THE NEW INDIA ASSURANCE CO. LTD

Registered Office: 87, M.G. Road, Fort, Mumbai - 400 001

REQUEST FOR PROPOSAL

FOR

THE PROCUREMENT OF AI/ML BASED SOLUTION FOR MONITORING AND INVESTIGATION OF FRAUD, WASTE & ABUSE OF HEALTH INSURANCE CLAIMS

RFP REFERENCE NO.	NIA/HEALTH/2025-26/FWA
Earnest Money Deposit	- For Non-MSME Bidders: ₹ 50,00,000/- (Rs. Fifty Lakh Only) - For MSME/ Start Up Bidders/ Bidders exempted as per GeM: Bid Security Declaration.
Address for Communication and submission of bids	Chief Manager, IT Department, Third Floor, Head Office, New India Assurance Co Ltd, 87, M.G. Road, Fort, Mumbai-1, E-mail: cwiss.rfp@newindia.co.in
RFP Release Date	30-01-2026
Last date of submission of RFP	As per GeM
Last date for submission of queries	As per GeM
Date and time of opening of technical bids	As per GeM

***For all other Timelines, Please refer to the GeM bid document.**

Index

SECTION I

1) INTRODUCTION:

The New India Assurance Company Limited (hereinafter called "NIACL") invites online bids for AI/ML based solution for real-time monitoring of fraud, waste and abuse in its health claim for retail/ group health insurance policies.

The tool should be capable of analyzing health claims data and claim documents to give probability/likelihood of the transaction or entity to be fraudulent as well as any potential leakage in the claim in conformity to policy wordings.

The tool should also provide exhaustive and customised analytical dashboards to monitor the overall data and drill down details of any identified transactions or entity. The tagging of claims should be at real time with a minimum capacity of up to 2000 claims per hour.

At NIACL, all health claims are processed by TPAs using the claim processing software solution of their own. The data flows to NIACL through web-services in four stages i.e. claims intimation, modification/enhancement, claim upload for payment and rejections/ UTR.

2) INVITATION TO BID:

2.1) NIACL invites bids from solution providers (bidder) for the **Procurement, implementation, integration and maintenance of AI/ML based solution for monitoring of Fraud, Waste and Abuse in Health Insurance claims** as per the specifications, terms, conditions and scope given in detail in this RFP document for a period of 3 years extendable further for 2 (1+1) years subject to satisfactory performance /services by the bidder and solely at the discretion of NIACL.

2.2) Bidder shall mean any entity which meets the eligibility criteria mentioned in this RFP and willing to provide the solution as required in this bidding document. The interested bidders who agree to all the terms and conditions contained in this document may submit their bids with the information desired in this bidding document (Request for Proposal).

2.3) Address for submission of Bids and contact details including email address for sending communications are provided in this RFP document.

2.4) The purpose of NIACL behind this RFP is to seek a detailed technical and commercial proposal for procurement of the solution desired in this document. The proposed solution must integrate with NIACL's existing infrastructure seamlessly.

2.5) This document shall not be transferred, reproduced or otherwise used for purpose other than for which it is specifically issued.

2.6) Interested Bidders are advised to go through the entire document before submission of Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for the supply, implementation, integration and maintenance of the proposed Solution for NIACL are invited to submit their Pre-qualification Bid, Technical and Commercial Bid in response to this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at NIACL's discretion. This RFP seeks proposal from Bidders who have the necessary experience, capability & expertise to provide NIACL the proposed Solution adhering to

NIACL's requirements outlined in this RFP.

2.7) A complete set of bidding documents can be downloaded from GEM portal as well as our website https://www.newindia.co.in/tender-notice

3) OBJECTIVE:

The objective of this RFP is to define the Scope of Work for the bidder in order to select a vendor suitable for supply, implementation, integration and maintenance of the Fraud, Waste and Abuse control solution for health claims. This document contains the details regarding scope, project timelines, evaluation process, terms and conditions as well as other relevant details which the bidder need to study and factor while responding to the document.

4) DISCLAIMER:

4.1 The information contained in this RFP document or information provided subsequently to Bidder(s) in documentary form/email by or on behalf of NIACL, is subject to the terms and conditions set out in this RFP document.

4.2 This RFP is not an offer by NIACL, but an invitation to receive responses from the eligible Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of NIACL with the selected Bidder.

4.3 The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary, obtain independent advice/clarifications. NIACL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

4.4 NIACL, its employees and advisers make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution for unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

4.5 NIACL also accepts no liability of any nature whether resulting from negligence or otherwise, however caused, by reliance of any Bidder upon the statements contained in this RFP.

4.6 The issue of this RFP does not imply that the NIACL is bound to select a Bidder or to appoint the Selected Bidder or Concessionaire, as the case may be, for the procurement of solution and NIACL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever and cancel the tender.

4.7 The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respects will be at the Bidder's risk and may result in rejection of the Bid.

5) DEFINITIONS:

In this connection, the following terms shall be interpreted as indicated below:

5.1 "The New India Assurance Company Limited" means NIACL (including domestic branches and

foreign offices) and subsidiaries.

5.2 "Bidder/Service/Solution Provider/System Integrator" means an eligible entity/firm submitting the Bid in response to this RFP.

5.3 "Bid" means the written reply or submission of a response to this RFP signed by their Authorized Signatory.

5.4 "Acceptance of Bid" means the letter/fax/e-mail or any memorandum communicating the acceptance of this Tender to the bidder.

5.5 "Authorized signatory of the bidder" means the person authorized through a valid Power of Attorney by the company's Board/Managing Director/Director for signing the bid documents on behalf of the company

5.6 "Law" shall mean any Act, notification, bye-law, rules and regulations, directive, ordinance, order, or instruction having the force of law enacted or issued by the Central Government and/or the Government of any state or any other Government or regulatory authority.

5.7 "Vendor/Service Provider" is the successful Bidder found eligible as per the eligibility criteria set out in this RFP, whose technical Bid has been accepted and who has emerged as L1 Bidder as per the selection criteria set out in the RFP and to whom notification of the award has been given by NIACL.

5.8 "The Agreement/Contract" means the agreement entered into between NIACL and the Vendor, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

5.9 "The Contract Price/Project Cost" means the price payable to the Vendor under the Contract for the full and proper performance of its contractual obligations.

5.10 "Requirements" shall mean statements that identify a necessary capability, characteristic, attribute, or quality of a system and include schedules, details, descriptions, and statements of technical data, performance characteristics and standards (Indian as well as International) as applicable and specified in the RFP.

5.11 "Business Day/Working Day" shall be construed as a day excluding Saturdays, Sundays, and public holidays declared under the Negotiable Instruments Act, 1881 by concerned State Governments or the Central Government of India.

5.12 "Clarifications" means Addenda, Corrigenda, and clarifications to the RFP.

5.13 "RFP" means Request for Proposal.

5.14 "Day" means a calendar day.

5.15 "Deliverables" means Solution including all its components as per this RFP in general.

5.16 "Personnel" means professionals and support staff provided by the Bidder and assigned to perform the Services or any part thereof.

5.17 "Timelines" - Wherever Timelines have been defined as days, weeks, months, they will mean calendar days, calendar weeks, and calendar months.

5.18 "Specifications" means all the functional, technical, operational, performance or other characteristics required of a Product or Service as mentioned in the RFP document or any of the annexures or Clarifications to the RFP document.

5.19 "Uptime" is the percentage of time that a system is operational i.e. when the system is up and running. Uptime for calculation purposes equals the total number of hours of the day in a quarter minus downtime in the number of hours (not including the scheduled maintenance hours) divided by any part of an hour treated as a full hour.

5.20 SLA – Service Level Agreement, the bidder needs to provide a guaranteed uptime as per agreed SLAs.

5.21 Fraud: It refers to any deliberate act of deception intended to secure an unfair or unlawful financial gain from an insurance company. This can involve exaggerating claims, fabricating incidents, or misrepresenting information during the application process.

5.22 Waste: It refers to the inefficient or unnecessary use of resources that results in higher costs without providing additional value. This can include overutilization of services, such as excessive medical tests that are not medically necessary, or mismanagement of resources within an insurance company. While waste may not involve intentional wrongdoing, it still

contributes to increased costs for both insurers and policyholders.

5.23 Abuse: It occurs when services are provided that are not medically necessary or are more costly than necessary, leading to higher expenses for the insurance company. Abuse differs from fraud in that it may not involve deliberate deception, but it still results in improper payments and financial loss. Abuse can occur in various forms, such as overbilling, providing unnecessary treatment, or manipulating billing codes to receive higher reimbursements.

6) THE TENDER OFFER:

6.1 The tender documents will be available on GEM Portal as well as on the official website of NIACL i.e. https://www.newindia.co.in/tender-notice

6.2 The online bids under two bids system comprising of:

a) The Technical Bid and

b) Commercial Bid should be submitted online on GeM portal

(Various documents to be submitted online and offline along with the technical and the commercial bid as mentioned in Section **II** of this document.)

6.3 If the last date for submission of offline documents happens to be a holiday due to some unforeseen circumstances, then the Offline documents can be submitted by 11.00 AM on the next working day.

6.4 At any time prior to the last date of receipt of bids, the Company may, for any reason, whether at its own initiative or in response to clarifications requested by the prospective bidders, modify the tender document.

6.5 The clarifications/addendum, if any, issued by the Company at any time before the due date of submission of the bid will become part of the tender document and would be notified on the GEM portal as well as on official website of NIACL i.e https://www.newindia.co.in/tender-notice

6.6 No bid shall be accepted after the due date & time.

7) NIACL's RIGHTS:

NIACL reserves the rights to:

7.1 Accept / reject any of the tenders.

7.2 Add, modify, relax, waive or alter any of the conditions stipulated in the tender specification wherever deemed necessary.

7.3 Reject any or all the tenders without assigning any reason thereof.

7.4 Reject any or all the tenders if the bid is not signed by the duly authorized person or the bid submitted is unsigned or partially unsigned.

8) REJECTION OF TENDER:

The tender is liable to be rejected inter-alia:

8.1 If it is not in conformity with the instructions mentioned therein.

8.2 If it is not accompanied by the requisite Tender Fee.

8.3 If it is received after the expiry of the due date and time.

8.4 If it is evasive or incomplete including non-furnishing the required documents.

8.5 If it is received from any blacklisted bidder or whose experience is not satisfactory.

8.6 If it does not fulfill eligibility requirement and technical requirements.

8.7 If it is not accompanied by the requisite BSD.

9) VALIDITY OF BID:

The bid should be valid for acceptance for a period of at least 180 days from the last date of

submission. The offers with a lesser validity period would be rejected.

10) BID SECURITY DECLARATION:

Bidder needs to submit Bid Security Declaration (BSD) as per Annexure -XII provided. Bid will be treated as non-responsive and will be rejected in the absence of BSD.

11) PERFORMANCE BANK GUARANTEE:

11.1 The successful bidder will have to furnish a Security Deposit/Performance bank guarantee (PBG), an amount equal to 5% (Five percent) of final contract value for proper fulfillment of the contract in the form of a Bank Guarantee from a nationalized/scheduled bank. Bidder's Bank must be on SFMS platform and SFMS copy (Message Type IFN 767) should be sent to HDFC Fort branch IFSC- HDFC0000060

11.2 The PBG should be valid for a period of 39 months from the date of successful implementation of the Fraud, Waste and Abuse Solution. In case the contract is extended after 3 years, the PBG needs to be endorsed to that effect to align with the new expiry date of the contract.

11.3 The PBG shall remain valid for extended claim reporting for three months from the last date of validity.

11.4 The Company shall invoke the security deposit in case the selected bidder fails to discharge their contractual obligations as per the agreed terms & conditions during the period of the contract. Notwithstanding what has been stated elsewhere in this agreement and the schedules attached herein, in the event the selected Bidder is unable to meet the obligation pursuant to the Implementation of the Project, Operation and Maintenance Services and any related scope of work as stated in this agreement and the schedule attached herein. NIACL shall have the option to invoke the performance Guarantee after serving a written notice of thirty (30) days to the selected Bidder. PBG for MSME vendors to be followed as per the format given in GeM portal.

12) ELIGIBLE BIDDERS:

The bidder should be eligible as per Eligibility (Pre-qualification) Criteria as given in the Annexure - 1

13) SCOPE OF WORK:

The scope of the work would include the supply, installation, configuration, customization, integration, deployment on premises and maintenance of an end-to-end AI/ML enabled Fraud, Waste and Abuse Control solution for the Health Insurance Claims which is scalable in nature and must integrate with the existing Insurance Software Solution of NIACL.

13.1 Fraud, Waste, and Abuse (FWA) Monitoring Solution:

13.1.1 The proposed software solution should be able to perform ETL (Extract, Transform and Load) functions on provided health claims data, including both metadata and documents, to analyze and assess the likelihood of claims or entities, being involved in fraud, waste or abuse.

13.1.2 The tool should be able to deliver real-time claims tagging for various outliers based on use-cases, scenarios, industry standard triggers for Health claim

adjudication, validation for policy terms and condition pertaining to the claim processing.

13.1.3 The processing capacity should be at least 2000 claims per hour on day 1 with future scalability options. The solution must provide analytical dashboards that offer comprehensive insights, including drill-down capabilities for identified suspicious transactions.

13.1.4 The solution should be able to monitor claims for Fraud, Waste and Abuse throughout the entire journey of claims, broadly in stages viz. pre-processing (on intimation), while processing the claim, post processing of the claim.

13.1.5 It should support seamless integration with New India's existing Core applications or other systems of the TPAs and any other systems as and when needed and is to include a customizable rules engine to adapt to evolving fraud detection needs in a dynamic manner.

13.1.6 The solution must also ensure data security and compliance with relevant regulations.

13.1.7 Also, if in case, in future, NIACL decides to move/change its Core Insurance Software to a cloud platform / or any other existing platform, the software solution proposed for the FWA should be able to integrate with the same seamlessly.

13.1.8 The solution is to be hosted in a cloud environment, the subscription of which will be in the name of NIACL.

13.2 **Unified Intake Frontend:**

The bidder should provide a Unified front end which will enable claims intake from various channels like emails, TPA front end, inward of physical documents, FTP documents, NHCX intake, WhatsApp channels and any other channels as deemed necessary for servicing customers as needed. This enables immediate claims data, documents and images intake from TPAs as well enables future onboarding of claims directly. The intake process should be AI/ML driven with auto classification and auto extraction of information.

13.3 **Data Lake (Storage and Processing platform):**

13.3.1 Creation of Data Lake on a MEITY approved cloud platform for ingesting structured, semi-structured and un-structured data from various sources (various Third-Party Administrators through API integration, NIACL ODS for policy/other requisite data or any other sources as required) viz. simple data, printed and Scanned hospital documents, x-ray, films, prescriptions, bills, invoices, KYC documents, stickers, logs, metadata etc. The list is not exhaustive, and any other type of document related to health claims may be included.

13.3.2 Perform data engineering tasks including ETL/ELT and develop various data repositories as part of the overall data lake.

13.3.3 To create suitable data models and schemas to facilitate fast and relevant reporting and dash-boarding in consultation with NIACL. The data shall have to reside within India all the time.

13.3.4 Data Lake should have an integrated Document Management and Document Processing System to intake, store and process the documents which will include text, clinical images, other relevant files, and other images received as part of claims.

13.3.5 This data lake will be a layer between NIACL's Core Insurance Solution and its empaneled Third-Party Administrators (TPAs). The data is to be collected at this data lake house through API integration with NIACL 's existing TPAs or from any other sources.

13.3.6 The data lake so created is to be compliant on all the prevailing security

standards/ regulations/Acts (e.g. DPDP Act 2023 and amended time to time) as given by Government of India, regulatory bodies such as IRDAI or any such law passed by Government of India /IRDAI or any other regulatory authorities in future in relation with protection of customer data and its privacy.

13.4 The solution Provider shall ensure deployment, management and maintenance of various security components/features/solutions in the subscribed cloud environment, including but not limited to Network security, Data Security, Application security, Endpoint/Host level security, Vulnerability Management, Web Accessibility (WCAG) as per prevalent laws, Centralized log monitoring for all the environments (Development, Testing and Disaster Recovery) etc.

13.5 The Solution Provider shall follow and comply with all the regulatory/statutory circulars/Master directions applicable to the company like IRDAI, MEITY, CERT, RBI, SEBI, Ministry circulars, DPDP, IT Outsourcing (RBI Master Circular), NIACL IT Security Policy etc. as applicable.

13.6 The Solution provider shall ensure Independent External Audits to be conducted as per the regulatory requirements and should facilitate in closure of the audit points.

13.7 The Solution Provider shall ensure to implement the BCP/DR practices as per the regulatory and NIACL requirements and conduct DR Drills at least once in every 6 months.

13.8 **New Data Models:** The vendor should provide comprehensive data models relevant to the general insurance industry, both in India and globally. If needed, NIACL may request the bidder to create or modify data models to suit specific requirements.

13.9 **Deployment, configuration and commissioning:**

13.9.1 It will be done of the Fraud, Waste and Abuse Monitoring Solution on a data lake for AI/ML based churning of data and sending real time alerts to NIACL and concerned TPA for pre-processing decision making based on risk scoring (high, medium, low) of the claims at various stages such as Pre-Authorization, Modification/enhancement, discharge, Settlement of Claims etc.

13.9.2 The bidder should propose architecture to achieve the same. Configuration of the tool for various industry standard rule-based triggers or as provided by NIACL as per **Annexure-XIII** (the list is representation of some of the most popular triggers but is not a comprehensive list.

