 2 additional Years at the sole discretion of the Trust, subject to satisfactory performance.
- In case of extension, the O&M costs for the extended period shall be as quoted in the financial bid.

13.1.2 Contract Execution

- The selected Bidder shall execute a formal contract with the Trust within 7 days of issuance of Letter of Intent (LoI).
- The contract shall incorporate this RFP, the selected Bidder's technical and financial proposals, and any addenda issued.
- The Bidder shall provide a Performance Bank Guarantee (PBG) as specified in the contract before commencement.

13.1.3 Governing Law

- Any disputes arising out of or touching this contract shall be decided by courts or tribunals situated at Guntur District of AP only. No suit or other proceedings shall be institute elsewhere.

13.1.4 Termination

Events constituting default and grounds for termination include:

- KPI performance below target for 2 consecutive quarters.
- Proven fraud committed by the Bidder or its employees.
- Failure to deploy minimum onsite team without prior approval.

- Material breach of contract terms not rectified within 30 days of notice.
- The Bidder being adjudged insolvent or winding-up proceedings initiated.
- Abandonment of project office or being non-contactable.
- Any representation or warranty found to be materially false or misleading.

13.2 Special Conditions of Contract

13.2.1 Confidentiality

- The Bidder shall treat all information received from the Trust, including beneficiary data, claim data, financial data, and operational data, as strictly confidential.
- No data shall be shared, sold, or disclosed to any third party without prior written consent from the Trust.
- Confidentiality obligations shall survive for 5 Years after expiry or termination of the contract.
- The Bidder shall ensure all its sub-contractors, employees, and agents are bound by equivalent confidentiality obligations.

13.2.2 Data Ownership

- All data generated, collected, or processed under this contract shall be the exclusive property of the Trust and the Government of Andhra Pradesh.
- Upon expiry or termination of the contract, all data shall be returned to the Trust in agreed formats within 30 days.
- The Bidder shall not retain any copies of Trust data after contract termination.

13.2.3 Intellectual Property Rights (IPR)

- All software developed under this contract, including source code, documentation, test cases, and designs, shall vest exclusively with the Dr Nandamuri Taraka Ramarao Vaidya Seva Trust.
- The Trust shall be the sole owner of all IPR for the custom-developed software.
- The Bidder shall not use any component of the software developed for the Trust for any other client or purpose.
- Open-source components used shall be compliant with applicable open-source licenses.
- At the end of the contract period or as and when requested by Trust, the Bidder shall hand over the latest and updated source code with all version history and documentation.

13.2.4 Continuous Service Obligation

- In the event of any service interruption, the Bidder shall ensure business continuity and provide an alternate mechanism to maintain cashless access services.
- The Bidder shall furnish a detailed business continuity and disaster recovery plan within 30 days of contract signing.

- The Bidder shall conduct DR drills at least once every 6 months and submit DR drill reports to Trust.

13.2.5 Exit Management

- At the end of the contract, or upon early termination, the Bidder shall provide comprehensive exit management support for a period of up to 6 months.
- Exit management includes: complete knowledge transfer, documentation handover, data migration support, and transition support to the successor vendor.
- The cost of exit management support shall be included in the Bidder's financial bid.

14. FINANCIAL BID STRUCTURE

14.1 Financial Bid Components

The Financial Bid shall provide a comprehensive cost breakup for the entire project duration. All costs shall be in Indian Rupees (INR), inclusive of applicable taxes.

Sl.	Cost Component	Details
1	**Design, Development, Implementation Cost (Lump Sum)**	All costs for design, development, testing, data migration, UAT, deployment, training, and go-live. Includes cost of all deliverables specified in the Tender.
2	**O&M Cost per year (for 5 Years) + 2 years (Extendable)**	Annual cost for O&M team (onsite), support, maintenance, enhancements, and change requests per O&M scope.
3	**Cloud Migration cost (Pre and Post charges)**	Cost for migrating from the current cloud to the Trust desired location.

14.2 Payment Schedule - Development Phase

Sl.	Milestone / Deliverable	Payment %	Conditions
1	Contract Signing and Project Kick-off at T1 initiation of milestone M1	**10%**	Submission of PBG; execution of contract.
2	AS-IS Study, SRS Sign-off at T1, milestone M1	**5%**	Approval of all deliverable by Trust
3	Core Module Development, Deployment and Go-Live (TMS, Empanelment, HBP) - Completion after T2, milestone M2	**20%**	Successful sign-off of milestone M2.
4	All Modules Development Completion - SIT Completion after T3, milestone M3	**10%**	Successful completion sign-off for all modules
5	Mobile Apps + Integration – SIT, Completion after T4, milestone M4	**20%**	Successful SIT and integration test sign-off

6	UAT Completion, CERT-In Audit Certificate, Data Migration, Go-Live after T5, milestone final sign off.	**15%**	UAT sign-off; CERT-In certificate; Go-Live report
7	Stabilization (3 months post Go-Live) during T6, milestone 0&M phase. These 3 months are post the 6 months of developmental phase.	**20%**	No P1/P2 incidents in stabilization period; all open items resolved.

