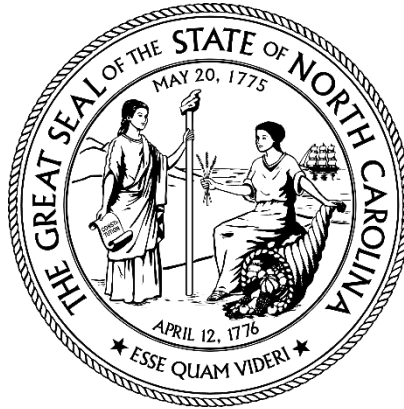




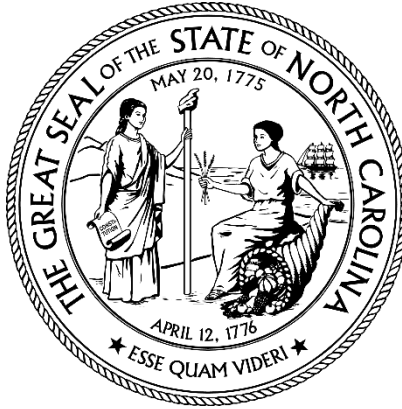
STATE OF NORTH CAROLINA

Department of Health and Human Services

Division of Health Benefits

Request for Proposal #30-2026-017-DHB

Provider Data Management Credentialing Verification Organization (PDM/CVO)



STATE OF NORTH CAROLINA

Request for Proposal

#30-2026-017-DHB

For internal State agency processing, please provide your company's Federal Employer Identification Number or alternate identification number (e.g., Social Security Number). Pursuant to North Carolina General Statute 132-1.10(b) this identification number shall not be released to the public. **This page will be redacted** before the procurement file is made available for public inspection.

This page is to be filled out and returned with your Proposal.

ID Number:

Federal ID Number or Social Security Number

Offeror Name

**STATE OF NORTH CAROLINA****Department of Health and Human Services****Refer ALL inquiries regarding this RFP to:**

Tyler Ragor

Contract Specialist

Medicaid.Procurement@dhhs.nc.govTyler.ragor@dhhs.nc.gov**Request for Proposal # 30-2026-017-DHB****Date RFP Issued/Posted: 6/12/2026****Date RFP Submissions due to the Department: at 2:00 p.m. EST****Proposals will be opened: at 2:00 p.m. EST****Contract Type:** Open Market**Commodity Number:** 811620 - Cloud-based software as a service**Description:** Provider Data Management/Credentialing Verification
Organization (PDM/CVO)**Using Agency:** Department of Health and Human Services, Division of Health
Benefits**Requisition No.:** N/A**EXECUTION**

In compliance with this Request for Proposal (RFP), and subject to all the conditions herein, the undersigned Offeror offers and agrees to furnish and deliver any or all services proposed, at the cost proposed and within the time specified herein. By executing this proposal, the Offeror confirms it has read, understands, and will comply with all specifications and requirements in the RFP and any addenda in the event of contract award. By executing this proposal, the undersigned Offeror certifies that this proposal is submitted competitively and without collusion (N.C. Gen. Stat. § 143-54), that none of its officers, directors, or owners of an unincorporated business entity has been convicted of any violations of Chapter 78A of the General Statutes, the Securities Act of 1933, or the Securities Exchange Act of 1934 (N.C. Gen. Stat. § 143-59.2), and that it is not an ineligible Contractor as set forth in N.C. Gen. Stat. § 143-59.1. False certification is a Class I felony. Furthermore, by executing this proposal, the undersigned certifies to the best of Offeror's knowledge and belief, that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from covered transactions by any Federal or State department or agency. As required by N.C. Gen. Stat. § 143-48.5, the undersigned Offeror certifies that it, and each of its subcontractors, for any Contract awarded as a result of this RFP, complies with the requirements of Article 2 of Chapter 64 of the NC General Statutes, including the requirement for each employer with more than 25 employees in North Carolina to verify the work authorization of its employees through the Federal E-Verify system. N.C. Gen. Stat. § 133-32 and Executive Order 24 (2009) prohibit the offer to, or acceptance by, any State Employee associated with the preparing plans, specifications, estimates for public Contract; or awarding or administering public Contracts; or inspecting or supervising delivery of the public Contract of any gift from anyone with a Contract with the State, or from any person seeking to do business with the State. By executing this proposal, you attest, for your entire organization and its employees or agents, that you are not aware that any such gift has been offered, accepted, or promised by any employees of your organization. **Failure to execute/sign proposal prior to submission shall render proposal invalid and it WILL BE REJECTED. Late proposals will not be accepted.**