13.9.3 The triggers on need basis will have to developed by the bidder/OEM of the tool on demand of NIACL with no extra cost to NIACL than that specified as part of TCO).

13.10 **Image forensic solution**:

13.10.1 The bidder shall provide a readily integrated or modular to be ready to integrate with the proposed solution for checking de-duplication of the documents related to the claims along with similarity checks with, but not limited to, date, document number, hospital or diagnostic centers, health vitals, health reports, treating doctors, labs etc.

13.10.2 The solution should be able to perform similar checks to detect images that, while not identical, are sufficiently similar to raising suspicion. This includes identifying images with subtle alterations, such as watermarks, seals, or logos being tampered with, as well as detecting document content (e.g., identical text or forms) reused across different claims.

13.10.3 It should leverage advanced algorithms (e.g. machine learning, deep learning) for robust image comparison, factoring in distortions or modifications typically employed in fraudulent document submission. Metadata analysis is to be also implemented for identifying images that have been altered after capture, such as those that have had their creation time or location data tampered with. This is a

representative example and the same can be modified to enhance the level of detection, with mutual agreement.

13.11 **Clinical journey extraction**:

The primary goal of this system is to automatically extract comprehensive timelines of patient clinical experiences from various data sources using advanced large language models (LLMs) and vision-language models (VLMs). This would involve processing unstructured clinical notes, medical images, and potentially other forms of patient data to reconstruct the sequence of diagnoses, treatments, and outcomes. Once these detailed clinical journeys are extracted, the system should enable a comparison against established standard treatment protocols/procedures for specific conditions. This comparative analysis will be crucial for identifying deviations from regular practices. We vision this capability as a valuable tool for clinical audits.

13.12 **Optical Character Recognition (OCR)**:

The solution should be a readily integrate-able or modular solution designed for seamless integration with the proposed FWA solution for digitizing health claims documents, such as invoices, bills, handwritten notes, prescriptions, discharge summaries, and more as stated below:

13.12.1 **Data Extraction:** The OCR solution should extract critical data from health claims documents, including patient details, treatment codes, service dates, amounts, medical provider information, and prescriptions.

13.12.2 **Handling Structured and Unstructured Formats:**It must be capable of processing both structured documents (e.g., invoices) and unstructured documents (e.g., handwritten notes), enabling the extraction of relevant information from a variety of formats.

13.12.3 **Handwriting Recognition:**The solution should support handwriting recognition, a key feature for health-related documents (e.g., prescriptions, doctor's notes), ensuring accurate data extraction from non-standard, handwritten text. Additionally, it should include adaptive learning algorithms that improve handwriting recognition accuracy as more documents are processed, continually enhancing its performance over time.

13.12.4 **Language Translation:**The solution should be capable of translating the various languages into English which should also include the capability of translation from any structured or unstructured document. The solution should be a proven one and readily available for deployment. A reputable and tested COTS platform will be given preference.

13.13 **Policyholder/Insured Onboarding and Underwriting Decision Support:**

The system should facilitate comprehensive policyholder onboarding, capturing both policy-level and member-level details, including coverage, limits, exclusions, special riders and other relevant information. It should also track claims trends that are linked to specific underwriting parameters, allowing this data to be made available through an intuitive user interface to support informed underwriting decisions. The triaging process for policy underwriting may be driven by a risk score, which is determined based on these trends and other material factors relevant to the policy's underwriting profile.

13.14 **Hospital Master Maintenance and Blacklisting:**

The system should facilitate the maintenance of Hospital Master Records, ensuring that each hospital's status—whether part of the Preferred Provider Network (PPN), Third-Party Network (TPN), or a non-network hospital—is accurately tracked and updated. The system should enable scoring or rating of hospitals to decide on the straight though processing or interventions needed. Additionally, the bidder must ensure that records of blacklisted or red-

flagged hospitals are consistently updated and maintained in real-time to prevent fraudulent claims and mitigate risks. The system should have capability to integrate with the third party-maintained hospital register with relevant details. System should enable suspension, watch list and blacklist of hospitals.

13.15 **Digitized Contracts with Hospitals:**

The vendor shall also digitize and store the digitized Contracts for all the paneled Hospitals (PPN) of NIACL (existing as well as paneled in future). The digitized record of the Schedule of Charges /Packages for various procedures should be maintained in Data Lake for applying it for drawing correlation and applying validation with the claims. The system should be capable of enabling capture of modified tariffs at the time of renewal or during the contract period.

13.16 **Drug Data Repository Maintenance and Pharmacy Leakage Prevention:**

The vendor must provide/create and maintain a drug data repository. The vendor should ensure that the drug data repository is continuously updated in accordance with industry standards, including critical details such as pricing, manufacturing brand, the ailment for which it is primarily prescribed and other relevant information. This information shall be used by the FWA Solution to identify and avoid pharmacy leakages, if any. Additionally, the solution should also be able to identify applicability of a medicine for a particular ailment, its dosage, prices etc. through machine learning of the solutions. In addition, system should allow flagging of high-cost drugs and their utilization.

13.17 **Dashboard Requirement:**

The vendor should be able to provide both custom dashboards and generic dashboards tailored to the general insurance industry in India and also specific to NIACL's own requirement. These dashboards should offer insights at both summary and granular levels, including key metrics such as the number of claims processed, number of policies processed, and number of frauds identified, data mismatches, and other relevant information. System should support self-service reporting and data visualization. Whenever required, new dashboards can be created to extract reports for any regulatory authority.

13.18 **Configuration and maintenance of analytical dashboard for monitoring health portfolio**.

Some of the examples are:

- Migration of patients
- Fraud risk dashboard
- Claim processors tracking/audit trail.
- Schedule of Charges and Package based utilization.
- Cashless vs. reimbursement percentage etc
- Cashless everywhere information
- Repudiation of claims
- Modern treatment claims related data
- Cost per claim for different geographical zones as well as PAN India.
- AYUSH claims data
- ICR policy wise, party-wise, office wise, Agent-wise, TPA wise, Region-wise year on year analysis

The list is only illustrative and not exhaustive. The bidder should be able to configure various alerts and dashboards; regulatory and compliance reports/MIS as may be required by NIACL from time to time. The solution system should be configurable as mentioned above for the alerts, dashboard, and reports/MIS.

13.19 **User privilege Management System:**

The system should provide role-based access into the solution with roles such as super user, admin, guest users etc. (the roles shall be decided in consultation with the successful bidder).

13.20 **Audit Of Claim:**

The FWA Solution should provide an Auditing interface for the Doctors from New India /Internal Auditors /Statutory Auditor to do the audit of the claims by accessing the information and relevant documents through an authorized access by the administrator. In addition, it should be able to integrate the investigation details and report from TPA investigation. A front-end facility is also to be there in the solution under the Audit interface to input the findings of tele-investigations or any other investigation conducted by NIACL/ TPA /any other party on behalf of NIACL such that it becomes part of information being processed for the approval of the claim.

13.21 **Training:**

Bidder shall provide user training to the optimal number of personnel identified by NIACL on functional and technical operational aspects of the solution and analysis of the claims based on certain alerts, navigations in the software solution and customization of the dashboard. At the end of each training session, an evaluation test needs to be conducted in coordination with NIACL to ascertain the effectiveness of the training. Training Material (in English) for Health Department as well as IT dept. users will be provided by the bidder. Training courses are to be organized on a half-yearly basis.

13.22 **Specific Terms and Conditions:**

13.22.1 All the data collected (raw and processed) in the entire exercise will be the sole property of NIACL.

13.22.2 No data will be shared with any third party or for any publications etc., unless written permission has been obtained from the Competent Authority in NIACL.

13.22.3 NIACL should have visibility over the Database schema.

13.22.4 NIACL may assign the Services provided therein by the Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all its assets.

13.22.5 NIACL shall have the right to assign such portion of the services to any of the sub-contractors, at its sole option, upon the occurrence of the following.

13.22.5.1 Bidder refuses to perform.

13.22.5.2 Bidder is unable to perform.

13.22.6 Termination of the contract with the Bidder for any reason whatsoever; (The company reserves the right to approach the legal forum for compensation of loss caused due to the act of the bidder).

13.22.7 Expiry of the contract. Such rights shall be without prejudice to the rights and remedies, which NIACL may have against the Bidder.

14 Termination for Insolvency:

14.1 NIACL may, at any time, terminate the contract by giving written notice to the Bidder, without any compensation to the Bidder, whatsoever if:

14.1.1 The Bidder becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to NIACL.

14.1.2 The Supplier being a company is wound up voluntarily or by the order of a court or a receiver, or manager is appointed on behalf of the debenture/shareholders or circumstances occur entitling the court or debenture/shareholders to appoint a receiver or a manager, provided that such termination will not prejudice or affect any right of action or remedy accrued or that might accrue thereafter to the NIACL.

14.1.3 The bidder shall make available to NIACL the complete software solution in order to make NIACL continue functionality of FWA control solution.

14.2 NIACL's Rights in the event of merger or acquisition of the bidder by another company:

14.2.1 The bidder shall give minimum 6 months' notice in advance to NIACL in the event of any proposed merger or acquisition activity by a company other than the bidder.

14.2.2 The bidder shall make available to NIACL the complete software solution to make NIACL continue functionality of FWA control solution.

14.2.3 NIACL reserves the right to continue the relationship with the acquiring or merged entity.

14.2.4 In the event of NIACL agreeing to continue the relationship with the merged or acquiring entity, the cost and price along with all other specifications as agreed in the tender shall continue to be performed by the merged or acquiring entity.

15 ASSUMPTIONS

15.1 NIACL shall not assume responsibility or liability for any infringements or unauthorized use of the licensed products. In the event of any claims related to licenses against NIACL, the chosen Bidder must address them, and all liabilities and claims must be resolved by the Bidder.

15.2 Additionally, if the selected Bidder fails to provide any necessary licenses, artefacts, or resource requirements to NIACL, NIACL will not cover any additional costs for obtaining such items at a later date.

15.3 The selected Bidder must also consider providing Technical Support for the Solution and related application software throughout the contract period, starting from day one.

15.4 It is imperative for the successful Bidder to ensure an adequate and skilled workforce for the delivery and achievement of SLA targets throughout the entire Contract duration.

15.5 The Bidder is expected to present a clear outline of the intended deliverables, including real-life examples, activities, and project phases required for project completion as outlined in the RFP.

16 IMPLEMENTATION AND INTEGRATION

16.1 The delivery of all products and/or systems and/or services and/or functionalities covered under this bid to be completed within a period not exceeding 4 months of issuance of Purchase Order. The bifurcation of the delivery schedule and project plan will have to be provided by the successful bidders. The implementation shall comprise of system configuration, customization, pilot implementation, integration with the NIACL applications, UAT and system roll out, training etc.

16.2 **Delay in Integration** - In case bidder is not able to complete required integrations within the stipulated period of 4 calendar Months from the date of order, penalty of Rs. 1,00,000/- per day subject to a maximum of Rs 1,00,00,000. The amount will be recovered by forfeiting the Performance bank guarantee. Penalty is not applicable for the reasons attributable to the NIACL or force Majeure.

16.3 **ESCALATION MATRIX:** The Bidder and NIACL will include an escalation matrix to resolve any issue that may crop up during the project period as given below:
(The same shall be exchanged at kick off of the project).

Escalation level 1	Name,Designation,Email and contact number of NIACL Employee should be given	Name,Designation, Email and contact number of Bidder's Employee/ Executive should be given
Escalation level 2	Name,Designation,Email and contact number of NIACL Employee should be given	Name,Designation,Email and contact number of Bidder's Authorized Signatory or above should be given

17 INFORMATION SECURITY

The Bidder personnel shall follow NIACL's information & Cyber security policy and instructions while working on the project.Bidder shall, upon termination of this Contract for any reason, or upon demand by NIACL, whichever is earliest, return any and all information provided to Bidder by NIACL, including any copies or reproductions, both hardcopy and electronic copy.

18 CONFIDENTIALITY

Both parties acknowledge that all materials and information which has or will come in its possession or knowledge in connection with the performance of this agreement, hereof, consists of confidential and proprietary data, who's disclosure to ruse by third parties will be damaging or cause loss to the company. The parties agree to hold such material and information in strictest confidence not to make use thereof other than for the performance of this agreement, to release it only to employees requiring such information, and not to release or disclose it to any other parties. The parties shall take appropriate action with respect to its employees to ensure that the obligations of non-use and non-disclosure of confidential information as per NDA is fully satisfied.

19 Right to Audit Clause:

NIACL shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance/security controls by the Bidder of its obligations/functions in accordance with the standards committed to or required by NIACL and the Bidder undertakes to cooperate with and provide to NIACL or any other agency appointed by NIACL, all documents and other details as may be required by them for this purpose. Any deviations or contravention identified as a result of such audit/assessment would need to be rectified by the Bidder failing which NIACL may, without prejudice to any other rights that it may have, issue a notice of default.

20 Cyber Security Testing/ VAPT:

The bidder will conduct security testing (Vulnerability Assessment & Penetration Testing) of the portal -which is dedicated to NIACL - twice in a year & shall submit the executive summary report to NIACL. Any serious gaps identified during this exercise, must be plugged on priority.

21 Business Continuity Plan:

The bidder should have BCP, processes in place & drills should be conducted on regular frequency (At least once in a year). In case of any disaster or any equivalent phenomenon, the bidder should have capability to carry out operations apropos our engagement.

22 Data Residency Clause:

Any data pertaining to NIACL's related operations must be hosted in India only.

23 Data Ownership

The ownership of the data shall always reside with NIACL. The Bidder will only act as a custodian of NIACL's data. No part of the NIACL's data shall be used by the Bidder for any purposes including but not limited to marketing and data mining. NIACL will have copyright on all content and media hosted on the website.

24 PURCHASE PRICE

24.1 Total cost of the FWA solution with support and inclusive of applicable taxes would be the Total Cost of Ownership (TCO) and has to be quoted in commercial Bid.

24.2 Prices payable to the Vendor as stated in the Contract shall be firm.

24.3 The Bidder will pass on to NIACL, all fiscal benefits arising out of reductions/ regulatory changes, if any, in Government levies viz. sales tax, excise duty, custom duty, GST etc. or the benefit of

discounts if any announced in respect of the cost of the items for which orders have been placed during that period.

24.4 All prices submitted on GeM shall be inclusive of all applicable Taxes

25 PAYMENT TERMS

25.1 The final Payment process will initiate only after the Successful implementation and execution of agreement by both the parties.

25.2 The invoices will be raised on a monthly basis after deducting penalties. Any sort of penalties will be levied and adjusted on a quarterly basis.

25.3 The applicable TDS will be deducted at the time of payment of invoices.

25.4 Payment will be released in the below phases:

25.4.1 **Implementation**

Stages	Stage description	Payment release (%) for Year 1
Milestone1	Project Kick off and mobilization	10
Milestone2	Requirement Sign off	15
Milestone 3	Development	25
Milestone 4	UAT Sign off	25
Milestone 5	Go Live	15
Milestone 6	Hypercare (3months, post go live)	10

25.4.2 **Support**

25.4.2.1 Period of three years post hypercare on subscription basis. To be paid quarterly in arrears .

25.4.2.2 No credit will be given for early deliveries and installation.

25.4.2.3 No advance payment for any portion of the total project costs shall be made.

25.4.2.4 For delayed deliveries and installation, penalty/liquidated damages will be applicable as mentioned in the related clauses of the RFP.

26 QUERIES

26.1 The queries, if any, can be communicated only through the GEM portal.

26.2 The queries received via any other mode will not be entertained.

26.3 The Company shall not be responsible for ensuring that the bidders' queries have been received. Any requests for clarifications received after the indicated date and time will not be entertained.

26.4 The clarifications (if any) issued at any time before the due date of submission of the bid will become a part of the tender document and would be notified on the official website of the Company

27 ADDENDUM/CORRIGENDUM

The vendors are advised to regularly check the NIACL official website https://www.newindia.co.in/tender-notice & GEM portal for addendum/corrigendum, if any published by NIACL.

28 TECHNICAL/FUNCTIONAL SPECIFICATIONS (T&FS) : As per Annexure II

29 SERVICE LEVEL AGREEMENT (SLA) & PENALTY

29.1 The successful bidder shall also sign a Service Level Agreement (SLA) with the NIACL to ensure the up-time of 99.95% on quarterly basis which shall be calculated as accessibility to the FWA

Solution and other associated components implemented by the bidder as part of the RFP requirement.

29.2 If the bidder fails to maintain guaranteed up-time of 99.95% on quarterly basis, NIACL shall impose a penalty. If the up-time is below 97%, the NIACL shall have full right to terminate the contract under this RFP. The penalty shall be deducted on quarterly basis from Financial Quarter ending month's billing.

29.3 The successful bidder will also have to enter into a Service level agreement for Service Support as per the terms and conditions of the RFP and covering the scope of work and technical requirements. The SLA requirements are as under: Service Parameter SLA Penalty Basis of Measurement/Remark:

Note: The percentage of uptime will be calculated on quarterly basis as follows:

Uptime Percentage = (Total Time - Downtime) / Total Time * 100

However, it is the responsibility/ onus of the selected bidder to prove that the outage is attributable to NIACL.

Critical Level	Response Time	Resolution Time
(Severity 1) Alerts to help processing of claim involving TATs	10 Min	Within 30 Mins of call reporting
(Severity 2) Dashboards /MIS	60 min	Within 8 Hrs of call reporting
(Severity 3) TBD	90 min	Next Working Day
(Severity 4) TBD	120 Min	Next Working Day

Note: NIACL reserves the right to modify the response time and resolution time based on the criticality.
*Escalation matrix for unresolved issues to be provided by the bidder.