14.3 Payment Schedule - O&M Phase

O&M cost shall be paid on a quarterly basis in arrears, subject to satisfactory performance as measured against the SLAs. Penalty deductions (if any) shall be applied before each quarterly payment.

14.4 Notes on Financial Bid

- Costs shall be quoted in INR, inclusive of applicable taxes. Taxes shall be stated separately.
- The Bidder shall bear the cost of all licenses required for the proposed solution, including databases, middleware, operating systems, and other software. All such licenses shall be included in the Bid Price. Perpetual licenses, wherever applicable, shall be procured in the name of Dr. NTR Vaidya Seva Trust (Dr. NTRVST). The Bidder shall clearly specify in the bid the details of all licenses included, including their type and validity.
- The Trust shall not bear any additional cost not quoted in the Financial Bid.

15. DATA PROTECTION AND INTELLECTUAL PROPERTY RIGHTS

15.1 Data Protection Framework

The Service Provider shall implement a comprehensive data protection framework aligned with:

- NHA Health Data Management Policy.
- HIPAA (Health Insurance Portability and Accountability Act) standards.
- GDPR principles for data privacy.
- Andhra Pradesh Legislature Portal Privacy Policy.
- Digital Personal Data Protection Act, 2023 (DPDPA) and rules thereunder.
- Any further legislation enacted by the Government of Andhra Pradesh or Government of India during the contract period.

15.2 Data Privacy Requirements

- All beneficiary data, health data, and financial data shall be treated as sensitive personal data.

- Data collection shall be limited to what is strictly necessary for scheme operations (data minimization principle).
- Beneficiary consent shall be obtained before collection and processing of health data.
- Data localization: all data shall be stored only on servers physically located within India.
- Data retention policies shall comply with applicable legal requirements and Trust guidelines.
- Data anonymization/pseudonymization for analytics and reporting purposes.
- Right to access and right to correction provisions for beneficiaries.

15.3 Intellectual Property Rights

All intellectual property created under this contract shall vest exclusively with the Dr Nandamuri Taraka Ramarao Vaidya Seva Trust:

- Custom-developed source code, documentation, databases, and data models.
- All business process designs, workflow configurations, and integration specifications.
- All reports, dashboards, and analytical models developed for the Trust.
- Training materials and user manuals.

Open-source software components shall be used in compliance with their respective licenses. The Bidder shall maintain a Bill of Materials (BOM) of all open-source components used, with version numbers and applicable licenses, and keep it updated throughout the project.

16. ADDITIONAL OPERATIONAL REQUIREMENTS

16.1 Helpdesk Services

The Service Provider shall provide a comprehensive IT helpdesk service available throughout the contract period. The helpdesk shall:

- Handle all queries, errors, incidents, and issues for both front-office (hospital users, field staff) and back-office (Trust officials) users.
- Define Standard Operating Procedures (SOPs) with call prioritization, severity codes, and escalation procedures.
- Track and route all service requests with severity level assignment.
- Notifying users of problem status and resolution through tickets, email, and SMS.
- Deploy a request tracking/helpdesk tool accessible to Trust officials for monitoring.
- Trust may audit call recordings to improve quality.

16.2 Training Requirements

- Provide exhaustive training to Trust officials, hospital staff (Vaidya Mithra, MEDCO, Hospital Administrator, MS), district coordinators, and field staff.
- Training shall be role-based and cover all modules relevant to each role.
- E-learning materials in the form of short videos (5-10 minutes), PowerPoint presentations, and PDF training guides shall be made available in English and Telugu.
- Training workshops at hospital premises for all empanelled hospitals at a core go-live milestone M2 and full go-live after final sign off and once every 6 months thereafter.
- Refresher training for all new features deployed during O&M phase within 2 weeks of go-live of the feature.
- Training for Mithras at each Sub-District Hospital, District Hospital, Medical College, and Network Hospital.

16.3 Version Control and Code Management

- Implement Git-based version control management from day one.
- Maintain complete version history with meaningful commit messages and release tags.
- At the end of contract period or as and when requested by Trust, hand over the latest and updated source code with all version history and comprehensive documentation.
- Branching strategy: minimum main, develop, release, and hotfix branches.

17. AS-IS STUDY

17.1 AS-IS Assessment

The Service Provider shall conduct a detailed AS-IS study covering:

- Detailed study of all scheme guidelines, geographic coverage, type of benefit, type of beneficiaries, and operational workflows.
- Interaction with Trust employees, officials, field staff, hospital staff, and beneficiaries to understand key issues, pain points, and improvement areas.
- Facilitation of stakeholder consultations to obtain feedback on problem areas, process gaps, and roles and responsibilities.
- Analysis of all data collected during field study and stakeholder consultations.
- Identification of all processes behind the services and assessment of bottlenecks and performance gaps.
- Review of current application architecture, technology stack, database structure, and integration landscape.
- Documentation of existing workflows, user roles, and access control structures.

17.2 To-Be Process Design

Based on the AS-IS study, the Service Provider shall design the To-Be processes:

- List all processes for all prioritized services and identify core/common processes for re-engineering.
- Design process maps, process metrics, and service levels for all re-engineered processes.
- Design optimum workflow structure with approval hierarchies.
- Re-engineer citizen interface for improved experience.
- Design interfaces with all external entities and systems.
- Balance process re-engineering effort with feasibility of implementation.
- Recommend re-alignment of organizational efforts where feasible for optimum outcomes.

17.3 BPR Deliverables by the Trust

- Detailed AS-IS Report documenting current state processes, gaps, and issues.
- To-Be Report documenting proposed improved processes and rationale.
- Business Process Re-engineering (BPR) Report with all process maps, workflows, and service level definitions.
- BPR report shall be reviewed and approved by Trust before commencement of development.

18. DATA MIGRATION

The complete migration of data from the legacy system to the new application suite is the sole responsibility of the Service Provider. This includes:

18.1 Scope of Data Migration

- Structured data: approximately 5 TB across 5,000+ database tables in Oracle (current production database).
- Unstructured data (documents): approximately 300 TB on NAS storage, with annual growth of approximately 80 TB.
- All historical transaction data: registrations, pre-authorizations, claims, grievances, empanelment records, and payment records.

18.2 Data Migration Activities

- It is the responsibility of the Service Provider to migrate the data (Structured and Un-Structed data) from existing service provider to Trust desired location.
- Knowledge transfer from existing vendor to understand complete data structure, business logic, and data quality issues.
- Data profiling and quality assessment of existing data.
- Data cleaning and standardization: address duplicates, incomplete records, and inconsistent coding.
- Data transformation to match new application data model and healthcare standards (ICD codes, LGD codes, etc.).
- Legacy Data Migration scripts development and dry-run in lower environments.
- Data validation and reconciliation: row counts, financial totals, and sample-based quality checks.
- Go-live migration with minimal downtime plan.
- Post-migration validation and sign-off by Trust.

18.3 Data Integrity Obligations

- Maintaining data integrity is the prime responsibility of the Service Provider throughout migration.
- All data corrections shall be tracked and reported to Trust.
- Impact analysis shall be performed before any data correction to ensure no unintended consequences.
- Migration reports shall be submitted to Trust for review before each migration phase.

19. MONITORING AND PERFORMANCE REVIEW

19.1 Scope of Monitoring

Monitoring under this contract shall include supervision and monitoring of all activities undertaken by the Service Provider, ensuring compliance with all provisions of the contract. Monitoring shall cover:

- Overall performance and conduct of the Service Provider and its team.
- Claims management and transaction processing capability and quality.
- Grievance redressal process and TAT compliance.
- Application availability, performance, and security.
- Adherence to SLAs defined in this RFP.
- Compliance with ABDM, PMJAY, and other national digital health guidelines.

19.2 Monitoring Activities of the Service Provider

The Service Provider shall cooperate with the Trust in effective monitoring and shall undertake:

- Ensure compliance with all terms, conditions, and provisions of the contract.
- Ensure monitoring of processes for seamless access to cashless health services.
- Ensure timely processing and management of all scheme transactions.
- Fulfil obligations as per agreed KPIs on an ongoing basis.
- Ensure compliance from all sub-contractors, vendors, and intermediaries.

19.3 Performance Review Meetings

- Fortnightly review meetings for the first 3 months; monthly thereafter.
- Quarterly review presentations to PMC.
- Trust has the right to call interim review meetings on specific issues.
- Agenda shall include: review of action taken from previous meeting, KPI results with variance analysis, risk review, fraud alerts, and any contract management issues.
- All meetings shall be documented; minutes shared with all parties within 3 working days.

20. EVENTS OF DEFAULT AND REMEDIES

20.1 Events of Default - Service Provider

The following events shall constitute Events of Default for the Service Provider:

1. Intentional or unintentional act of undisputedly proven fraud by the Service Provider or its employees.
2. Failure to perform or discharge obligations under the contract without valid Force Majeure justification.
3. Successive infringement of contract terms without rectification within the notice period.
4. Arrears in payment of any penalty, charge, or lien specified in the contract.
5. False or misleading representation or warranty.
6. Engaging in any activity prohibited by law or constituting a breach of applicable statutes.
7. Adjudication as bankrupt or initiation of insolvency proceedings.
8. Winding up order by a court of competent jurisdiction.
9. Abandonment of the project office or being non-contactable.
10. Material data breach resulting from Service Provider's negligence.

20.2 Notice and Rectification

For Events of Default (other than fraud), the Trust shall issue a rectification notice providing 30 days for the Service Provider to remedy the default. Failure to remedy within 30 days shall entitle the Trust to terminate the contract with the full settlement as on date of termination.