30 SUB-CONTRACTING

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the Bidder directly through their employees, and there shall be no subcontracting done by the Bidder without prior approval of NIACL.In the event of the bidder engaging another vendor (sub vendor) to execute the associated activities of, including but not limited to, security management, NIACL should be informed about the activity in advance in writing. The engagement can be performed only with the prior written approval of NIACL and shall not violate rule of Law, regulatory compliance and also be restricted to not more than 10% or as approved by NIACL of overall activity of the bidder. NIACL reserves the right to refuse and ask for replacement of any such sub vendor without disturbing the business as usual. Any legal, product liability including the liability on Intellectual property, infringement, and third party liability shall be borne by the bidder even if the act emanates from omission/commission of such sub vendors.

31 DEVIATION FROM SPECIFICATION

31.1.1 If the bidder wishes to depart from the pre-qualification & technical bid criteria in any respect, he shall draw the attention to such points of departure explaining fully the reasons thereof and furnish the same as per Annexure III. Unless this is done, the requirements of pre-qualification & technical bid criteria will be deemed to have been accepted in every respect. Also, the marks

for technical evaluation will be awarded depending upon the degree of compliance.

31.1.2 The Company reserves the right to accept/reject any or all of the deviations shown by the bidder

32 INSPECTION BY THE COMPANY OFFICIAL

NIACL representatives shall have free access to the vendor's work premises at any time during working hours for the purpose of inspecting. The successful bidder shall provide the necessary facilities for such inspection.

33 ROYALTIES AND PATENTS:

Any royalties or patents or the charges for the use or infringement thereof that may be involved in the contract shall be included in the price. The bidders shall protect NIACL against any claims thereof

34 VIOLATIONS BY VENDOR

The selected vendor may be blacklisted for future & security deposit will be forfeited in case serious violations are observed and NIACL's decision in this matter will be final and binding on the vendor.

35 AGREEMENT

The successful bidders shall enter into a detailed Agreement with the Company. The contract period for providing Integration & Implementation of Web & Mobile Applications and related services will be for a period of Three Years from the date of Agreement. SLA mentioned in the RFP will cover performance and availability of the solution deployed for Integration & Implementation of portals/apps and related services

The performance of the selected bidder shall be reviewed every year and if the vendor fails to meet expectations, NIACL reserves the right to terminate the contract at its sole discretion by giving three months' notice. Any offer falling short of the contract validity period (Three Years from the date of Agreement) is liable for rejection.

36 Integrity Pact:

The Integrity Pact (IP) (Annexure X) duly signed by the authorized official of NIACL and the Contractor, will form part of the contract / supply order. Proforma of the IP is enclosed along with the tender document (Annexure- XI) and shall be returned by the bidder along with the technical bid, duly signed by authorized person. All the pages of the IP shall be duly signed by the same authority. Bidder's failure to return the IP along with the bid, duly signed may lead to outright rejection of such bid.

37 EARNEST MONEY DEPOSIT

37.1 The intending bidders should submit Demand Draft / Bank Guarantee in favor of "The New India Assurance Company Limited", payable at Mumbai.

37.2 The Demand Draft / Bank Guarantee should be from a scheduled bank and has to be valid for 180 days from the last date of tender submission. Bidders can use the bank's standard Demand Draft / Bank Guarantee format for submitting the EMD.

37.3 The Demand Draft / Bank Guarantee should be irrevocable to the bidder during the validity period.

37.4 The EMD will not carry any interest.

37.5 Bidder's Bank must be on the SFMS platform and SFMS copy (Message Type IFN 767) should be sent to HDFC Fort branch IFSC- HDFC0000060. In case if SFMS is not received the application will be rejected.

37.6 The MSE bidders and other eligible bidders as per GeM are exempted from depositing the EMD. In place of EMD, they have to submit a Bid Security Declaration for participation in the RFP as per Annexure-12 which is mandatory.

37.7 For this purpose, MSE bidders shall also submit the Udyam registration certificate and other

relevant certificates, clearly indicating capacity and monetary limit. However, exemption is only for EMD, if such a bidder is successful, then Performance Bank Guarantee shall be submitted. The MSE registration certificate submitted must be valid as on bid submission date.

37.8 The EMD provided by the bidder will be forfeited if –

37.8.1 The bidder withdraws the tender after acceptance.

37.8.2 The bidder withdraws the tender before the expiry of the validity period of the tender.

37.8.3 The bidder violates any of the provisions of the accepted terms and conditions of this tender specification.

37.9 EMD will be adjusted/refunded to the successful bidder, only after signing of the contract and submission of Performance Bank Guarantee, completion of formality etc. in all respects to the satisfaction of NIA.

37.10 In case of unsuccessful bidders, the EMD will be refunded to them after intimation is sent to them about rejection of their tenders.

SECTION II

1. PART A – TECHNICAL BID (ONLINE)

The technical bid, apart from the online template filling up, should contain the scanned copies of following documents. The documents shall be arranged in the same order as mentioned in online bidding format.

a) Demand Draft/ Bank Cheque for Tender Document Fees.
b) Eligibility Criteria as per Annexure-I along with supporting documents.
c) Technical Compliance as per Annexure -II
d) Deviations, if any as per Annexure-III
e) Non-Blacklisting Undertaking as per Annexure V
f) Integrity pact (Duly signed and stamped) as per Annexure –XI
g) Bid Security Declaration as per Annexure - XII
h) Power of Attorney /Authorization Letter
i) Other supporting documents as per the tender requirement.

2. PART B – TECHNICAL BID (OFFLINE)

The following documents are required to be submitted offline in physical/hard copies at the address given for submission by the date and time as mentioned in the RFP, in one sealed envelope super-scribed as "Offline Document Submission" for "Request for Proposal (RFP) for "**PROCUREMENT, IMPLEMENTATION, INTEGRATION AND MAITENANCE OF AI/ML BASED SOLUTION FOR MONITORING AND INVESTIGATION OF FRAUD, WASTE AND ABUSE OF HEALTH CLAIMS** " failing which the bidder may be disqualified and their tender may not be opened:

a) Original DD/Bankers' Cheque towards tender document fees.
b) Integrity pact (duly signed and stamped) as per Annexure –XI
c) EMD/Bid Security Declaration as per Annexure – XII
d) NDA

The details of the DD/any other accepted instrument, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time.Otherwise, the submitted bid will not be acceptable.

3. PART C - COMMERCIAL BID (ONLINE)

Commercial bid as per Annexure-VI

Note: No offline documents are required to be submitted for commercial bid

SECTION III

1. GENERAL TERMS & CONDITIONS

PROCEDURE FOR PROCESSING THE TENDER DOCUMENT:

1.1) The Committee/Individual constituted by the Company will open the Part 'A' electronically and off-line document cover physically and on GeM. In case the Part 'A' does not contain required documents, their offer would be rejected.

1.2) Each and every aspect in the Eligibility Criteria and Technical Bid including deviations, if any, would be discussed by the Committee/Individual.

1.3) Each proposal will be evaluated by the Company based on Quality and Cost Based Selection (QCBS) process where quality of Bidder is of prime concern along with the cost of work.

1.4) In QCBS initially the quality of technical proposal submitted by the bidder as per the criteria given in RFP will be ascertained. Only those responsive proposals that have achieved minimum qualifying score in evaluation of technical bid will be considered further.

1.5) After technical bid evaluation, the commercial bid of responsive technically qualified bidders is opened, a final combined score is arrived at by giving predefined relative weightages for the score of technical proposal and score of commercial proposal.

1.6) The weightage for technical evaluation score shall be 70% and commercial evaluation score shall be 30%. The applicant has to submit the technical bid as well as commercial bid in prescribed manner while submitting the bid in response to this RFP.

1.7) The Bidders securing Highest Combined Marks shall be recommended for award of contract. The Company will follow the internal procedure for necessary approvals and thereafter proceed with notification of award of contract.

1.8) This procedure is subject to changes, if any, and the procedure adopted by the Company for opening the tender shall be final and binding on all the parties.

2.TECHNICAL EVALUATION

I. Technical bids of only those Bidders who qualify in the eligibility criteria will be evaluated thereafter. Bidders found ineligible will be disqualified and won't be allowed to participate in technical evaluation.

II. Technical Bids received within the prescribed date and time will be opened online on GeM portal. The basis / parameters for technical evaluation are as under :

Marking Scheme for technical evaluation

A. Product Readiness & Maturity (25 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
A1	Commercial Off-the-Shelf Product	The solution should be a ready-to-use product, not a custom-built prototype, proven in production with multiple clients.	10	**10:** Live product used by ≥5 Health insurance clients for ≥2 years **8:** Live product used by ≥5 insurance clients for < 2 years **5:** 2–4 clients > 2 years usage **3:** 2–4 clients <= 2 years usage **0:** Custom / pilot-only solution	Details of the COTS Solution. Satisfactory Letter or Sign-off documents from clients certifying both successful implementation and active operational status.
A2	Product Versioning & Roadmap	The product should have formal version releases, updates, and a clear roadmap, ensuring stability and continuous improvement.	3	**3:** ≥2 major releases in last 24 months + roadmap shared **1:** Ad-hoc releases, no roadmap **0:** No versioning	(i) Version release history for the last 2 Years.(STQC certified) (ii) Brief product roadmap for next 36months.
A3	Configuration over Customization	The solution should meet most requirements through configuration (e.g., rules, dashboards) instead of costly coding or development.	5	**5:** ≥80% requirements configurable via UI **2:** 40–79% configurable **1:** Requires heavy coding	Screenshots or document showing configuration through UI (rules, workflows, dashboards). Demonstration during presentation to be given by the vendors.
A4	Implementation Time to Go-Live		7	**7:** ≤12 weeks (documented plan)	

		Deployment should be fast, ensuring minimal business disruption.		**4:** 13–16 weeks **0:** >16 weeks / unclear	(i). Detailed Implementation plan with timelines. (ii). Reference timeline from similar projects.
B. Data Ingestion, ETL & Data Preparation (20 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
B1	Built-in Data Ingestion	Solution should be able to read and import data from multiple TPA and insurance sources, such as claims, policy, provider, payment, and external reference data.	5	**5:** ≥5 source types ingested **2:** 2–4 sources **0:** ≤1 source	(i). Simple architecture diagram showing how data is received (Push/pull) (ii). Document listing data source types supported.
B2	ETL Capability	Solution should extract, clean, validate, and transform data into a format suitable for AI/ML models, minimizing manual effort.	5	**5:** Full ETL workflow with validation, error handling, and transformation mappings **2:** Partial ETL / manual steps required **0:** No ETL capability	(i). ETL Workflow document showing extract, validation, transformation steps. (ii). Screenshot or demo evidence of ETL process. Demonstration during presentation to be given by the vendors.
B3	Data Harmonization & Standardization	Ability to combine and standardize heterogeneous TPA / provider data into a consistent format, ensuring all claims and provider data are comparable.	5	**5:** Supports ≥3 heterogeneous formats and standardizes fields **2:** Partial standardization **0:** No harmonization	(i). Document listing supported data formats and standardized fields. (ii). Sample before/after data format showing harmonization.
B4	Data Quality & Refresh	Solution should include automatic quality checks and be able to update and reconcile data regularly to maintain accuracy for fraud analysis.	5	**5:** Automated data quality + scheduled refresh / reconciliation **2:** Manual quality checks or infrequent refresh **0:** No quality control	(i). Brief document explaining data quality checks and reconciliation process. (ii). Sample report or dashboard screenshot.
C. Integration, Interoperability & Plug-and-Play Capability (20 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
C1	Standard APIs	Solution should provide open APIs for seamless integration with existing systems,	5	**5:** REST/JSON APIs documented & demonstrated **2:** File-based integration only	(i). API overview or integration document showing REST/JSON APIs.

		reducing manual work and risk.		**0:** No integration clarity	(ii). Integration flow diagram with existing systems. Sample API request/ response demo screenshot.
C2	Interoperability	Solution should work in a heterogeneous environment with multiple vendors or platforms, ensuring future compatibility.	5	**5:** Open standards (REST, JSON, HL7/FHIR, JDBC, etc.) **2:** Limited proprietary formats **0:** Closed system	(i). List of supported platforms and systems (ii). Declaration of use of open/standard technologies.
C3	Plug-and-Play Deployment	Solution should minimize changes to existing systems, ensuring faster adoption and reduced IT risk.	5	**5:** No core system changes required **3:** Minor changes required **1:** Major re-engineering required	Implementation plan clearly specifying the changes required to existing systems.
C4	Proven Scale	Solution should be able to handle large volumes of claims and users without performance issues.	5	**5:** ≥1 million claims/month per client (references) **2:** ≤1 million claims/month **0:** No evidence of scale	(i). Client certificate or reference stating monthly transactions/ claim volumes. (ii). Performance or capacity summary from live usage.
D. Dashboards, Reporting & Usability (15 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
D1	Customizable Dashboards	Solution should provide drag-and-drop or configurable dashboards, allowing users to tailor views without coding.	5	**5:** Fully configurable dashboards **3:** Limited filters / layout changes **1:** Fixed dashboards	(i). Screenshots/ Demo access showing configurable dashboards. (ii). Brief note explaining how users can modify the dashboard without coding.
D2	Role-Based Views	Different stakeholders (management, investigators, and operations) should see relevant dashboards with their KPIs and metrics.	5	**5:** Separate dashboards per role **2:** Generic dashboard only **0:** Not supported	(i). Sample screenshots showing different dashboards for each role. (ii). Short role-to-dashboard mapping document.
D3	Reporting & Export	Solution should provide scheduled reports with export capabilities for audit, regulators, or management.	5	**5:** Scheduled reports + PDF/Excel export **2:** Manual export only **0:** No reporting	(i). Sample scheduled report formats. (ii). Short note on report scheduling and distribution.
E. Fraud Analytics & Case Management (10 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**

E1	Pre-Configured Fraud Use Cases	Solution should come with ready-to-use fraud scenarios, reducing time to detect known patterns.	5	**5:** ≥6 pre-configured fraud typologies **2:** 3–5 typologies **0:** ≤2 / custom only	List of pre-configured fraud scenarios available in the solution.
E2	Case Management & Audit Trail	Solution should support end-to-end case workflow, including investigation tracking and immutable audit trail.	5	**5:** Full workflow + audit trail **2:** Partial workflow **0:** No case management	(i). Screenshots of end-to-end case workflow. (ii). Sample audit trail or activity log showing user action and timestamp.
F. AI/ML Capabilities (10 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
F1	Fraud Detection Techniques	Solution should include multiple AI/ML techniques such as supervised learning, unsupervised learning, anomaly detection, and graph analytics to detect complex fraud patterns.	5	**5:** Multiple ML techniques + model monitoring & explainability **2:** 1–2 techniques, partial explainability **0:** No AI/ML	(i). Summary document listing AI/ML Techniques used. (ii). Sample output or dashboard showing fraud detection results.
F2	Model Training & Feature Engineering	Ability to prepare data, generate features, train models, and continuously improve detection accuracy.	5	**5:** Automated feature generation, training, validation, and model lifecycle management **2:** Partial or manual model preparation **0:** No ML preparation	(i). Brief document explaining how models are trained and improved over time. (ii). Sample model performance or monitoring report.
G. Proof of Concept & Product Demonstration (50 Marks)					
Sl.	**Parameter**	**Description**	**Max**	**Scoring Criteria**	**Documents to be Submitted**
G1	Mandatory PoC	Demonstration using sample or real TPA claims data, showing fraud detection, dashboards, and case creation.	20	**20:** ≥5 fraud scenarios detected and demonstrated end-to-end **10:** <5 scenarios **0:** No PoC	(i). POC demonstration using sample or real claims data. (ii). List of fraud Scenarios
G2	Live Product Demo	Full demonstration of product features and workflow for evaluators to verify capabilities.	20	**20:** Live demo with ingestion → dashboards → case management **10:** Recorded or generic demo **0:** Slides only	Live product demonstration covering ingestion, dashboard and case management.

G3	IT Security	Solution should conform to all relevant / applicable Security Guidelines of NIACL, Regulatory Bodies and any other laws of the Government.	10		**Relevant Certification related to the conformity.**
Total Marks			**150**		

NB: Information provided by the applicant as mentioned in the table above should be submitted with supporting documents like work orders/ certificates strictly on the client's letter head. Any other form of submission will be summarily rejected. The documents as mentioned above are to be submitted mandatorily and no requests will be entertained for non-submission of documents citing NDA or client confidentiality.

III. The bidder will have to *demonstrate* proven capabilities in each of the segments as defined under the terms of reference of RFP and due weightage will be given to each segment in the overall scoring.

IV. Applicants scoring less than 70% (cut-off score) in the technical evaluation, shall not be considered for further evaluation process and will not be considered as technically qualified.

V. For comparison of the combined Technical and Price Score of all Firms, following formula will be used:

Final Technical Score (Out of 70) = (Technical Score under evaluation/ Highest Technical score achieved) x 70.

VI. Only those Bidders who achieve the specified cutoff scores would be short-listed for Commercial Bid Evaluation. The NIACL reserves the right to revise the cutoff for technical score.

VII. Technical Proposal will be evaluated for technical suitability, competence and proposal to meet NIACL'S specified requirements. The criteria for evaluation of technical bids are as under:

2. COMMERCIAL BID EVALUATION

I. Only those Bidders who achieve the specified cutoff scores would be short-listed for Commercial Bid Evaluation. The NIACL reserves the right to revise the cutoff for technical score.

II. After opening of commercial proposals, the commercial bid would be awarded marks out of maximum 30 based on formula below:

Final Commercial Score (Out of 30) = 30 x LFB (numeric value)/ FBE (numeric value).

Where, LFB is the Lowest Commercial Bid Offer and FBE is the Commercial Bid under evaluation.

3. FINAL EVALUATION

I. Final Score will be obtained based on the formula below as per 70:30 Weightage for Technical and Commercial scores:

Combined Score (Out of 100) = Final Technical Score + Final Commercial Score.

II. On the basis of this total score, the bidder obtaining the Highest Combined Score in evaluation of technical and commercial evaluation will be ranked CS-1 followed by proposal securing lesser marks as CS-2, CS-3 etc.

III. The Bidders securing Highest Combined Marks and ranked CS-1 shall be recommended for award of contract. The Company will follow the internal procedure for necessary approvals and thereafter proceed with notification of award of contract.

4. CONTACTING NIACL

I. For any clarifications, bidder can contact NIACL through formal channels over GEM portal.

II. No Bidder shall contact NIACL on any matter relating to its Bid, from the time of opening of Price Bid to the time the Contract is awarded.

III. Any effort by a Bidder to influence NIACL in its decisions on Bid evaluation, Bid comparison or contract award may result in the rejection of the Bidder's Bid.

5. AWARD CRITERIA

I. The contract will be awarded based on Total marks obtained through QCBS evaluation as specified above.

II. NIACL will notify successful Bidder(s) in writing by email that the Bid(s) has/have been accepted. The Selected Bidder has to return the duplicate copy of the same to the NIACL within 7 working days, duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

III. The successful Bidder will have to submit a Non-Disclosure Agreement (wherever applicable) as per Annexure VIII of this document together with acceptance of all terms and conditions of RFP.

IV. Copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

V. The notification of award will constitute the formation of the Contract.

VI. The successful Bidder(s) shall be required to enter into a contract/ SLA with NIACL, within 30 days of award of the tender or within such extended period as may be decided by NIACL

VII. Until the execution of a formal contract, the Bid document, together with the NIACL's notification of award and the vendor's acceptance thereof, would constitute a binding contract between NIACL and the successful Bidder

VIII. The contract/ agreement will be based on Bidder's offer document with all its enclosures, modifications arising out of negotiation /clarifications etc. and will include SLA, project plan – phases & milestones and schedule, copies of all necessary documents, licences, certifications etc.

IX. NIACL reserves the right to stipulate at the time of finalization of the contract if any other document(s) need(s) to be enclosed as a part of the final contract.

X. Failure of the successful Bidder to comply with the requirements/terms and conditions of this RFP

shall constitute sufficient grounds for the annulment of the award.

6. GENERAL GUIDELINES FOR BIDDERS

I. While submitting the bid, the bidder is required to comply with inter alia the following CVC guidelines detailed in Circular number 03/01/12 (12-02-6 CTE\SPI(I)2\161730) dated 13-01-2012. (Commission has decided that in all cases of procurement the following guidelines may be followed)

II. In a RFP, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of item/product in the CVC guidelines referred to the final solution that bidders will deliver to the customer.

III. If an agent submits a bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same RFP for the same item/product.

7. TERMINATION CLAUSE:

The contract may be terminated:

I. If at any point of time, the services of vendor are found to be non-satisfactory the contract will be terminated.

II. The Vendor will not sub-contract or permit any personnel other than vendor's engineers to perform any service or other activities required by NIACL without prior permission from NIACL.

III. The vendor should maintain the confidentiality of the data stored on the computer system. No engineer / staff of the vendor shall carry any personal floppy, USB drives, Blank CDs inside the Company's premises. Back-to-back clause, apart from New India standards, i.e., if the solution is deployed in NIACL's client's setup or government setup then all the confidentiality and data security norms will be applied to the successful bidder.
In case of termination NIACL shall be obliged to give 3 (Three) months' notice in advance. Vendor needs to provide minimum 6 months' notice for termination of contract

8. Contract Expiry/Termination

I. The Vendor shall hand over the solution in 100% working condition on termination or at the end of the contract. Any breakdown call that has been reported before termination of the contract shall have to be corrected by the Vendor before handing it over to NIACL.

II. After successful completion of contract terms/termination and if service term has not been extended, the bidder has to cooperate with NIACL or any of its designated 3rd party for migration of complete data to on premise/ cloud hosted infrastructure on mutually agreed terms.

III. The Bidder should handhold the migration process until the entire Solution / Data gets ported completely.

IV. The Bidder should sort out operability issues, if any, for smooth shifting of such data.

V. Service providers should be responsible to destroy the data upon request from NIACL as per NIACL Data Destruction Policy, with special emphasis on destroying all data at all locations.

VI. Any product related details and information like digital product library ratings, infographics, documents etc., shall be the Intellectual property of NIACL.

9. Workspace:

NIACL doesn't commit to providing any working space and communication system for the vendor, although it can be worked out on best efforts basis. If not available, the vendor will have to arrange for a workspace within the city.

10. Enclosures:

Annexure-I (Pre-Qualification Criteria for bidders)
Annexure-II (Proforma for Technical Bid)
Annexure-III (Deviations Format)
Annexure-IV (Queries format)
Annexure-V (Non-Blacklisting Undertaking)
Annexure-VI (Commercial Bid)
Annexure-VII (Agreement Format)
Annexure-VIII (NDA Format)
Annexure-IX (Integrity Pact Instructions)
Annexure-X (Integrity Pact)
Annexure – XI (Bid Security Declaration)
Annexure – XII (Land Border with India)

Annexure – I

Eligibility (Pre-Qualification) Criteria for Bidders and OEM

S N	Criteria/ Category	SI/ Prime Bidder	Required Supporting Documents
1	Entity	(i)The bidder must be a registered entity in India under the Companies Act 1956/2013 or relevant applicable law for partnerships / proprietorships. (ii)The bidder must be in operation for at least 5 years as on the date of bid submission. The condition of prior turnover and prior experience may be relaxed for Start-ups (registered by Department for Promotion of Industry and Internal Trade), provided that the Start-up meet the necessary quality & technical specifications	Copy of Certificate of Incorporation issued by the Registrar of Companies.
2	Annual Turnover	Average annual turnover more than 100 crore for the bidder over the last three (3) Financial Years i.e. for FY 2022-23, 2023-24, 2024-25 Exemption is provided for MSME categories as per prevalent regulations. The condition of prior turnover and prior experience may be relaxed for Start-ups (registered by Department for Promotion of Industry and Internal Trade), provided that the Start-up meet the necessary quality & technical specifications	Certificate for CA/auditor, Audited annual report. In case audited report is not available for 2024-25, duly signed provisional report to be submitted
3	Experience Criteria - Solution Implementation Experience	The Bidder/ Proposed technology partner/OEM Partner shall have successfully executed at least one Project of minimum value INR 5 Cr related to supply and implementation of Fraud, Waste and Abuse control/monitoring solution and other related modules specifically in Health Insurance in the last Five (5) years. The condition of prior turnover and prior experience may be relaxed for	Purchase Order and letter of satisfaction in the name of the Bidder or Contract copy

		Start-ups (registered by Department for Promotion of Industry and Internal Trade), provided that the Start-up meet the necessary quality & technical specifications	
4	OEM Authorization	(i) The bidder must be an authorized partner/reseller of OEM for solution being proposed. (ii) The bidder should have a direct back-to-back support agreement with the OEM.	OEM Letter/MAF
5	Certification	The Bidder shall have following Certifications valid at the time of submission of bid: 1. ISO 9001 for quality management or equivalent 2. ISO 20000 for IT Service Management or equivalent certification 3. ISO 27001 for Information Security Management System or Equivalent certification 4. CMMI Level 3 Certificate or higher	Copies of certifications to be provided

Eligibility Criteria for OEM

SN	Eligibility Criteria for OEM	Documents to be Submitted
1	The OEM for Insurance Claim Fraud Analytics solution should have an office in India as on date of tender submission **AND** having operating revenue of more than INR 200 Crore per year in India for the last three financial years. (2022-23, 2023-24, 2024-25)	CA certified copies of accounts / Audited Annual reports in support and self-certification on OEM letterhead.
2	The OEM should have a ready and tested Health Claim Fraud Analytics solution which can be further customised as per the need of NIACL	POC of the product
3	The proposed Insurance fraud analytics solution should provide deployment options on cloud and be cloud vendor agnostic to deploy on any MeitY approved private cloud infrastructure.	Self-Declaration by bidder signed by authorized signatory
4	The proposed solution should be offered as a single integrated solution with all components (as per SOW)	MAF with proposed product listing and Self-certification from OEM to be provided
5	The proposed OEM should have an existing capability and infrastructure to provide technical support as per SLA.	Document supporting the capability and Infrastructure/ Affidavit by authorized signatory giving support and skill matrix , support matrix with details of support centers

Note :

a) *Participation shall be restricted to either the OEM or its authorized dealer(s)/reseller(s), but not both. Where the OEM participates directly, it shall be treated as the Prime Bidder and shall be required to meet all eligibility criteria applicable to the Bidder. If the OEM participates, bids from its authorized dealer(s)/reseller(s) shall not be considered, and vice versa.*
b) *Bidder response should be complete with all relevant documents attached.*
c) *Documentary proof, sealed and signed by authorized signatory, must be submitted.*
d) *Proposals of the bidders may be rejected in case of incomplete/false information or non-submission of documentary proof.*
e) *Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. NIA will not make any separate request for submission of such information.*
f) *NIA may contact the bidder referenced customer for verifications of facts and hence the bidder should ensure that their customers are intimated in advance. In case NIA wishes to visit such customers, the bidder has to take necessary approvals and arrange the meeting. NIA will not make any separate request to the bidder's customers for this purpose.*
g) *NIA reserves the right to verify references provided by the Bidder independently. Any decision of the NIA in this regard shall be final, conclusive and binding up on the bidder. The NIA may accept or reject an offer without assigning any reason whatsoever.*
h) *The Bidder shall also disclose all ongoing litigation or disputes which may have an impact on its financial stability or ability to perform this Contract.*

Annexure -II

Technical Specifications

#	Technical Specifications	Compliance (Yes /No)	Remarks
	General/ Administrative		
1	The proposed solution should be a pre-integrated/pluggable (modular) solution containing Data Management, Data Quality, Analytics, Alerting and Investigation, Monitoring and Visualization capabilities all as one solution		
2	The proposed solution should control access to applications, modules and functions based on user roles and privileges.		
3	The proposed solution should allow users to access procedures through easy to use front end interfaces		
4	The proposed solution should capture detailed auditing information related to key user activities within the system. Some key system actions may also be audited, for example automatic disposition of an alert. Audited actions should include (but are not limited to):		
	• Login / logout		
	• Performing a search (including details of the query and results if desired)		
	• Viewing / editing/printing		
	• Deleting		
	• Administration actions (i.e. changing configuration)		
5	The proposed solution should Provide Entity Level Security so that users should also be able to use classifications (rules based on entity field values) to provide a more granular level of access control.		
6	The proposed solution platform must be cloud-agnostic and must support all major public cloud and private cloud ecosystems namely but not exhaustive AWS, GCP, Azure, etc.		
7	The proposed platform must be easy-to-deploy and must allow deployment automation using infrastructure-as-code techniques.		
	Data Management & Data Quality		
8	The proposed solution should support data quality measurement on an on-going basis embedded into batch/ near real-time Ingestion of semi-structured data like user activity log, geographic information, XML, JSON, etc. Automation for validation and aggregation of data for a single source of truth with the standardized store		
9	A centralized data store in form of data Lakehouse to handle future data requirements Data marts lakehouse based on company's requirements and Analytical platform with integrated environment for creation, management, and deployment of AI/ML models		
10	The proposed solution should support data cleansing and de-duplication, duplicate suspect processing, house holding, with array of out-of-the- box standardization rules conform data to corporate standards – or can build customized rules for special situations.		
11	The proposed solution should have business rules and GUIs for automatic merging and manual merging.		
12	The proposed solution should provide fuzzy logic to induce tolerance during matching		

13	The proposed solution should use the parsed data to provide flexible matching criteria		
14	The proposed solution should enable to define rules for record and/or field selections during the merging process		
15	The proposed solution should have the capability to enrich data from internal data sources		
16	The proposed solution should have the capability to enrich data from external/third party data sources		
17	The proposed solution should have transformations to perform analytical operations like Correlations, Distribution Analysis, Frequency and Summarization.		
18	The proposed solution shall contain the data, software, processes needed to cleanse, consolidate, and transform the data from their source system format to the data warehouse format.		
19	The proposed solution shall be able to check incoming data for quality, reliability, consistency, and validity, and then transform as required.		
20	The proposed solution shall facilitate data profiling based on dynamic, user defined validation rules and support identification of user defined 'events' to trigger alerts (through email reports) to users		
21	The proposed solution Data Management should have capability of Interoperating with application integration technology in a single solution architecture, Supporting data integration across hybrid cloud and intercloud environments		
22	The proposed solution should have capability to enable data services for use in broader architecture approach		
23	The proposed solution should support the delivery of data to, and the access of data from, a wide variety of data stores, repositories, and data management tiers in application deployments,		
24	The proposed solution should support Non-relational DBMS integration		
25	The proposed solution should support Self-service data integration		
26	The proposed solution shall have the capability to correct mistakes in spellings, inconsistencies, casings, and abbreviations		
27	The proposed solution shall support correction logic for Indian names, addresses, phone numbers, other identification proof documents and demographic details		
28	The proposed solution shall support profile matching through multi-field text matching functionality on profile information (comparison could be on combination of name, address, telephone number etc.)		
29	The proposed solution shall provide facility to save the queries and edit the same in future to derive newer queries		
30	The proposed solution should be able to create networks based on both transaction as well as relationship-based data, and create a nodes and links among the entities (client, agent, bank account number, demographics etc.,.)		
31	The proposed solution should support various types of matches such as exact / fuzzy match etc. with the watch list		
32	The proposed solution should have functionality to "flag / unflag" entities as and when they are added to / removed from a watch list		
33	The solution should provide the capability to drill through to source level information in the data profiling report		
34	The solution should perform the data quality functionalities without creating a copy of the data in a proprietary/external format		
35	The solution should have the ability to correct mistakes in spellings, inconsistencies, casings and abbreviations		
36	The solution should have pre-built libraries for standardization of INDIA specific data		
	- vocabulary libraries		
	- grammar rule libraries		
	- phonetics libraries		
	- standardization rules and libraries		

	- regular expression libraries		
37	The proposed solution shall support correction logic for Indian names, addresses, phone numbers, other identification proof documents and demographic details . The solution should have the ability to identify gender of individuals using the INDIA specific vocabularies		
38	The proposed solution should be customizable and allow enhancement of its knowledge base by constantly updating Indian Dictionary		
39	The solution should enable parsing of data into atomic level information for better matching		
40	The solution should provide safe string encode/decode capabilities		
41	The solution should provide a unified capability and system for both offline and online Dedupe		
42	The solution should provide following transformation nodes pre-built:		
	Clustering		
	Pattern Analysis		
	Basic Statistics		
	Frequency Distribution		
	Identification Analysis		
	Gender Analysis		
43	The solution should have the capability to identify duplicates and cluster records		
44	The solution should have intuitive, flexible rules to identify households		
	Advanced Analytics		
45	The proposed solution should contain a sophisticated and GUI based predictive modeling and analytical workbench		
46	The proposed solution shall enable identification of cases for further investigation identified as a result of audit of alerted policies / claims.		
47	The proposed solution should enable identification of suspicious profiles through a judicious mix of anomaly detection, business rules, predictive modeling and network analytics		
48	The proposed solution should provide interactive entity resolution capabilities that help analysts get the most accurate picture of complex relationships		
49	The proposed solution should provide out-of-box entity analytics and direct intelligence analysts by showing closeness, betweenness and influence to highlight areas/ entities of potential interest		
50	The proposed solution should use the most advanced techniques to detect rare events, outliers and/or influence points to help you determine, capture or remove them from downstream analysis (e.g., models).		
51	The proposed solution should have modern statistical, data mining and advanced machine-learning techniques		
52	The proposed solution should help analysts to visualize complex network of relationships between entities - such as people, places/ locations, things and events over time and across multiple dimensions		
53	The proposed solution should help analysts identify entity relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively		
54	The proposed solution should provide in-built features and advanced techniques for the analyst to detect rare events, anomalies and outliers and/or influence points to help determine, capture or remove them from downstream analysis		
55	The proposed solution should support Clustering of entities that are either user Defined or statistically chosen		
56	The proposed solution should be capable of providing centrality metrics like betweenness, closeness, eigenvector etc. which determine the importance of nodes in a network.		
57	The proposed solution should support detection of patterns from the transaction data set over a defined time period for particular individuals / groups		