20.3 Penalty Cap

The maximum total penalty amount in any given period shall be limited to the **20%** of the invoice amount for that particular period.

20.4 Force Majeure

Force Majeure events (natural disasters, war, pandemic, government-imposed restrictions, etc.) shall be documented and notified to the Trust within 7 days of occurrence. The Service Provider shall take all reasonable steps to minimize the impact and restore services within the shortest possible time. Compensation claims during Force Majeure periods shall be negotiated in good faith.

21. Compliance to be maintained

21.1 Compliance

The Service Provider shall ensure the following compliance be maintained throughout the contract period:

Requirement	Details	Timeline
CERT-In Security Audit	From CERT-In empanelled agency; covering code, database, APIs, and functionality	Before production deployment, Every 6 months during O&M
GIGW Compliance	All government web portals must comply with Guidelines for Indian Government Websites	Before go-live
ABDM Milestone Compliance	M1, M2, M3,M4 milestones as per ABDM framework	As per ABDM mandated timelines
WCAG 2.0 Compliance	Level AA for all citizen-facing applications	Before go-live

Note: All the above security parameters will be done by the audit agency identified by the Trust and the bidder should be responsible for fixing all the vulnerabilities identified.

21.2 Vulnerability Management

- All critical vulnerabilities identified by CERT-In, Trust, or any authorized body shall be fixed within 24 hours.
- High severity vulnerabilities shall be fixed within 72 hours.
- Medium severity vulnerabilities shall be fixed within 7 working days.
- All vulnerability fixes shall be regression-tested before deployment.
- Vulnerability status reports shall be shared with Trust as part of monthly reporting.

ANNEXURES

Annexure 1: Current Application Architecture (Overview)

The existing Dr Nandamuri Taraka Ramarao Vaidya Seva Trust application suite operates on the following architecture:

Component	Current Technology
Operating System	Linux
Application Server	JBoss
Frontend	JSP (Java Server Pages)
Database (RDBMS)	Oracle
Scheduler	Crontab
Reporting	Custom Built
Mobile Application	Flutter
Architecture Style	Monolithic
Number of VMs	Approximately 70

Note: The detailed current application architecture diagram shall be shared with shortlisted bidders during the pre-bid conference and upon execution of a Non-Disclosure Agreement (NDA).

Annexure 2: Current Database Statistics

Parameter	Details
Structured Data (RDBMS)	Approximately 5TB
Number of Database Tables	Approximately 5000+
Unstructured Data (NAS Storage)	Approximately 300 TB
Annual Incremental Storage Growth	Approximately 80 TB per year
Current Concurrent User Base (Dr NTRVS)	Approximately 1,50,000
Current Concurrent User Base (EHS)	Approximately 1,00,000
Current Concurrent User Base (WJHS)	Approximately 20,000
Internet Bandwidth	More than 1 Gbps (current)
No. of physical servers	6
No. of virtual Machines	70+

Annexure 3: Schemes - User Base and Module Coverage

Scheme	Current Concurrent Users (Max)	Active Modules
Dr Nandamuri Taraka Ramarao Vaidya Seva	1,50,000	Empanelment, Operations/TMS, Grievance, Medical Audit, Accounts, Health Camps
Employees Health Scheme (EHS)	1,00,000	Empanelment, Operations/TMS, Medical Reimbursement, Grievance
Working Journalists Health Scheme (WJHS)	20,000	Empanelment, Operations/TMS, Grievance
Medical Reimbursement	Included in EHS	Medical Reimbursement Module

Annexure 4: Indicative Workflow Reference Points – (Attachment-1)

The following are indicative workflow reference areas for the Service Provider's reference during the AS-IS study and BPR phase. Detailed workflow documents shall be shared with the shortlisted Bidder upon execution of NDA.

- Patient registration and beneficiary verification workflows.
- Pre-authorization initiation, PPD processing, and approval/rejection workflows.
- Enhancement and resubmission workflows.
- Discharge and claim submission workflows.
- Claims payment processing and RTGS workflows.
- Grievance registration and resolution workflows.
- Medical audit scheduling and reporting workflows.
- Hospital empanelment, renewal, and de-empanelment workflows.
- Field staff performance monitoring and incentive payment workflows.
- Medical reimbursement claim submission and approval workflows.
- IVRS-based beneficiary feedback workflows.