58	The proposed solution should have flexibility of high performance imputation of missing values in features		
59	The proposed solution should be able to discover new patterns in the dataset (detect untrained patterns) and identify defined patterns in the dataset (trained patterns)		
60	The proposed solution should support processing, trend-analysis and modeling for forecast of data-points		
61	The solution should provide for model selection based on either the training, validation (default) or test data using several criteria such as profit or loss, AIC, SBC, average square error, misclassification rate, ROC, Gini, or KS (KolmogorovSmirnov)		
62	The proposed solution should provide for Decision trees with Splitting criterion: Prob Chi-square test, Prob F-test, Gini, Entropy, variance reduction. (Optional)		
63	The proposed solution should support trend analysis and modeling / forecasting for identified parameters on entities, transaction-wise data received from multiple sources		
64	The proposed solution should enable incorporating the solutions into business processes, surrounding infrastructure and products		
65	The proposed solution should support profile matching through user-defined (configurable) business rules through ad-hoc querying across multiple fields of entity-wise information from in-house and external agency data		
66	The proposed solution should allow Analysts and Investigators to make use of a fraud intelligence repository which gets populated containing information of performance of past models and scenarios, to improve accuracy of current predictive models should be able to define risk based on different levels such as relationships with entities and transactions (and its log) etc.		
67	The proposed solution should provide the ability to configure rolling aggregations as part of scenarios design on-the-fly.		
68	The proposed solution should allow alerts to be generated whenever flagged entities with high risk rating and having some level of suspicious activity		
69	The proposed solution should enable Capturing and Displaying a Value Associated with a Risk Indicator-Fired Event. Using the alerts API, users should be able to configure alert scorecards that capture a value as well as show the score weight. This will assist triage users in understanding the severity of violations as well as the total makeup for the alert score.		
70	The proposed solution should support detection of patterns so that criteria for various thresholds can be reviewed and modified.		
71	The proposed solution should have capability for lineage of Alerting Activity to Cases, Etc. Investigator Users working on cases, investigations, etc. should have the ability to see the alerting activity that caused the object (case) to be created — this should include details of the decisions and comments made by the user who triaged the alert and made the initial disposition decision.		
72	The proposed solution should be scalable to incorporate any additional functional requirements and application of additional niche analysis capabilities (such as text analytics etc.).		
73	The proposed solution should provide in-built feature of detailing rule robustness through measures of true positive, false positive and false negative as visual diagnostics		
74	The proposed solution should provide in-built feature of editing, enhancing, removing or defining the rules from scratch as custom categories basis requirements of the disease SOP which might change over time		
75	The proposed solution shall support identification of common patterns / factors / profile characteristics that could enable selection of criteria for selection of cases.		
76	The proposed solution shall provide a rich set of data mining algorithms that can be used for classification, regression, clustering, detection of outliers and anomalies and scoring of transactions/ entities.		
77	The proposed solution shall support detection of patterns from the transaction data set over a defined time period for particular individuals / groups		

78	The proposed solution shall support automated algorithms which will help the end-users to run multiple algorithms at a time and hence compare the results between them.		
79	The proposed solution shall support profile matching through user-defined (configurable) business rules through ad-hoc querying across multiple fields of Policies, claims and clients.		
80	The proposed solution shall help in determining patient segments based on a variety of customizable relationships and attributes – Location, demographics, disease type, symptoms etc.		
81	The proposed solution shall identify the risks associated with a given set of clients / agents/ claimants		
82	The proposed solution shall allow identification of localities/ regions where high numbers of risky Policies, claims and client profiles are detected.		
83	The proposed solution shall support analysis of voluminous patient data to identify patterns and determine risk rating of a particular Policy		
84	The proposed solution shall support ad-hoc querying of the data		
85	The proposed solution shall support Time Series and scenario ("What-If") analysis for dependent variables.		
86	The proposed solution shall have capability to use data obtained from internal and external data sources etc. and analyze scenarios of high risk and deviation		
87	The proposed solution shall generate periodic, region-wise, location-wise and form- wise analytical reports of the Central repository		
88	The proposed solution shall support assessment of impact of a particular policy decision on the workload on a particular office		
89	The proposed solution support Model developers make use of a fraud intelligence repository which gets populated containing information of performance of past models and scenarios, to improve accuracy of current predictive models should be able to define risk based on different levels such as relationships with entities, etc.		
90	The proposed solution should facilitate forecasting at various levels of hierarchies for different geographies with specific forecasting algorithms used for each hierarchy		
91	The proposed solution should enable analysts to be able to carry out scenario analysis / what –if analysis on the forecasted model allowing for changes in future parameter values.		
92	The proposed solution shall allow alerts to be generated whenever flagged policy/client with high-risk rating are present		
93	The proposed solution shall support detection of patterns so that criteria for various thresholds can be reviewed and modified.		
94	The proposed solution shall support selection of criteria for Identification of cases for special Business audit		
95	The proposed solution should enable Text Analytics Visualization, which should enable text analytics visualizations, enabling analysts to use text analytics to analyze unstructured text and within a workspace visualize and explore the results.		
96	The proposed solution can monitor changes in profile/ demographic data as per the applicable watch listed entities		
	Alerts and Investigations Framework		
97	The proposed solution should incorporate two key aspects – one is an advance analytics solution which provides dashboards and reporting at aggregated level for key officers and stakeholders, and the other should be an investigative workbench which also enables operational stakeholders to take action on the alerts that emerge for a policy, assess the evidence around the same, and take a decision on further action on the alert.		
98	The proposed solution should take an open, hub and spoke, data-driven approach so that the investigator analyst can configure solution capabilities to respond to new trends and business problems, access new data sources, and expand the use of the solution across the organization as requirements change		

99	The proposed solution should provide in-built features for Alert and Event Management with - Governance, audit and compliance, Prioritized queuing model, Enrichment, Scenario-fired event model, including scenario context, Manual alert creation and routing, Alert domains, and Custom disposition actions.		
100	The proposed solution should provide a built-in functionality of alert-based investigation and alert exploration and triage - in which alerts are reviewed to determine the probability that they represent suspicious behaviour and are evaluated for their importance		
101	The proposed solution should provide built in features to apply an appropriate disposition of the alert - such as closing, suppressing, moving to another queue (such as high or low priority), linking to a different object, and sending the alert information to an external system after a decision is reached about how to handle the alert		
102	The proposed solution should provide the ability for alert dispositions to be configured to Capture the disposition comment and date/time in Alerts Comment Manager so that it is visible to other analysts who may triage subsequent versions of that alert		
103	The proposed solution should provide an option to automatically disposition the alert when a new alerting event arrives. For example, the alert may be automatically assigned to an investigative team		
104	The proposed solution should provides users, such as supervisors or managers, with an overview of alert dispositions. This overview should include:		
	• An overview of user activity		
	• A report showing a department's acceptance rate and velocity (with adjustable date range)		
	• A report showing an individual analyst's disposition history		
105	The proposed solution should enable the investigator to Prioritize alerts, , Visualize alerts in different views to gain context., Enhance alerts by adding entities and integrating and connecting data., Escalate by routing alerts or changing their priorities, Create manual alerts., Manage multiple alert domains., Designate an alert to prompt a deeper investigation through its alerts and event management capabilities		
106	The proposed solution should enable to not just identify the entity against whom the alert was created, but also related alerts, related entities and their interlinkages.		
107	The proposed solution should provide facility to define rules and set threshold-based alerts for the same on the data used for query and analysis supported by solution		
108	The proposed solution should provide in-built feature of powerful search capabilities to explore the contents of the data repository, enabling the investigator to discover information relevant to a current investigation or information about which to base a new investigation. If the search returns something suspicious, the solution should enable the investigator to take the findings and develop the interesting results into an investigation workspace for analysis.		
109	The proposed solution should enable phonetic searching for free text searches, object labels, and specific entity fields using the Advanced Search window		
110	The proposed solution should enable synonym searching for free text searches, object labels, and specific entity fields using the Advanced Search window		
111	The proposed solution should provide in-built features for search and discovery through Exploration and Visualization, Free-text search, Filters and Facets and Geospatial search		
112	The proposed solution should provide in-built features of powerful search and surfacing results using Boolean operators for search, searching for exact phrases, proximity search, searching using wildcards, fuzzy search, specifying precedence, searching in specific fields, searching using numeric operators (for e.g. search for objects where the age field is greater than 10) , searching for all values within a range and searching for reserved characters		
113	The proposed solution should allow users to:		
	• Restrict a search to entity types, fields, comments or insights.		
	• Define their search terms by entering strings, select dates / date-ranges or choosing from reference data values		
	• Incorporate multi or single character wildcards in their search		

	• Build queries using AND, OR and NOT operators.		
	• Use the fuzzy search modifier to help match on words with alternative or incorrect spellings.		
	• Use the proximity modifier to search for specified words to be within a specified distance of each other		
	• Apply boosting to increase or decrease the relevancy for search results that match a specific part of the query		
	• Use query builder interface or text editor.		
114	The proposed solution search feature should allow user to select/deselect entities of interest like Name, father name etc to narrow down the search results for enhanced understanding		
115	The proposed solution should come in with in-built feature of workspace for interactive intelligence analysis, which will provide an investigator work area that enables the investigator to gather objects of interest - such as entities and alerts, to the investigation from the data repository.		
116	The proposed solution should provide in-built feature of multiple visualizations to view relationships between the objects of interest and associated information - such as locations associated with the data plotted on a map, events associated with the data plotted on a timeline, network view of relationship within the data, tabular views and detailed information views of the data.		
117	The proposed solution should come with an in-built feature to provide flexibility of adding different objects of interest to the investigation workspace as well as multiple investigation workspaces to a specific investigation.		
118	The proposed solution should come in with out of box feature of documenting insights for e.g. "Network diagram from workspace captured as an insight" - which will help investigators document the investigation findings. The insights could include information about an alert, a snapshot of a network diagram, or other visualizations		
119	The proposed solution should provide in-built feature of documenting insights which can be saved and retrieved later for continued development and be printed to retain a hard copy of the investigation findings.		
120	The proposed solution should have in-built features for Entity analytics through Entity resolution, Network analytics and visualization, Network link expansion, Network node decorator and enrichment		
121	The proposed solution should enable users who are working with and exploring large, complex networks, to configure node and link styles based on the conditions of the data. For example, the nodes representing a case object on the network chart could have a red background if the value in the risk_level of an entity is high risk.		
122	Administrators should be able to configure the following, based on the relationship or entity data: line color, style, and weight icon, node color, node border color, node shape, node border width, node scale, additional label, and indicator icon, all through Graphical User Interface		
123	The proposed solution should enable configuration to exclude Specific Entity Types from Default Expansion in Network View. Users should be able to exclude specific indexed entity types from the default expansion in the network view. If an end-user selects a node and performs a one-level expansion, the excluded entity types should not appear on the network. Also, these entity types should appear as an option if the user chooses to expand a node by type.		
124	The proposed solution should have pre-configured features to identify and extract entities such as names, persons, organizations / companies and locations from text data. It should also be able to use a customized list of entity pattern based on rules		
125	The proposed solution should have in-built feature for Transaction analysis using Transaction network visualization.		
126	The proposed solution should provide capability for visualization and drilling down into networks		
127	The proposed solution should allow Users of network visualization/ other appropriate visualization to be able to drill down further into networks and view additional links as required		

128	The proposed solution should come with in-built features of multiple instances of network diagrams related to an investigation - that will be dynamically surfaced - by presenting a selected object (such as an alert) as the central object and other relevant connected objects linked as appropriate.		
129	The proposed solution should come with in-built features of making customizations to the network diagrams such as - incremental zooming for better viewing, moving the network diagram around the canvas, adding objects from the network diagram into existing or new investigation workspaces and adding the entire network into existing or new insight documentations		
130	The proposed solution should come with in-built features of the network diagrams within investigation workspaces to be viewed as a table, as a detail list, within a map context, or on a timeline, all as appropriate		
131	The proposed solution should come with in-built features of the network diagrams within investigation workspaces to apply modifications or change settings and properties to one or more selected nodes, add, delete, group, and ungroup nodes and links, expand relationships to perform in-depth investigations and hide or reveal nodes to better surface entities and relationships of interest		
132	The proposed solution should allow additional links and entities which are external to the network data, to be added to the network		
133	The proposed solution should allow Analysts to interact through an in-built network viewer to see entire social networks and the flow of transactions. There should be features to enable expand or trim the network as required, explore communities and individual relationships, and manipulate the network layout, as well as overlay transaction information to show exchanges between two parties. Finally, there should be features to take snapshots and clips of the insights that they develop, collaborate with other investigators and document their findings.		
134	The proposed solution should support network analysis and in-built features such as Network viewer/Node link diagram, Visualize complete networks and relationships through multilevel expansion, Identifies areas of interest and centrality within the network by showing entity closeness, betweenness, influence and more, Node decorators to Help analysts identify entities at a glance and investigators understand network data by highlighting useful information on the node icon view.		
135	The proposed solution should have in-built features for Surveillance and alert creation so that Analysts can author scenarios to uncover anomalous events for triage.		
136	The proposed solution should provide the ability for administrators to monitor and administer workflows. This includes the ability to:		
	• View, suspend, resume or cancel active workflows.		
	• View and release claims on active workflow tasks.		
	• Ability to view running tasks		
	• Shows status and location in overall workflow process		
	• Properties of task		
	• History		
	• Create new workflows from central admin location.		
	• Specify columns to be displayed in Tasks tab and My Tasks homepage control		
137	When creating workflows, the design screens should highlight missing properties on tasks so the Administrator can add the necessary details prior to saving the workflow		
138	The proposed solution should provide users, such as supervisors or managers, with an overview of completed and incomplete workflow tasks as well as reports showing individual user activity. Reports should illustrate the times of peak activity for completion of workflow tasks and allows for optimization of staffing.		
139	The proposed solution should provide an element in the workflow designer to enable administrators to send email notifications at specified points of the workflow.		

140	The proposed solution should have built-in capabilities to assign Alerts/Cases to different strategies and queue for assignment from drop-down		
141	The proposed solution should have features to embed Graphs to understand profiles, Geo-maps to understand locations of persons, organizations, and events		
142	The proposed solution should contain sub-components that are updated upon page refresh, including KPI's/ metrics going out of range and other items of interest that become available		
143	The proposed solution shall provide facility to define Business rules in simple business terms with logical conditions like IF, ELSE, AND, OR etc.		
144	The proposed solution should have capability to enable officers to segregate cases separately for investigators and other control functions using workflow stages		
145	The proposed solution shall enable assessment of registration details for determining / modifying risk profile rating		
146	The proposed solution should have optimization capability to help in allocation of alerts for different geographies / RO / circle members as per severity of investigation		
147	The proposed solution shall provide facility to define rules and set threshold-based alerts for the same on the data used for query and analysis		
148	The proposed solution should allow addition of Additional links and entities which are external to the network data, to be added to the network and changes saved		
149	The proposed solution should allow Networks to be visualized based on a temporal view – so that the chronology of events are depicter through a time slider		
150	The proposed solution should accept parameters for retrieving network entity details and relationships between any two entities and visualize links and networks based on these parameters		
151	The proposed solution should retrieve relationship between any two (specified) links in a network through a "shortest path" algorithm and enable visualization of the relationship.		
152	The proposed solution should have inbuilt business rules engine to implement scenarios with ability to add new scenarios. Scenario/ Rule / Alert management can be created through a simple to use GUI interface where it is possible to add new rules, modify existing alerts etc. with alerts automatically changing as soon as the changes are made		
153	The proposed solution should be able to execute scenarios in specific order. Business rule engine should have capability to change scenario parameters easily		
154	The proposed solution should use updatable user defined tables as decision elements such as: Negative and / or positive files		
155	The proposed solution should have the ability for each transaction to be evaluated by every rule.		
156	The proposed solution should be able to list, by priority, of all rules triggered by a transaction. –		
157	The proposed solution should provide the ability for administrators to configure pages within the end-user application to display lists of objects of a given entity type that meet specific criteria for e.g. High Priority Cases, Medium Priority,		
158	The proposed solution should have capability to visualize the network related to alerts or risk networks. The networks as well as other alert reports should be capable of color coding to highlight risky / high risk entities.		
159	The proposed solution should enable analysts to be able to add comments and make notes in alerts / investigations		
160	The proposed solution should provide reports on alerts		
161	The proposed solution should allow Analyst to be able to make notes in alerts		
162	The proposed solution should allow Alert management team to be able to electronically upload custom watch lists for use in the application		

163	The proposed solution should enable officers to not just identify the entity against whom the alert was created, but also related alerts, related entities (Policies, claims and clients etc.,.) and their interlinkages.		
164	The proposed solution should enable officers to identify areas of scrutiny and further questioning during the pre-audit preparation through desk audit		
165	The proposed solution should enable identification of cases/exceptions for further Investigation based on modus operandi factors discovered from investigated cases.		
	Visualization and Reporting Specifications		
166	The proposed solution analytical reporting should allow 'On-the-fly' hierarchy creation for being able to traverse to lowest information to undertake root cause analysis		
167	The proposed solution analytical reporting should be able to maintain Mobile device logging history and also be able to backlist/whitelist devices		
168	The proposed solution analytical reporting should support exploration of relationships (either transactional or demographic / profile based) of entities through appropriate visualization. Adequate emphasis on core measures such as deviation, size of entity etc. should be depicted as node size / link width etc.		
169	The proposed solution analytical reporting shall have capability to generate analytical reports on the basis of modus operandi factors discovered from investigated cases.		
170	The proposed solution analytical reporting shall enable tracking client/policy post triaging/investigation, it is required to earmark such profiles in the system and to generate reports for associated transactions		
171	The proposed solution analytical reporting shall have capability to generate MIS reports using GUI		
172	The proposed solution analytical reporting should have feature wherein Report can be drill down to most granular level		
173	The proposed solution analytical reporting should have feature wherein Upon identification of actionable items can access the underlying transactional information lead to the exception.		
174	The proposed solution analytical reporting shall have capability to generate MIS reports regarding Ageing of cases: This report should provide date of identification of the fraud case, number of elapsed days since identification, deviation as on date of identification, etc.		
175	The proposed solution analytical reporting should allow collaboration within departments and users by means of commenting and replying. Additional functionality of attaching supporting documents to substantiate the comments should be possible		
176	The proposed solution analytical reporting should be able to enable display of trend within a dashboard with the functionality to zoom the indicators for better view		
177	The proposed solution analytical reporting, in case of change in the underlying database, should provide functionality of auto-repairing of the reports		
178	The proposed solution analytical reporting should support Printing dashboard - Should allow printing of individual dashboards and email options		
179	The proposed solution Should support advanced analytics, statistical analysis, forecasting and advanced aggregation		
180	The proposed solution should provide facility to generate static or dynamic interactive visualization charts and graphs		
181	The proposed solution should support analysis of cases to determine patterns that may help the department in optimizing existing resources and reducing pending cases		
182	The proposed solution should support Visual depiction, highlighting and color coding based on entity risk should be reflected in the network visualization/ other appropriate visualization		