Annexure 5: Compliance and Standards Reference

Standard/Guideline	Reference/Issuing Authority
ABDM Guidelines (M1, M2, M3, M4)	National Health Authority (NHA), Government of India
PMJAY HEM 2.0	National Health Authority (NHA), Government of India
PMJAY TMS 2.0	National Health Authority (NHA), Government of India
PMJAY HBP 2022	National Health Authority (NHA), Government of India
PMJAY SAFU Guidelines	National Health Authority (NHA), Government of India
EHR Standards	National Health Authority (NHA), Government of India
FHIR Release 4	HL7 International
ICD-10 / ICD-11	World Health Organization (WHO)
SNOMED-CT (with India Extension)	SNOMED International / NHA
LOINC	Regenstrief Institute
LGD Codes	Ministry of Panchayati Raj, Government of India
GIGW	Ministry of Electronics and Information Technology (MeITY)
CERT-In Guidelines	Indian Computer Emergency Response Team (CERT-In), MeITY
WCAG 2.0	World Wide Web (W3C)
Aadhaar Authentication (AUA/KUA)	Unique Identification Authority of India (UIDAI)
NHA Health Data Management Policy	National Health Authority (NHA), Government of India

Annexure 6: Bid Submission Checklist

Bidders are advised to use this checklist to ensure completeness of their submissions:

Sl.	Document / Requirement	Enclosed (Y/N)	Page Reference
1	Covering letter on company letterhead (signed by authorized signatory)		
2	Board resolution/Power of Attorney for authorized signatory		
3	Certificate of Incorporation		
4	Financial Capability Details		
5	MOA and AOA		
6	Audited financial statements (last 3 Years)		
7	CA certificate for annual turnover		
8	CA certificate for net worth		
9	Self-declaration on blacklisting/debarment		
10	Self-declaration on no insolvency proceedings		
11	EPF returns / HR certificate for full-time staff strength		
12	Technical proposal document		
13	Proposed architecture design		
14	Compliance matrix against all functional requirements		
15	CVs of all key personnel with certificates		
16	Client completion certificates for all claimed projects		
17	Work orders for all claimed projects		
18	Any other documents defined in the RFP		

Model Form of Contract Agreement

This contract agreement is made on the *[insert number]* day of *[insert: month]*, *[insert: year]*.

Between

(1) *[insert: Name of Client]*, (hereinafter called “the Client”), and

(2) *[insert: name of the bidder]*, (hereinafter called “the Service provider”).

Whereas the Client desires to select a Service Provider for “Design, Development, Implementation with end-to-end Maintenance of Dr Nandamuri Taraka Ramarao Vaidya Seva (Dr NTRVS) Application Suite with existing Website and have agreed to such engagement upon and subject to the terms and conditions appearing below in this Contract Agreement.

NOW IT IS HEREBY AGREED as follows:

1. Article 1 - Contract Documents

1.1 *Contract Documents*

The following documents shall constitute the Contract between Dr Nandamuri Taraka Ramarao Vaidya Seva Trust and the Service Provider, and each shall be read and construed as an integral part of the Contract:

This Contract Agreement and the Appendices attached to the Contract Agreement.
(a) Notification of Award
(b) The Bid Price quoted by the bidder
(c) Special Conditions of Contract
(d) General Conditions of Contract
(e) Bid document with modification if any
(f) *Any other documents*

1.2 *Order of Precedence*

In the event of any ambiguity or conflict between the Contract Documents listed above, the order of precedence shall be the order in which the Contract Documents are listed in the agreement.

1.3 *Definitions* (Reference GCC Clause 1)

Capitalized words and phrases used in this Contract Agreement shall have the same meanings as are ascribed to them in the General Conditions of Contract.

2. Article 2 - Contract Price and Terms of Payment

2.1 *Contract Price*

The Client hereby agrees to pay to the Service Provider an amount of *Rs.**Xxxx/-* (to be filled at the time of award) for the scope of work mentioned in the RFP &resources mentioned in the Commercial Form. The Contract Price in consideration of the performance by the Service Provider of its obligations under the Contract.

3. Article 3 - Effective Date for Determining Time for Operational Acceptance

3.1 *Effective Date*

The time allowed for execution, delivering deliverables and Acceptance of the same should be determined from the date when all of the following conditions have been fulfilled:

(a) This Contract Agreement has been duly executed for and on behalf of the Client and the Service Provider;

(b) The Service Provider has submitted to the Client the Performance Security.

4. Article 4 – Jurisdiction

4.1. Any legal proceedings arising out of the agreement shall be subject to the appropriate court jurisdiction of Hon’ble High Court of Andhra Pradesh.

5. Article 5 – Appendixes

5.1. The Appendixes listed in the attached List of Appendixes shall be deemed to form an integral part of this Contract Agreement.

5.2. Reference in the Contract to any Appendix shall mean the Appendixes attached to this Contract Agreement, and the Contract shall be read and construed accordingly.

IN WITNESS WHERE OF Dr NTR VST and the Selected Bidder/ Service provider has caused this Agreement to be duly executed by their duly authorized representatives the day and year first above written.

For and on behalf of the Client (Purchaser)

Signed: _____

In the capacity of *[insert: title or other appropriate designation]*

in the presence of _____

For and on behalf of the Service Provider

Signed: _____

In the capacity of *[insert: title or other appropriate designation]*

in the presence of

Place: Signature with seal

Date:

Bid Security (EMD) form

File. No: ……..