183	Provides variety of charts are including bar/3-D bar with multiple lines, pie/3-D pie, line, scatter, heat map, bubble, animated bubble, tabular data formats, etc.,		
184	Graphical Data format / Representation - Bar Chart, Targeted Bar Chart, Waterfall Chart, Line Chart, Pie Chart, Scatter Plot, Time Series Plot, Bubble Plot, Tree Map, Dual Axis Bar Chart, Dual Axis Line Chart, Dual Axis Bar Line Chart, Dual Axis Time Series Plot, Schedule Chart, Vector Plot, Numeric Series Plot, Needle Plot, Step Plot, Dot Plot, Butterfly Chart, Stock High Low Plot, Stock Volume & Volatility, Bubble Change Plot, Comparative Time Series Plot		
185	Controls & Filters (Global & Local) - Drop Down List, Simple List, Button Bar, Text Input, Slider		
186	Containers - Vertical, Horizontal, Stack, Prompt Containers		
187	The proposed solution should support understanding of alert performance in terms of true positives / false positives etc. should be assessable and measurable through reports		
	Text Analytics		
188	The proposed solution should combine text data wrangling, text data exploration, visualization, text parsing, topics, concepts, categories and sentiment all in a single framework, integrated in-memory processing environment.		
189	The proposed solution must have a utility capable of visualizing and extracting (text-mining) information relevant for the alerts from internal documents (such as claim documents, reports, etc.,)		
190	The proposed solution should be an interactive, user-friendly, web-based visual and programming interfaces		
191	The above referred library should be configurable for addition/deletion/modification of keywords/phrases		
192	The text mining utility should be capable of accepting bulk upload of documents		
193	After processing document reference and the keyword searched to be included in the alert message		
194	The text mining utility should have algorithms to minimize false positives (Eg: Standard NLP libraries, stemming/lemmatization capabilities etc.)		
195	Text mining utility should have intelligent self-learning capability		
196	The proposed solution uses natural language processing (NLP) to analyse and transform text into formal representations for text processing and understanding. This includes automated text parsing, word and sentence tokenization, segmentation, stemming, compound decomposition, synonym detection, part-of-speech tagging, categorization documents, named entity recognition and semantic parsing. It should also directly support the use of regular expressions (REGEX) for matching purposes.		
197	The proposed solution's natural language should be able to provide entity and fact extraction, categorization, search and summarization from unstructured data.		
198	The proposed solution should have Smart search applications by categorizing documents, associating entity relationships and building a contextual search application for exploration within text, using machine learning and semantic analysis		
199	The proposed solution combines machine learning with business knowledge to generate new rules for improved accuracy.		
200	The proposed solution should provide automatic discovery of topics for initial taxonomy development:		
	• Automated machine discovery identifies the core themes in the input document collection with associated relevance scores.		
	• Term relationships within topics can be interrogated and explored with term clouds (with configurable thresholds), interactive term maps and by drilling into topics to evaluate relevancy and refine discovered topics.		
201	Ability of generation of configurable categorization rules; Automated initial category rule definition based on user-refined generated topics. Easy-to-understand Boolean rule definitions create the categorization model (i.e., taxonomy). System-generated rule robustness is detailed in true positive, false positive and false negative visual diagnostics.		

202	The proposed solution should employ sophisticated dimension reduction techniques that enable advanced filtering through weighting, integrated spell checking and transformation of qualitative data into compact formats.		
203	The proposed solution should combine Statistics and linguistics to provide more accurate sentiment analysis results based on Statistical modelling: Provides predefined default parameters – that can also be configured – to identify the document sentiment from text. Lets subject-matter experts define the elements to be examined for sentiment assessment. Hybrid approach: Provides the unique ability to use both statistical rigor and linguistic rules to define sentiment models driving more detailed sentiment evaluations.		
204	The proposed solution should provide named entity recognition concepts. Predefined concepts are available – no rule writing is required. These address common entity definitions for date, location, time, etc. Custom concepts can be written using a suite of predefined operators.		
205	The proposed solution should seamlessly integrate with existing systems and open-source technology.		
206	Out-of-the-box analytical programming interfaces for text summarization, text data segmentation, text parsing and mining, topic modelling, text rule development and scoring, text rule discovery, term mapping and topic term mapping, conditional random field and search.		
207	The proposed solution should include additional Text Mining features such as - Output lists of terms to drop/keep and term frequency counts, easy drag and drop between keep and drop terms, ability to apply customized start and stop lists (for terms to include/exclude from processing), ability to include custom-defined categories and custom concepts		
208	The proposed solution should provide in-built feature of detailing the status of each step of text model creation, processing status and message dialogue to help diagnose model development issues (such as an insufficient number of documents in the collection to generate topics).		
209	The proposed solution should provide in-built project management options that permit multiple text models to be simultaneously developed and run, with associated descriptions indicating each model's development status		
	Image Analytics		
210	The proposed solution should use image analytics techniques for various use-cases using different types of medical images such as diagnostic report images, discharge summary etc.		
211	The proposed solution must have capability for image segmentation to detect nature and extent of presence or absence of disease/sickness as per due diligence diagnostics reports.		
212	The proposed solution should be using algorithms for image matching and de-duplication models.		
	Encryption and Security		
213	Standard encryption/decryption techniques/policies should be enabled		
214	Enabling robust security measures to protect data stored in the cloud. This includes encryption of data at rest and in transit, access controls, and multi-factor authentication to prevent unauthorized access		
215	The system should comply with data protection regulations which includes implementing measures to protect customer privacy rights		
216	The system should ensure that the personal information of the users is secure and should comply with regulations, such as The Digital Personal Data Protection Act 2023 (DPDPA 2023), the General Data Protection Regulation (GDPR). The system should ensure that controls are align with requirements of The Health Insurance Portability and Accountability Act (HIPAA)		
	Portal and Dashboard		
217	The solution to create a web portal for administrative purposes and to view the dashboards / reports with filters. The portal should use responsive technology to enable rendering on various formats including desktops, laptops, tablets and mobile technology. The solution is expected to provide 50 standard reports / dashboards of varying complexity to be derived from the datastore.		

	The dashboards could be of the following reports (including but not limited to): • Upload statistics of each partner – hospitals, networks, customers etc • Error rate and error types • Quality of data and fill rates • Time to process • TAT and MIS reports		

Functional Specifications

S.N.	Functional Specifications	Compliance (Yes/No)	Remarks
1	The solution shall have the capability to improve the operational efficiency of the Insurance Companies by integrating structured, semi structure and unstructured data from multiple sources such as Proposal form, Policy, historical information, financial documents, social media, medical documents etc., to reconcile the suggested changes/orders and provide intelligence on mismatches based on the order of priority.		
2	The solution shall have the capability to analyze suspicious claims and provide insights into the cases to be further investigated by the Insurance Company.		
3	The solution shall have the capability to conduct post issuance validation and robust data platform for acknowledge validation, acceptance, and analysis on a continuous basis.		
4	The solution shall have the capability to continuously monitor entities like policy holders, claims, payments, claim payouts etc. for estimating the Risk, Compliance, and aid in the Internal Audit & Fraud/ Revenue abuse		
5	The solution shall have the capability to evaluate audit trail/log involved in policy lifecycle and transactions lifecycle to alert the unauthorized activities promptly		
6	The solution should have the capability to identify Back door entry of blacklisted entities and parties using manipulative KYC documentation		
7	The solution should have the capability to identify multiple instances of similar/ same entities like policy holders, policies, claims , hospitals, medical professionals , insurance intermediaries and employees of any other stakeholders etc.		
8	The solution should have the capability to find out correlated policy holders, policies, claims, accounts etc. through common addresses, father name, mobile no. email address , national identifier and other related demographics. (any attribute/parameter attached to member level data /claim level data we chose to provide)-		
9	The solution should aid in a Risk-based underwriting to assess the fraud risk associated with each policy more accurately.		
10	The solution should have robust analytical and decision support capabilities to significantly reduce the claims authorization TAT (Turnaround Time) when they are subjected to investigation due to high risk score or low application score.		
11	The solution shall have a Risk-based underwriting capability that relies on objective data and algorithms, to evaluate fraud risks which can help reduce human bias in the decision-making process leading to fairer and more consistent underwriting decisions.		
12	The solution shall have an Early warning system that aids in monitoring of events (Issuance, application, payments, address update, service request etc.,), entities (Policyholders, Nominees, life assured, Agents, Demographics, Account number etc.,), and their networks (Known/Unknown and/or disclosed /undisclosed relationship between the entities).		
13	The solution shall have the capability to efficiently evaluate the validity and eligibility of claims, ensuring that legitimate claims are processed and validated promptly.		
14	The solution shall have the capability to detect unusual patterns or indicators of potential fraud, helping insurers identify fraudulent claims more effectively		

15	The solution shall have the capability to detect suspicious/ fraudulent acts of using a stolen identity, creating a false death certificate, or even staging a fake accident or crime		
16	The solution shall have the capability to identify entities misrepresenting information on their insurance application to secure a policy with lower premiums		

Note : The engine should continuously upgrade and evolve and should not be restricted.

CAPABILITIES OF FRAUD DETECTION AND INVESTIGATION

Sr.No	Capabilities of Fraud Detection and Investigation	Compliance (Yes/No)	Remarks
1	Modeling Engine		
2	Network Fraud Modelling and Monitoring Platform		
3	Reporting Engine		
4	Search and Discovery : *Free-text search. • Form search and Query Builder. • Filters and facets. • Geospatial search, exploration and visualization. • Text analytics visualization		
5	Surveillance Engine (Continuous Monitoring) : * Author scenarios • Restrict defined scenarios for parameter adjustment by role. • Scenario testing. • Creation of score based on scenario(s). • Batch or on-demand execution		
6	Entity analytics: * Entity resolution. • Network analytics and visualization. • Network link expansion. • Network node decorator and enrichment.		
7	Transaction analysis • Transaction network visualization		
8	Single Unified Platform • Gather data from across the enterprise and external sources within a single interface. • Use alert queues to bring the highest risk cases to the top of the list in order to maximize resources and return on investment. • Increase the speed of triage, investigation and audits with detailed descriptions of why an individual or business has attracted a high fraud propensity score. •Automatically view graph networks of linked individuals and other key entities and data points (e.g. address, phone number, bank account, IP address etc.) in order to quickly identify and understand relationships and hidden patterns of connectivity that exist with your data		
9	Advanced Intelligence Search		
10	Use fuzzy matching to improve entity resolution across data sources that don't share a unique identifier		
11	Dramatically improve detection rates, while minimizing false positives that drain investigative and audit resources		
12	Assess subjects against their peer groups, through anomaly detection and peer grouping. This approach identifies outliers, detects identity theft, and helps identify new or unknown approaches to fraud		
13	Compare all data points about a particular policyholder, claimant or service provider to known past cases of fraud, waste or abuse with predictive analytics and prioritize these alerts as early as possible to minimize related losses.		
14	Easily identify criminal fraud networks and related risks using network link analysis (social network analysis).		

15	Anomaly Detection : Determine new potential areas of insurance fraud by looking for outliers/anomalous behavior across a number of key datasets such as service providers, claimants, claims and applications. Analyze the characteristics of a new claim or application, using a series of statistical models such as peer group comparison, clustering and trend analysis to understand whether it could be a potential anomaly		
16	Text Mining: Solution should have the capability to maximize the value of current information assets buried within unstructured data. However, this data will need to be assessed both against readiness for use and accessibility.		
17	Network Analysis/Link Analysis		
18	Alert Generation & Management		
19	Intelligent Fraud Repository		
20	Case Management		
21	Heuristics based fraud scenario monitoring		
22	Reporting		

Integration requirements

SN	Integration Requirements	Compliance (Yes/No)	Remarks
1	Integration with external portals including but not limited to, Geo tagging, , CIBIL, PEP, LexisNexis, UIDAI, negative databases, Central Fraud Registry, Sanchar Sathi, upcoming Central Suspect Registry, Open Government Data Platform, Credit Banks, State Government websites for Crop related data etc.		
2	Integration with third party solutions including but not limited to IDFY, IDMERIT, etc.		
3	Integrations with internal portals including but not limited to CAS, CRM, PAS, DMS, etc.		
4	Ability to integrate with other existing fraud solutions in place and work parallelly		
5	Ability to integrate with social media platforms		
6	Ability to integrate with document management solution		
7	Ability to integrate with CCM and configure & customize rules as per requirements		
8	Ability to integrate with GIC (General Insurance Council) & IIB to identify claims with multiple insurance companies for same accident or injury to receive multiple payouts		
9	Ability to integrate with GIC (General Insurance Council) , LIC (Life Insurance Council) & IIB to identify claims with multiple insurance companies for same accident or injury to receive multiple payouts		
10	Ability to integrate with Government Secure Database to identify duplicate insurance policies taken through different channels and insurers on same crop in Crop insurance		

UI/UX requirements

SN	UI/UX Requirements	Compliance (Yes/No)	Remarks
1	AI driven interfaces which are responsive to individual user behaviors to reduce cognitive load and support faster decision making		
2	Clear and intuitive interfaces which improves decision making and accuracy to reduce false positives		
3	Tailored interfaces to match workflow and preferences of the users		
4	User centric approach for UI / UX configuration and customization of case management workflows		
5	Visually engaging interfaces and clear presentation of relevant information under case management module allowing easy identification of fraudulent cases		
6	Availability of designs for varied user personas and configuration of the same		
7	Intuitive Interfaces for compliance management with visually appealing alerts		
8	Visually appealing representation of data through interactive dashboards to easily identify patterns and anomalies		

9	Intuitive UI / UX for rule management with search, modify, create, configure & delete options		
10	UI to configure parameters with tooltips and generate reports		
11	Intuitive UI in case management module to easily retrieve documents and verify data during case management		
12	Use of supportive icons and tooltips to enable faster and accurate decision making by investigators		

Deliverables expected by NIACL for Fraud Detection and Investigation

Sr.No	Deliverables expected by NIACL for Fraud Detection and Investigation	Compliance (Yes/No)	Remarks
1	Alert Tracking and Triaging with Reports		
2	Network Modeling and Scoring Platform		
3	Fraud Scenario Modelling		
4	Fraud Alert Analysis Report		
5	1. Multi level Network exploration		
6	2. Community Detection		
7	3. Network Time travel		
8	4. Entity Linkage Strength Scoring		
9	5. Automatically assess risk and detect suspicious claims		
10	6. Automatically detect previously unknown relationships between claimants, doctors, agents, hospitals, addresses, bank accounts		
11	Manage potential fraudulent cases through a workflow driven approach		
12	Generate reports, measure claims statistics, identify fraud hotspots and measure the performance and effectiveness of the current detection strategy		
13	Discover new and emerging trends and patterns of collusiveness and frauds		
14	Reduce No of False Positives Fraud alerts		
15	Automated consistent and transparent process and traceable decision making		
16	Multilayered Detection methods to detect fraud at individual claim, business transaction, entity or network level		
17	Social network analysis (for linking entities and visualising relationships);		
18	Restrict data access at the record and element level through a powerful security model.		
19	Should have the analysis capability for detecting, linking and aggregating fraud risks and related alerts which entails sophisticated network attribute scoring models, that visually represent links in data from multiple systems in a single environment.		
20	Should be able to generate alerts across claim/or new business application, entity, associated social network to raise alerts on high risk cases for fraud.		
21	Should have the capability to manage the routing and processing of potentially fraudulent alerts and assists in proactive triage within the investigative function		
22	Each time an alert or a fraud referral/case is completed, the results are stored within the Intelligent Fraud Repository as Known Outcomes. This repository of 'Known Outcomes' can then be utilised in the application of supervised analytics/predictive models within the Alert generation process		
23	The solution: • Should allow system administrators to access the business rules, models, and network analytics run within the alert generation process; • Provides the ability to generate and test the validity of new fraud business rules and analytical models; Includes an easy-to-use GUI that guides users through a repeatable process for		

	registering, testing and validating models. It also supports the champion challenger capability of confirming the best fit models.		
24	• Should be able to provide the investigation team with an integrated end-to-end solution to manage cases. These include: • Adaptable workflows which provide increased governance and a structured and consistent approach to investigations, with review and sign-off steps included where required. • Tasking templates that promote collaboration and ensure tasks are tracked throughout the investigation process. • Intuitive page designs and controls that lead investigators through the steps of the investigation and facilitate full case management capabilities for even the most complex of cases. Specific controls can be configured to allow for updates and additional data to be recorded as the investigation progresses. An event log that provides users with an overview of the activities involved in an investigation, including due dates and priorities. • Drop down lists, which ensure data entry is accurate and consistent, can also easily be changed and updated by Customer Name to reflect changes in the underlying data and/or business processes. A relationship manager, which allows entities to be linked to the case so that investigators have a complete view of all relevant information without having to run additional searches. • Attachments which allow for relevant documents, including emails and images, to be uploaded into an investigation. The contents of these uploads can index for search, allowing investigators to quickly find a case simply by searching for a related term or phrase. • Hyperlinks, that allow users to quickly access key sites used within an investigation through a single NIACL .		
25	Reporting toll should be a comprehensive, easy-to-use reporting software solution that integrates with the solution's analytical and data management components to provide a complete reporting environment for the fraud solution. It includes role based, self-service interfaces for all types of users within a well-defined fraud organization and a centralized point of administration		

Scope of Work:

SN	Fraud Analytics – Detection and Investigation	Compliance (Yes/No)	Remarks
1	Supply, Install, configure, customize , integrate and deploy to implement suitable software and hardware components to establish state of the art analytics and BI platform. This will include:		
2	a. **Continuous Policy Monitoring & Early Warning**: System driven Post issuance verification and validation analytics. Continuous monitoring of policies using the policy profiling across renewal, servicing and risk patter using hybrid analytics (Combination of business rules & Policy, predictive model and anomaly detection models)		
3	a.1. **Screening and Entity Resolution:** Analytics to enable Client/Agent Onboarding screening deploying data quality techniques including fuzzy match and associated sensitivity levels. Ongoing screening / entity resolution match the clients/agents periodically against the internal or external watchlist.		
4	a.2 **Network Link Analytics & Alerting**: Analytics to identify and alert suspicious relationships across all parties and entities (Applicant, Policy Holder, Insured, Nominee, Agent, Bank Account, GST, PAN, Mobile etc.,).		
5	a.3 **Claim Fraud Assessment & Scoring**: System driven claims assessment algorithm and scorecard to efficiently evaluate the validity and eligibility of claims, ensuring that legitimate claims are paid promptly. Automated and data-driven decision-making analytical insights that can expedite the fraud investigation process, to take swift action against fraudulent claims.		

Annexure- III

DEVIATIONS FORMAT

S/N	Bidder's Name	Page No. (tender Ref)	Clause(tender Ref)	Description in the tender (tender Ref)	Deviation Details	Reasons for deviation
1						
2						

Note: - NIACL reserves the right to accept/reject any or all the deviations shown by the bidder. The format of GeM is also acceptable.

Authorized Signatory
(Name & Designation, seal of the firm)

Annexure-IV

QUERIES FORMAT

Sr. No	Bidder Name	Page No. (tender Ref)	Clause (tender Ref)	Description in the tender (tender Ref)	Query
1					
2					

Note: Queries may be communicated only GeM portal. No queries will be accepted on telephone or through any other means. The queries should be sent in .xls/.xlsx format with above fields only. The format of GeM portal is also acceptable.

Annexure-V

NON-BLACKLISTING UNDERTAKING

Tender Ref: NIA/HEALTH/2025-26/FWA

We, M/s _____, participating in the bid, confirm that we have not been disqualified/blacklisted/de-panelled and the product quoted is not disqualified/blacklisted/de-panelled by any Central/State Government Department/Public Sector Banks/Financial Institutions in India including NIACL during the last three years starting from June, 2022 till last date of submission of this tender.

Dated at _____this _____day of _____20___

Signature of the Company Secretary

Signature Name:

Designation:

Name & Address of the company:

Seal of the Company

Annexure-VI

Commercial Bid Format

SN	Cost Head	Year 0 (Implementation and Hypercare)	Year 1	Year 2	Year 3	Total Cost	Year 4	Year 5
1.	Licenses and Software Cost							
2.	Infrastructure Cost (Cloud Platform) Production, DR and UAT environment							
3	One time implementation Cost including integration							
4	Support Cost (L1, L2 and L3)							
5	Any other cost with details							
Total Cost inclusive of GST (Total of Year 0 , Year 1, Year 2 , Year 3 to be considered for commercial evaluation).								

Note:

- Year 1 will start after successful implementation, signoff and hyper-care
- Total cost for Year 0, Year 1,Year 2,Year 3 to be considered for commercial evaluation.
- Bidder need to provide cost for Year 4 and 5 which can be opted at the discretion of the Company and when opted, becomes binding on the bidder.

Additional Man-month cost to manage change request in agreement with company (Post completion Go Live and signoff as per RFP)

S.No	Type	Cost (INR per month) inclusive of GST
1	Functional Experts	
2	Technical Experts (Data, Integration, Developers)	
3	Testers	
4	Data Modelers	

Annexure-VII

AGREEMENT DRAFT
(Should be on Rs.100/- stamp paper)

This agreement was made on this _____ day of _____between _____ hereinafter called the "BIDDER" and THE NEW INDIA ASSURANCE CO. LTD., hereinafter called "THE COMPANY" sets forth the terms and conditions for the “THE PROCUREMENT OF AI/ML BASED SOLUTION FOR MONITORING AND INVESTIGATION OF FRAUD, WASTE & ABUSE OF HEALTH INSURANCE CLAIMS

Note:
A detailed agreement providing the RFP clauses and provisions will be provided to the successful bidder.

a) SIGNED SEALED & DELIVERED BY
THE WITHIN NAMED INSURANCE COMPANY

Chief Manager

_____
In the presence of

Witnesses: 1 _____

Witnesses: 2 _____

b) SIGNED SEALED & THE WITHIN
DELIVERED BY WITHIN NAMED(BIDDER)

_____
In the presence of

Witnesses: 1 _____

Witnesses: 2 _____

Annexure-VIII

NDA FORMAT

(Should be on Rs.100/-stamp paper)

This confidentiality and non-disclosure agreement is made on the.....day of....., 20.... BETWEEN (Bidder), (hereinafter to be referred to as "-------") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns a company incorporated under the Companies Act, 1956 and having its principal office at .....(address).

AND THE NEW INDIA ASSURANCE COMPANY LIMITED (hereinafter to be called "NIACL") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns having its Registered Office at ……. (address) on the following terms and conditions:

WHEREAS, in the course of the business relationship between the aforesaid parties, both the parties acknowledge that either party may have access to or have disclosed any information, which is of a confidential nature, through any mode and recognize that there is a need to disclose to one another such confidential information, of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure;

NOW THEREFORE, in consideration of the mutual promises contained herein, the adequacy and sufficiency of which consideration is hereby acknowledged and agreed, the parties hereby agree as follows: –

This Agreement shall apply to all confidential and proprietary information disclosed by one party to the other party, including information included in the caption 'Definitions' of this Agreement and other information which the disclosing party identifies in writing or otherwise as confidential before or within thirty days after disclosure to the receiving party ("Confidential Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, electronically or through visual observation or by any other means to one party (the receiving party) by the other party (the disclosing party) provided any information which has been disclosed in an intangible form shall reduce to writing within fifteen (15) business days for such information to be deemed as Confidential Information

1) DEFINITIONS

a) CONFIDENTIAL INFORMATION means all the information of the Disclosing Party which is disclosed to the Receiving party pursuant to the business arrangement whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, inventions, techniques, processes, plans, algorithms, software programs, source code, semiconductor designs, schematic designs, business methods, customer lists, contacts, financial information, sales and marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs, operations, strategies, inventions, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription lists, customer lists, photo files, advertising materials, contract quotations, charity contracts, documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, statistics, facts, figures, numbers, records,

professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barristers, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors, Surveyors, Loss Assessors, Investigators, Forensic experts, Scientists, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Indian Evidence Act, 1872, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives,, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defences taken before a Court of Law, Judicial For a, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Disclosing Party. The above definition of Confidential Information applies to both parties equally; however, in addition, without limitation, where the Disclosing Party is the NIACL, no information that is exempted from disclosure under section 8 or any other provision of Right to Information Act, 2005 shall at any time be disclosed by the Receiving Party to any third party.

b) MATERIALS mean including without limitation, documents, drawings, models, apparatus, sketches, designs and lists furnished to the Receiving Party by the Disclosing Party and any tangible embodiments of the Disclosing Party's Confidential Information created by the Receiving Party.

2) <u>COVENANT NOT TO DISCLOSE</u>

The Receiving Party will use the Disclosing Party's Confidential Information solely to fulfill its obligations as part of and in furtherance of the actual or potential business relationship with the Disclosing Party. The Receiving Party shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Disclosing Party or its subsidiaries or affiliates, and shall not disclose the Confidential Information to any unauthorized third party. The Receiving Party shall not disclose any Confidential Information to any person except to its employees, authorized agents, consultants and contractors on a need to know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms at least as restrictive as those specified in this Agreement.

In this regard, the agreement entered into between the Receiving Party and any such person/s shall be forwarded to the Disclosing Party promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the Receiving Party shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information. The Receiving party shall use at least the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use. In no event, shall the Receiving Party take all reasonable measures that are lesser than the measures it uses for its own information of similar type. The Receiving Party and its Representatives will immediately notify the Disclosing Party of any use or disclosure of the Confidential Information that is not authorized by this Agreement. In particular, the Receiving Party will immediately give notice in writing to the Disclosing Party of any unauthorized use or disclosure of the Confidential Information and agrees to assist the Disclosing Party in remedying such unauthorized use or disclosure of the Confidential Information. The Receiving Party and its Representatives shall not disclose to any

person including, without limitation any corporation, sovereign, partnership, company, Association of Persons, entity or individual

i) the fact that any investigations, discussions or negotiations are taking place concerning the actual or potential business relationship between the parties,

ii) that it has requested or received Confidential Information, or

iii) any of the terms, conditions or any other fact about the actual or potential business relationship.

This confidentiality obligation shall not apply only to the extent that the Receiving Party can demonstrate that:

a) The Confidential Information of the Disclosing Party is, or properly became, at the time of disclosure, part of the public domain, by publication or otherwise, except by breach of the provisions of this Agreement; or

b) was rightfully acquired by the Receiving Party or its Representatives prior to disclosure by the Disclosing Party;

c) was independently developed by Receiving Party or its Representatives without reference to the Confidential Information; or

d) the Confidential Information of the Disclosing Party is required to be disclosed by a Government agency, is the subject of a subpoena or other legal or demand for disclosure; provided, however, that the receiving party has given the disclosing party prompt written notice of such demand for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order prior to such disclosure.

e) is disclosed with the prior consent of or was duly authorized in writing by the disclosing party.

3) RETURN OF THE MATERIALS

Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the receiving party's counsel, solely for the purpose of proving the contents of the Information.

4) OWNERSHIP OF CONFIDENTIAL INFORMATION

The Disclosing Party shall be deemed the owner of all Confidential Information disclosed by it or its agents to the Receiving Party hereunder, including without limitation all patents, copyright, trademark, service mark, trade secret and other proprietary rights and interests therein, and Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as granting any rights to the Receiving Party, by license or otherwise in or to any Confidential Information. Confidential Information is provided "as is" with all faults. By disclosing Information or executing this Agreement, the disclosing party does not grant any

license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event, shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

5) REMEDIES FOR BREACH OF CONFIDENTIALITY

1) The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors) and that any unauthorized disclosure of any Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

2) The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

6) TERM

This Agreement shall be effective on the first date written above and shall continue in full force and effect for the term of the assignment and for a period of two years thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind both parties, and also their successors, nominees and assignees for the term of the assignment and for a period of two years thereafter.

7) GOVERNING LAW & JURISDICTION

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of

law provisions. Any proceedings arising out of or in connection with this Agreement shall be brought only before the Courts of competent jurisdiction in Mumbai.

8) ENTIRE AGREEMENT

This Agreement sets forth the entire agreement and understanding between the parties as to the subject-matter of this Agreement and supersedes all prior or simultaneous representations, discussions, and negotiations whether oral or written or electronic. This Agreement may be amended or supplemented only by a writing that is signed by duly authorized representatives of both parties.

9) WAIVER

No term or provision hereof will be considered waived by either party and no breach excused by the Disclosing Party, unless such waiver or consent is in writing signed by or on behalf of duly Constituted Attorney of the Disclosing Party. No consent or waiver whether express or implied of a breach by the Disclosing Party will constitute consent to the waiver of or excuse of any other or different or subsequent breach by the Receiving Party.

10) SEVERABILITY

If any provision of this Agreement is found invalid or unenforceable, that part will be amended to achieve as nearly as possible the same economic or legal effect as the original provision and the remainder of this Agreement will remain in full force.

11) NOTICES

Any notice provided for or permitted under this Agreement will be treated as having been given when (a) delivered personally, or (b) sent by confirmed telecopy, or (c) sent by commercial overnight courier with written verification of receipt, or (d) mailed postage prepaid by certified or registered mail, return receipt requested, or (e) by electronic mail, to the party to be notified, at the address set forth below or at such other place of which the other party has been notified in accordance with the provisions of this clause. Such notice will be treated as having been received upon actual receipt or five days after posting. Provided always that notices to the NIACL shall be served on the Information Technology Department of the Company's Head Office at Mumbai and a CC thereof be earmarked to the concerned Branch, Divisional or Regional Office as the case may be by RPAD & email.

IN WITNESS, WHEREOF THE PARTIES HERE TO have set and subscribed their respective hands and seals the day and year herein above mentioned.

a) SIGNED SEALED & DELIVERED BY THE WITHIN NAMED INSURANCE COMPANY

Deputy General Manager

_____

In the presence of

Witness:1 _____

Witness:2_____

b) SIGNED SEALED & DELIVERED WITHIN NAMED (BIDDER)

_____

In the presence of

Witness:1_____

Witness:2 _____

Annexure-IX

Integrity Pact Instructions

The Integrity Pact (IP) duly signed by the authorized official of NIA and the Contractor, will form part of the contract / supply order. Performa of the IP is enclosed along with the tender document (Annexure-XI)and shall be returned by the bidder along with the technical bid, duly signed by authorized person.All the pages of the IP shall be duly signed by the same authority. Bidders failure to return the IP along with the bid, duly signed may lead to outright rejection of such bid.

Details of Independent External Monitors (IEMs):

SN	Name	Contact No	Email ID
1	**Shri Deepak Chaturvedi**	9930408711	chaturvedideep@rediffmail.com
2	**Shri Kishore Kumar Sansi**	9686009000	kishoresansi1@gmail.com

Annexure-X

INTEGRITY PACT

(Should be on Rs.100/-stamp paper)

INTEGRITY PACT Between The New India Assurance Company Limited (NIA) hereinafter referred to as "The Principal", and …… hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for …… The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

1) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -
   a) No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
   b) The Principal will, during the tender process, treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
   c) The Principal will exclude from the process all known prejudiced persons.
2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ Contractor(s) which term shall include Vendor(s)/Agency(ies)/Sub-contractor (s) if any, etc.

1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.
   i) The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

   ii) The Bidder(s)/ Contractor (s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
   iii) The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including

information contained or transmitted electronically.

iv) The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any. Similarly, the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/ Contractor(s). Further, as mentioned in the Guidelines all the Payments made to the Indian agent/ representative have to be in Indian Rupees only. The "Guidelines on Indian Agents of Foreign Suppliers" is placed at page nos. 6-7.

v) The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents or any other intermediaries in connection with the award of the contract.

vi) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

The "Guidelines on Banning of business dealings" is placed at Page nos. 8-15.

Section 4 – Compensation for Damages

1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public-Sector Enterprise in India that could justify his exclusion from the tender process.
2) If the Bidder makes an incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.
2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.
3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply

with the obligations under this agreement.

2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman cum Managing Director, New India.
3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor (s)/ Subcontractor(s) with confidentiality.
4) The principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6) The Monitor will submit a written report to the Chairman cum Managing Director (CMD) of NIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.
7) If the Monitor has reported to the CMD, NIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the CMD, NIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
8) The word 'Monitor' would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of NIA.

Section 10 – Other provisions

1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Head Office of the Principal, i.e. Mumbai.
2) Changes and supplements as well as termination notices need to be made in writing.
3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

(For & On behalf of the Principal) (For& On behalf of Bidder/Contractor)

(Office Seal) (Office Seal)

Place ----------
Date ----------

Witness 1:
(Name & Address)

Witness 2:
(Name & Address)

GUIDELINES FOR INDIAN AGENTS OF FOREIGN BIDDER(S)/ CONTRACTOR(S)

which term shall include Vendor(s) /Agency(ies)/Sub-contractor (s) if any,etc.

1) REGISTRATION OF AGENTS

1.1) There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with NIA shall apply for registration in the prescribed Application – Form.

1.2) Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by NIA.

1.3) Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian Representative is working on the basis of salary or as retainer, a written document to this effect should be submitted by the party (i.e. Principal) before finalizing the order.

2) DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA, IF ANY.

2.1) Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1) The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Company, it shall be confirmed whether it is real substantial Company and details of the same shall be furnished.

2.1.2) The amount of Commission/Remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3) Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by NIA in Indian Rupees only.

2.2) Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1) The name and address of the foreign principals indicating their nationality as well as their status, i.e., whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2) The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.

2.2.3) Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by NIA in India in equivalent Indian Rupees on

satisfactory completion of the Project or supplies of Stores and Spares in case of operation items.

2.3) In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission/ remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4) Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by NIA. Besides this there would be a penalty of banning business dealings with NIA or damage or payment of a named sum.