Project Name: …….

(To be issued by a bank scheduled in India as having at least one branch in Vijayawada) Whereas ..... (Here in after called “the Bidder”) has submitted its bid dated..... (Date). For the execution of ..... (Here in after called “the Bid”) KNOW ALL MEN by these presents that WE ..... of ..... having our registered office at ..... (Here in after called the “Bank”) are bound unto the (hereinafter called “The Managing Director, APMSIDC, Mangalagiri”) in the sum of ..... for which payment well and truly to be made to the said APMSIDC itself, its successors and assignees by these presents.

The conditions of this obligation are:

a. If the bidder withdraws its bid during the period of bid validity or

b. If the bidder, having been notified of the acceptance of its bid by the APMSIDC during the period of bid validity:

1) fails or refuses to execute the contract form if required; or

2) fails or refuses to furnish the performance security, in accordance with the bid requirement;

c. bidder submits fabricated documents.

We undertake to pay the above amount upon receipt of its first written demand, without the APMSIDC having to substantiate its demand, provided that in its demand the will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee of Rs. ---------- will remain in force up to….. and any demand in respect thereof should reach the Bank not later than the above date.

Place: Signature of the Bank Official

Date: with seal

Forms

Form P#1: Application Form

Date:

From	The Managing Director, (APMSIDC), Government of Andhra Pradesh. Address: 2nd Floor, PHYCARE Building, Plot No. 9, APIIC IT Park, Survey No. 49, Near Visalandra Printing Press, Autonagar, Mangalagiri, Andhra Pradesh - 522503 E-mail id: aphmhidc@gmail.com

Ref: <Project Name>

Dear Sir,

We, the undersigned, apply to the above referred Project and declare the following: -

a. We have examined and have no reservations about the RFP Document.

Having examined the Bidding Documents, we, the undersigned, offer to provide the services specified as per the RFP for the sum (here in after called total bid price) as quoted in commercial bid or such other sums as may be determined in accordance with the terms and conditions of the contract.

We undertake, if our bid is accepted, to commence work as per the schedule and to achieve the effectiveness of the contract within the respective timelines stated in the Bidding Documents.

Construction of the Contract

i. We have read the provisions of tender and confirm that these are acceptable to us.

ii. We further declare that the bid is unconditional.

iii. We undertake, if our bid is accepted, to commence the work as per the schedule immediately upon your Notification of Award to us, and to achieve Completion within the time stated in the Bidding Documents.

iv. If our bid is accepted, we undertake to provide an Implementation cum Performance Security in the form and amounts, and within the timelines specified in the Bidding Documents.

v. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

vi. We, hereby, declare that only the persons or firms interested in this proposal as principals are named here and that no other persons or firms other than those mentioned herein have any interest in this proposal or in the Contract to be entered into, that this proposal is made without any connection with any other person, firm or party likewise submitting a proposal, that this proposal is in all respects in good faith, without collusion or fraud.

vii. We have collectively examined and have no reservations about the RFP Document.

viii. We agree to be jointly and severally liable for the full performance of the Contract if our Bid is accepted.

b. We agree to abide by this bid, which consists of this letter, EMD with technical bid, commercial bid, Pre bid meeting addendum if any and other attachments (specify the attachments) as per the tender document.

c. We do not have any conflict of interest in accordance with Data sheet

We understand that you may cancel the process at any time and that you are not bound either to accept any application that you may receive bidders to bid for the contract(s) subject to this, without incurring any liability to the Bidders, in accordance with the Data Sheet.

Name & Designation.....

Signature.....

Duly authorized to sign the Application for and on behalf of.....

Stamp/ Seal…….

Attachments: As per the technical/commercial bid specifications

Form P#2: Declaration regarding Clean Track Record

Name of the Bidder:
Name of the Project:

Sir,

1. I have carefully gone through the Terms & Conditions contained in the RFP Document …… I hereby declare that my company/ has not been debarred/blacklisted during last five Years as on Bid calling date by any Central or State Government/ Quasi Government Departments/ Banks (IBA) or Organizations in India for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices or not having any legal tangle with Govt. Organizations pending in any of the courts in India. There are no cases between the bidder and quasi government or government organizations.
2. In the event our organization was debarred or blacklisted or got into legal tangle at any point of time, I am declaring and listing the same for your reference.
3. I further certify that I am an authorized officer in my company to make this declaration.

Date: .....

Name.....
In the capacity of.....
Signed.....
Duly authorized to sign the Application for and on behalf of .....
Stamp/Seal……

Form P#3: Financial Strength Details

A. Details of Annual Turnover for Preceding 3 Years.

	Year 1 (2023-24)	Year 2 (2024-25)	Year 3 (2025-26)	Average Annual Turnover
Turn Over (In Rs. Crores)				

B. Details of Net Worth

	Year1 (Last Financial Year i.e. as on 31st March 2026)
Paid up Capital (Rs. Cr)	
(Add) Free Reserves (Rs. Cr)	
Total Net Worth (Rs. Cr)	

(Signature of Bid Signatory)

Seal of the Firm

Certificate from the Statutory Auditor

This is to certify that .....(name of the Bidder) has an average annual turnover (in the last three financial years) and Net Worth (in the last financial year) as shown above

Name of Authorized Signatory (CA):

Designation:

Name of firm:

UDIN No:

(Signature of the Authorized Signatory)

Seal of the Firm

Turnover details as per pre-qualification criteria mentioned in this RFP (taking into consideration all amendments issued to this document if any) are to be provided along with supporting documents.

Form P#4: Details of Local Presence

Name of the Bidder:

Name of the Project:

Date: .....

This is to certify that _____ (company name) having its local office at (address)_____has the following centre(s) in the State of Andhra Pradesh

Name and location of delivery centre	Contact person details	Number of projects handled	Skill sets	Indian Client List (Mention a few)

Name and location of the Organisation	Address	Number of employees

Note: In case, the bidder does not have local presence in AP at the time of bidding, a self-declaration has to be provided by the bidder that they will establish a project office in AP within 1 month from the issue of NoA if they are awarded the project.

Place:

Date:

Bidder's Signature and Seal:

Form P#5: Relevant Project Experience

Name of the Bidder:

Name of the Project:

Past experiences of Bidder in application/ Portal/ Website development and maintenance

Sl. No	Name of the Client/ Department	Description of Project	Contact address, Name of the officer, Mobile number, eMail_ID of the department	Value of the Project	Project Start Date & End Date	Central Government/ State Government/ PSU/ Private	Certificate Enclosed (Yes / No)

Note: Work order and Proof of Go-live/ Project completion certificates from client shall be provided. Non-compliance to this shall lead to non-evaluation of the projects.

Place:

Date:

Bidder's Signature and Seal:

Form P#6: Conflict of Interest

Name of the Bidder:

Name of the Project:

(Bidders own format on the company letter head)

Form P#7: Declaration as per GO.Ms.12 Dated 08.05.2015 of ITE&C (Infra) Dept., GoAP.

(On the Bidders letter head as per tender document)

Declaration as per GO.Ms.12, Dated 08.05.2015:

Clause 6:

1. Bidders can submit their bids with self-declarations in respect of the pre-qualification criteria prescribed in the RFP.
2. The procuring agency shall evaluate the bids based on the self-declaration and select the successful bidder.
3. The successful bidder should submit the documents to prove their pre-qualification as specified in the RFP, within 5 working days from the date of declaration of successful bidder.
4. APMSIDC will receive support documentation, verify the compliance with the requirements of the RFP and if they are in order, issue the award notification.
5. Failure to submit all support documents by the successful bidder within specified time or non-compliance with the self-declaration or non-fulfilment of the pre-qualification criteria specified in the RFP, upon their verification, shall entail forfeiting the EMD and Blacklisting of such bidder for a period of two Years as specified in the RFP. In such cases, the procuring agency may proceed further with the next-ranked bid.

Place:

Date:

Bidder's Signature and Seal:

Form T#1 - Understanding of the Project

Name of the Bidder:

Name of the Project:

Description of the Approach, Methodology and Work Plan for Performing the Assignment **(To be submitted on the Bidder's Letter Head)**

a. Bidders understanding of the Project.
b. Bidders Proposed Solution Approach, Methodology & Architecture
c. Proposed Services/ Product quality
d. Security and governance standards for business activity
e. Manpower Deployment & Retention strategy.
f. Capacity Building/ Training Plan
g. Any other relevant items related to the project.
h. Overall Project/ Engagements, Level Risks and Mitigation.
i. Issues and Risks in operation & maintenance of the Project.
j. Exit management plan

Clear articulation, description and Extent of compliance to technical requirements specified in the scope of work to be submitted along with Strength of the Bidder to provide services including examples or case-studies of similar solutions deployed for other clients.

Place:

Date:

Bidder's Signature and Seal:

Manufacturer Authorization Form - Digital Sign

[Location, Date]

To,
The Managing Director, APMSIDC
Address: 2nd Floor, PHYCARE
Building, Plot No. 9, APIIC IT Park,
Survey No. 49, Near Visalandra
Printing Press, Autonagar,
Mangalagiri, Andhra Pradesh -
522503
E-mail id: aphmhidc@gmail.com.

Subject: Manufacturer Authorization Form (MAF) for Digital Sign Services

Tender Ref No: _____, Dt: _____

Dear Sir,

We, <Digital Sign Service Provider>, who are the established and reputable manufacturers of Signing and Authentication solutions having factories at <Address> do hereby authorize M/s <Bidder Company Name> at having their registered office at <Bidder Address> who is the vendor submitting its bid pursuant to the Request for Proposal issued to offer their quotation, negotiate and conclude a contract with you against the above bid invitation with our products.