****

GUIDELINES ON BANNING OF BUSINESS DEALING

CONTENTS

1) Introduction

1.1) The New India Assurance Company Limited (NIA), being a Public-Sector Entity, has to ensure preservation of rights enshrined in the Constitution. NIA has also to safeguard its commercial interests. NIA deals with Agencies (which term shall include Bidders/ Vendor(s)/ Agency(ies)/ Contractor(s)/ Sub- contractor(s) if any, etc.), who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of NIA to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure compliance with the constitutional mandate, it is incumbent on NIA to observe principles of natural justice before banning the business dealings with any Agency.

1.2) Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if tendered, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2) Scope

2.1) NIA reserves its rights to remove any such Agency from its list of approved suppliers /

contractors or to ban business dealings if it is found to have committed misconduct and also to suspend business dealings pending investigation. Such stipulation should be incorporated in every Sale/Purchase/Work Order.

2.2) Similarly, in case of sale of material, NIA reserves its rights to remove any such Agencies / customers / buyers from the approved list, who indulge in lifting of material in unauthorized manner. Such stipulation should be incorporated in every Sale/Purchase/Work Order.

2.3) However, absence of such a clause does not in any way restrict the right of Company (NIA) to take action / decision under these guidelines in appropriate cases.

2.4) procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5) These guidelines apply to the entire Liaison and other offices of NIA located in India, but not to any branch, representative, subsidiary or other offices of NIA outside India.

2.6) It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7) The banning shall be with prospective effect, i.e., future business dealings.

3) Definitions

In these Guidelines, unless the context otherwise requires:

i) 'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer shall mean and include a public limited company or a private limited company, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor/ Supplier / Purchaser / Customer/ Bidder/ Tenderer in the context of these guidelines is indicated as Agency.

ii) 'Inter-connected Agency' shall mean two or more companies having any of the following features:

a) If one is a subsidiary of the other.
b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;
c) If management is common;
d) If one owns or controls the other in any manner;

iii) 'Competent Authority' and 'Appellate Authority' shall mean the following:

a) For Companywide (entire NIA) banning, the CMD NIA shall be the Competent Authority as per these guidelines.
b) For consideration and passing orders on First Appeals against the order of the CMD NIA on banning, Executive Committee (EC) of the Board of NIA shall be the 'Competent Authority'.
c) In case the supplier/vendor/contractor etc. is not satisfied with the decision of the First Appellate Authority, it may approach NIA Board as Second Appellate Authority.
d) CMD, NIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines, except in the matter of Appeals as specified above.

iv) 'Investigating Department' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department of NIA, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) 'List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders

/ Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers etc.

4) Initiation of Banning/ Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of NIA may also be competent to advise such action.

5) Suspension of Business Dealings

5.1) If the conduct of any Agency dealing with NIA is under investigation by any department, the CMD NIA may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the CMD NIA, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2) The order of suspension shall be communicated to all Departmental Heads within NIA. During the period of suspension, no business dealing may be held with the Agency.

5.3) As far as possible, the existing contract(s) with the Agency may continue unless the CMD NIA, having regard to the circumstances of the case, decides otherwise.

5.4) If the gravity of the misconduct under investigation is very serious and it would not be in the interest of NIA as a whole, to deal with such an Agency pending investigation, the concerned General Manager may send his recommendation to CMD NIA along with the material available. If CMD NIA considers that depending upon the gravity of the misconduct, it would not be desirable for NIA and allits offices and Subsidiaries to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the offices of NIA, including Branch, Liaison and Representative offices by the CMD NIA, a copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue. Suitable advisories may also be issued to Subsidiaries of NIA.

5.5) For suspension of business dealings with Foreign Agencies/ Contractors/ Vendors etc.(hereinafter referred to as Agency), following shall be the procedure :-

i) Suspension of the foreign agency (ies) shall apply throughout the Company. Subsidiaries / liaison offices would be suitably advised.

ii) Based on the complaint forwarded by General Manager of the department concerned or received directly by Vigilance Department, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of NIA to continue to deal with such agency, pending investigation, Vigilance Department may send such recommendation on the matter to General Manager of department concerned to place it before a Standing Committee consisting of the following:

1. **GM Finance,**
2. **GM O.S.D. – Convener of the Committee**
3. **GM I.T.M.G.**
4. **GM (Any Other)**

The committee shall expeditiously examine the report, give its comments/recommendations within twenty-one days of receipt of the reference by Head of concerned department.

5.6) If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7) It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6) Ground on which Banning of Business Dealings can be initiated

6.1) If the security consideration, including questions of loyalty of the Agency to the State, so warrants;

6.2) If the Director/ Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public-sector enterprises or NIA, Re during the last five years;

6.3) If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc.;

6.4) If the Agency continuously refuses to return / refund the dues of NIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5) If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6) If business dealings with the Agency have been banned by the Govt. or any other public-sector enterprise;

6.7) If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and/or fudging/forging/tampering of documents;

6.8) If the Agency uses intimidation / threatening or brings undue outside pressure on the Company (NIA) or its official in acceptance / performances of the job under the contract;

6.9) If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10) Willful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Company (NIA) or not;

6.11) Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Company (NIA) or even otherwise;

6.12) Established litigant nature of the Agency to derive undue benefit;

6.13) Continued poor performance of the Agency in several contracts;

6.14) If the Agency misuses the premises or facilities of the Company (NIA), forcefully occupies, tampers or damages the Company's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent Authority may decide to ban business dealing for any good and sufficient reason).

7) Banning of Business Dealings

7.1) Normally, a decision to ban business dealings with any Agency should apply throughout the Company including Subsidiaries. However, the Competent Authority can impose such ban unit-wise only if in the particular case banning of business dealings by respective office

of NIA will serve the purpose and achieve its objective and banning throughout the Company is not required in view of the local conditions and impact of the misconduct / default to beyond the concerned office of NIA. Any ban imposed by Corporate Office shall be applicable across all offices of the Company, unless specified otherwise. Subsidiaries would be suitably advised.

7.2) If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.3) Procedure for Banning of Business Dealings with Foreign Agency (ies).

i) Banning of the agencies shall apply throughout the Company. Subsidiaries shall be suitably advised.

ii) Based on the complaint forwarded by the head of the concerned department or received directly by CVO, an investigation shall be carried out by Vigilance department. After investigation depending upon the gravity of the misconduct, Vigilance department may send their report to CMD NIA who may place it before the standing Committee (as specified in 5.5 (ii) above) The Committee shall examine the report and give its comments / recommendations within 21 days of receipt of the reference to the CMD NIA.

iii) If the committee opines that it is a fit case for initiating banning action, the CMD NIA will direct the G.M concerned to issue show-cause notice to the agency for replying within a reasonable period.

iv) On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by G.M concerned to the Committee specified in 7.3(ii) above for consideration and recommendation to the CMD NIA for decision.

v) The decision of the CMD, NIA shall be communicated to the agency by the concerned Head of Department.

8) Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1) If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2) The effect of such an order /issuance of such Show-Cause Notice would be that the Agency would not be disqualified from competing in Open Tender Enquiries but Limited Tender Enquiry may not be given to the Agency concerned.

8.3) Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9) Show-cause Notice

9.1) In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or mis-behavior may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defense.

9.2) If the Agency requests for inspection of any relevant document in possession of NIA, necessary facility for inspection of documents may be provided.

9.3) The Competent Authority may consider and pass an appropriate speaking order:

a) For exonerating the Agency if the charges are not established;

b) For removing the Agency from the list of approved Suppliers / Contactors, etc.

c) For banning the business dealing with the Agency.

9.4) If it decides to ban business dealings, the period for which the ban would be operative

may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10) Appeal against the Decision of the Competent Authority

10.1) The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2) Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11) Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority (as specified in 3(iii) above) upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee (as specified in 5.5 (ii) above) for examination and recommendation.

12) Circulation of the names of Agencies with whom Business Dealings have been banned

12.1) Depending upon the gravity of misconduct established, the Competent Authority of the Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public-Sector Enterprises, etc. for such action as they deem appropriate.

12.2) If Government Departments or a Public-Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3) If business dealings with any Agency have been banned by the Central or State Government or any other Public-Sector Enterprise, NIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter- connected Agencies.

Annexure – XII

BID SECURITY DECLARATION

(To be submitted in the Bidder's letterhead)

[To be included in TECHNICAL BID (OFFLINE and ONLINE)

To
The Chief Manager
Information Technology Department
The New India Assurance Co. Ltd
Head Office, 87, MG Road, Fort
Mumbai-400 001.
Dear Sir/Madam,
Re: Request for Proposal (RFP) for XXXXX

I/We_____ (bidder name), understand that, according to aforementioned RFP Terms & Conditions, bids must be supported by a Bid Securing Declaration.
I/We accept that I/We will be suspended from participation in any future contract/tender with you for 3 years from the date of submission of Bid in case if I/We:

a) have withdrawn/modified/amended, impairs or derogates from the tender, our Bid during the period of bid validity specified in the form of Bid; or
b) Violates any of the provisions of the accepted terms and conditions of this tender specification.
c) If any statement or any form enclosed by us as part of this Bid turns out to be false / incorrect at any time during the period or prior to signing of Contract.
d) having been notified of the acceptance of our Bid by the purchaser during the period of bid validity (i) fail or refuse to execute the contract, if required, or (ii) fail or refuse to furnish the Performance Security, in accordance with the Instructions to Bidders.

I/We understand this Bid Security Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the receipt of your notification of the name of the successful Bidder for this tender.

Date: For _____ Signature _____

Name _____
Authorized Signatories
(Name & Designation, seal of the firm)

Annexure- XIII

RULE-BASED TRIGGERS
(The list given above is indicative only and not exhaustive)

	TRIGGERS
1	**Provider location and profile related**
2	Claims from hospitals located far away from insured residence
3	Blacklisted hospital claims
4	hospital stationery with inadequate details
5	Bills looking too perfect in order/serial order
6	claims with visible tampering of documents,overwriting diagnosis, xrays
7	claims without supporting pre post hospitalisation bills
8	claims with discrepancies in diagnosis and line of treatment,mismatch in ICD and CPT code
9	incomplete /poor medical history
10	claims without signatue of the insured on pre auth
11	reimbursement claim from network hospital
12	claim with missing post op H/P reports,surgical /anesthetists notes missing
13	similar format, pattern and clinical details on disharge cards /bills
	Diagnosis or surgery specific triggers
14	Chronic /life style disease claims
15	increased LOS
16	Infertility/abortion/miscarriage claims
17	medical management for exact 24 hrs and expensive medicine
18	acute medical illness claims-common as well as uncommon diseases
19	surgical conditions treated conservatively
20	orpaedic illness being managed conservatively
21	medical conditions managed surgically in first year of policy-suspecting PED
22	Clinical findings do not corelate with chief complaints or diagnosis
23	unjustified ICU admission
24	surgical treatment for face ,nose or ear
	Policy and claim history related
25	policy with single person covwered and minimum SI
26	repeated claims from same or different hospital for self or family members
27	claims made immediately after SI enhanced
28	claims from members with frequent change of insurers
29	second claim in same year for acute medical conditions /minor surgical conditions-especialy in young aged 25 to 35
30	member with regular claim history
	billing and tariff related
31	cost of treatment much higher than expected
32	pharmacy cost more than 50% of claim

33	high value claim for small hospital
34	delayed pre auth request,claim intimation on weekend or holidays
	member based triggers
35	claims from members creating abnormal pressure to serttle claims unusually high knowledge of policy terms
36	member unwilling to meet face to face /does not provide phone number /attitude evasive, hosstile, uncooperative ,complaining
	Primary triggers
37	incomplete address on policy
38	within 10-15 days of expiry
39	timely submission of claim doc within 7 days from discharge
40	average claim size 40 thousand to 1.5 Lakh
41	unsigned discharge summary
42	unsigned claim forms
43	lab reports signed by lab technicians only
44	missing /incorrect contact details of hosp/insured
45	no landline number of hosp on hospital stationary
46	systematic presentation of documents
47	submission of hospital registration certificate , IPD record of hospital and like documents in advance without query
48	invalid /tempered ID proof
49	all documents written and attested in one go
50	payment in 2 parts-advance and balance at discharge
51	calculation mistakes in bills
52	High end antibiotics
53	no radiological investigations to avoid submission
54	same look alike xray films
55	profession mentioned as bussiness or dependent to avoid verification at workplace
56	frequent calls to check their claim status
57	submission of cheque without printed name for NEFT
58	weird style of despatching like in 'form' they will simple mention name and policy number of sender
59	late hour submission of documents
60	printout of queries from website(because despatched letter never reachjed at address mentioned in policy)
61	they will avoid submission of adhaar card, voter card,old type driving lisence
62	different signature of same insured / doctor
	Triggers to be kept in mind during cashless authorization
63	hospital of border areas like Sonepat,Bahadurgarh,Jhajhar Loni
64	hospitalisation in different zone
65	high value claims from B grade hospitals
66	irrelavant investigations
67	admission not justified
	Cashless
68	Check with patient/attender for reason of hospitalisation and correlate with hospital record
69	IP register for time and date of admission
70	OT register and OT notes
71	pharmacy receipts matching with treatment

72	previous consultation papers
73	h/o alcohol and substance abuse
	Reimbursement
74	check with HR for attendance of patient during hospitalisation
75	check the reason for hospitalisation n that particular hospital
	Audit triggers
76	NME should not be deducted as admission in general ward
77	claims above 1 lac are high value claims
78	hospital is a corporate
79	claims against cashless denied claims
80	package rate mismatch
81	members of same family getting admitted and discharged together
82	ailment capping
83	cases processed over and above suminsured irrepective of any amount
84	claims above 2 lac are high valued claims
85	manual or semi manual process
86	claims sent to insurer for approval before settlement
87	new joinees upto 3 months
	Triggers
88	Claim immediately after any endorsement
89	multiple insurance policies
90	frequent claims from single source
91	hospitalisation just after waiting period
92	inflated bills unnecessary items
93	belonging to chain of hospital where same physician visits
94	fracture and arthroscopic cases
95	some particular disorders like fever and AGE
96	cases where pre or post hospitalisation claims claimed
97	aggressive monitoring and compulsory physical visits
	Triggers
98	Repeated claims from single insured having same diagnosis
99	multiple group mediclaim from same hospitals exeed 30%
100	more than 2 claims reported in a policy
101	more than 2 claims reported in the same employee ID
102	same proposer in different policies
103	same account number with different insured
104	any agent / coorporate/DO specific instructions to blockagent code, policies
	Manual triggers
105	Non standard format of documents
106	false proposal,documents submitted.eg KYC
107	frequent change of doctors/treatmentor non comprehensive treatment
	Hospitalization related
108	recurrent illness like urinary stones,uterine fibroids
109	chronic disorders ,psychosomatic conditionslike IBS,repetitive stress injury,fibromyalgia,
110	unregistered or unrecognised hospitals
111	adverse past claims experience from same hospitals

112	bills without gst number
113	Handwritten bills without stamp
	Policy related
114	applied during year /month end
115	member selection by physically handicapped specialcategories house wives,
	Reimbursement claims
116	existing data of claim history related to hospitals /nursing homes
	System generated trigger
117	policy number wise trigger
118	LOS >3 days
119	policy end date less than 90 days
120	doctor fees >50% claim amount
121	fraud claims within family in the past
122	claims within 3 months of inception
123	suspected location cases-Rewari,Faridabad,Noida,Meerut,Ghaziabad etc
	non system generated trigger points
124	treatment expenses usually in higher side compared to etiology
125	unnecessary and costly investigation
126	Higher number of perpatient average medical investigation
127	fluctuating monthly claim of health care providers
128	photocopied stationery may be used
129	print of stationery not clear
130	spelling mistakes in medical records
131	change in logo of hospitals
132	papers of substandard qualities used in claims(thickness)
133	same photograph enrolled under different names and different policies
134	OPD claims converted to IPD
135	hospital faculty taking treatment in the same hospital
136	frequent and regular follow up
137	maxcimum number of policy enrolled on same policy address
138	investigation report without doctors prescription
139	mismatch between doctors prescription and chemists bill
140	bills with no bill breakup
	Triggers
141	dialysis claims(patient existence)
142	Infectious disease claims
	Triggers- claim / policy
143	Misrepresentation of facts
144	insured non traceable
	Provider triggers
145	fabrication of documents
	System triggers
146	claim reported after 3 months from hospitalisation
	Retail (automated)
147	online sold retail policies
148	claim reported with claim amount 90% of SI

	Group
149	claims from unrecognised hospitals
150	family with multiple medical mangement claims every year
151	family additions and deletions every year by the employee
152	duplicate bank acc no
	Scrutiny by doctors
153	Claims without supporting prepost hospitalization papers
154	Doctors speciality/registration number not indicated
155	Variation in physicians statement
156	Belonging to chain of hospitals where same doctor visits
157	Long stay unreasonable as per standard medical practice
158	Unexpected change in treatment, additional treatments,costly equipments.
159	Difference in handwritting for same doctor,missing pages
	specific triggers
160	Ambulance /bloodbank bill not in proper format or provideon plain paper
161	Medicined purchased not as per discharge advice
	SLA based triggers
162	As specified in the SLA of respective insurer
	Hospital based triggers
163	first claim from hospitals (network/non network)
	manual process
164	Catarat surgery at age lessthan35
165	same DOA in family
166	patient age does not match
167	accidental cases
	Scrutiny of claim documents
168	Claim Form
169	Medical certificate -claim form
170	Claim documents and application-number of years of policy coverage ,date of illness detected
171	Treating doctors details
172	ISO Logo
173	Date of reports
174	Details of reference
175	Invoice-suppliers details,TIM number