Yours faithfully,
(Authorized Signatory)
Printed Name & Designation
Seal/Stamp, Date and Business Address:

Manufacturer Authorization Form - Telecom Service Provider

[Location, Date]

To,
The Managing Director, APMSIDC
Address: 2nd Floor, PHYCARE
Building, Plot No. 9, APIIC IT Park,
Survey No. 49, Near Visalandra
Printing Press, Autonagar,
Mangalagiri, Andhra Pradesh -
522503
E-mail id: aphmhidc@gmail.com.

Subject: Manufacturer Authorization Form (MAF) for SMS Services

Tender Ref No: _____, Dt: _____

Dear Sir/Madam,

We, M/s <Telecom Operator / SMS Provider Name>, having our registered office at <Address>, are an established and authorized provider of Telecom and Enterprise Messaging Services, including Transactional SMS, OTP, Alerts, and DLT-compliant messaging services.

We hereby authorize M/s <Bidder Company Name>, having their registered office at <Bidder Address>, to:

- Participate in the above-mentioned tender
- Submit bid, negotiate, and sign the contract
- Provide SMS services using our telecom infrastructure/platform

Scope of Authorization

The authorization includes:

- Bulk SMS (Transactional / Service Implicit)
- OTP Messaging
- Emergency Alert Messaging
- DLT Registration, Headers, Templates Management
- Integration via SMPP / HTTP APIs

Undertakings

1. We confirm that M/s <Bidder Name> is our authorized partner for providing SMS services for this tender.
2. We ensure full support for connectivity, delivery, and uptime during the contract period.

3. All services will comply with guidelines of Telecom Regulatory Authority of India and DoT.
4. We confirm that necessary DLT platform compliance, headers, and templates will be supported.
5. This authorization is valid only for the above-mentioned tender.

Validity

This MAF is valid till completion of the tender process and contract period.

Yours faithfully,

(Authorized Signatory)

Printed Name & Designation

Seal/Stamp, Date and Business Address:

Commercial Forms

Form C#1- Commercial Proposal Submission Form

(To be submitted ONLINE on the e-Procurement portal only)

(Do NOT submit a physical/hardcopy financial bid. The online submission alone shall be considered for evaluation)

[Location, Date]

To,
The Managing Director, APMSIDC
Address: 2nd Floor, PHYCARE
Building, Plot No. 9, APIIC IT Park,
Survey No. 49, Near Visalandra
Printing Press, Autonagar,
Mangalagiri, Andhra Pradesh -
522503
E-mail id: aphmhidc@gmail.com.

Dear Sir,
We, the undersigned, offer to provide the Services for [Insert title of Assignment] in accordance with your Request for Proposal dated [Insert Date], and our Technical Proposal.
Our attached Financial Proposal is for the sum of [***Insert amount(s) in words and figures***].

This amount is inclusive of the Domestic taxes such as --------- (***Indicate the amounts against each***).
We hereby confirm that the financial proposal is unconditional and we acknowledge that any condition attached to the financial proposal shall result in rejection of our financial proposal.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.
We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,
Place:
Date:
Bidder's Signature and Seal:

Form C#2- Commercial Form

(To be submitted ONLINE on the e-Procurement portal only)

(Do NOT submit a physical/hardcopy financial bid. The online submission alone shall be considered for evaluation)

Name of the Bidder:

Name of the Project:

Sl. No	Description	Quantity	Total Price without taxes (Rs.)	Taxes/ Duties etc. Price (Rs.)	Total price with taxes and duties etc. (Rs.)
(a)	(b)	(c)	(d)	(e)	(f) =(d) + (e)
1	Development / Implementation Cost	Lumpsum			
2	O&M Cost (For 5+2 Years)	Per Year			
3	Cloud Migration cost – DC & DR (Pre)	Lumpsum			
4	Cloud Migration cost – DC & DR (Post – end of contract period)	Lumpsum			
5	Other Cost (Software, Licences, etc.)	Per Unit			
Total					

Note:

1. The team shall work for the department as defined in the this RFP.
2. Dr NTR VST reserves its right to alter the scope (increase quantity/ remove certain items).
3. All other tasks pertinent to the contract even though may not have been mentioned in the bid document are assumed to have been included in the work.
4. Deduction of taxes at source will be made as per applicable laws from the payments to be made to the vendor.

5. Bids will be evaluated including Taxes.
6. The cost of S. No 1 will be settled on a Milestone basis as specified in this RFP.
7. The cost of S.No 2 will be settled on Quarterly based.
8. The cost of S.No 3 & 4, will be settled after complete data migration and Full System Acceptance at the end of milestone final sign off.
9. The cost of S.No 5 will be settled after submission of invoices to the Trust.

Place:

Date:

Bidder's Signature and Seal:

—End of Tender Document—

Digitally signed by
ANANTHALAKSHMI PADMAVATHI ARUMILLI
Date: 29-09-2026 19:51:15