OFFEROR:

STREET ADDRESS:

P.O. BOX:

ZIP:

CITY & STATE & ZIP:

TELEPHONE NUMBER:

TOLL FREE TEL. NO:

PRINCIPAL PLACE OF BUSINESS ADDRESS IF DIFFERENT FROM ABOVE

PRINT NAME & TITLE OF PERSON SIGNING ON BEHALF OF OFFEROR:

FAX NUMBER:

OFFEROR'S AUTHORIZED SIGNATURE:

DATE:

EMAIL:

Offer valid for at least **240** calendar days from date of proposal opening unless extended by the State in writing. After this time, any withdrawal of offer shall be made in writing, effective upon receipt by the agency issuing this RFP.

ACCEPTANCE OF RESPONSE

If any or all parts of this proposal are accepted by the State of North Carolina, an authorized representative of the Department of Health and Human Services shall affix his/her signature hereto and this document and all provisions of this Request for Proposal along with the Offeror's proposal, and the written results of any negotiations shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the successful Offeror.

FOR STATE USE ONLY: Offer accepted and Contract awarded this ____ day of _____, 20____, by

(Authorized Representative of NC Department of Health and Human Services)

Table of Contents

1.0 General Procurement Information and Notice to Offerors.....8

1.1 Important Notices 8

1.2 Procurement Information 9

1.3 Request for Proposal Functionality and Related Notices..... 10

1.4 Schedule and Important Events..... 11

2.0 Purpose of RFP13

2.1 Introduction 13

2.2 Contract Term..... 14

2.3 Contract Type 14

2.4 Agency Background 14

3.0 RFP Requirements and Specifications15

3.1 Scope Of Work 15

3.2 General Requirements and Specifications..... 29

3.2.1 REQUIREMENTS 29

3.2.2 Specifications..... 29

3.2.3 Site and System Preparation 29

3.2.4 Equivalent Items 29

3.2.5 Enterprise Licensing..... 29

3.2.6 ENTERPRISE ARCHITECTURE STANDARDS 30

3.3 Security Specifications 30

3.4 Enterprise Specifications 32

3.5 Business and Technical Requirements 33

3.6 Business and Technical Specifications..... 116

3.7 Option Requirements and Specifications - RESERVED 125

4.0 Cost of Vendor’s Offer.....125

4.1 Offer Costs125

4.2 Payment Schedule.....126

5.0 Evaluation.....126

5.1 Source Selection 126

5.2 Evaluation Criteria 127

5.3 Best and Final Offers (BAFO)..... 128

5.4 Possession And Review 128

5.5	Competitive Range	129
5.6	System Demonstrations.....	129
6.0	Vendor Information and Instructions	129
6.1	General Conditions of Offer	129
6.1.1	Vendor Responsibility	129
6.1.2	Rights Reserved	130
6.1.3	Solicitation amendments or revisions.....	130
6.1.4	Oral Explanations.....	131
6.1.5	E-PROCUREMENT	131
6.1.6	Electronic Vendor Portal	131
6.1.7	Protest Procedures	131
6.2	General Instructions for Vendor.....	132
6.3	Instructions for Offer Submission.....	134
7.0	Other Requirements and Special Terms.....	138
7.1	Vendor Utilization Of Workers Outside of U.S.	138
7.2	Financial Statements	138
7.3	Financial Resources Assessment, Quality Assurance, Performance and Reliability	139
7.4	Vendor's License or Support Agreements	139
7.5	Resellers - Reserved	139
7.6	Disclosure Of Litigation.....	139
7.7	Criminal Conviction.....	140
7.8	Security and Background Checks.....	140
7.9	Assurances.....	140
7.10	Confidentiality of offers.....	141
7.11	Project Management.....	141
7.12	Meetings	142
7.13	Recycling and Source Reduction - Reserved.....	143
7.14	Special Terms And Conditions.....	143
7.15	Technical Operations	153
7.16	Help Center.....	154
7.17	Testing	155
7.18	Incident Prioritization.....	157
Attachment A: Definitions		158
Attachment B: Department of Information Technology Terms and Conditions.....		170

Section 1: General Terms and Conditions Applicable to All Purchases	170	
Section 2: Terms and Conditions Applicable to Information Technology Goods and Services	182	
Section 3: Terms and Conditions Applicable to Personnel and Personal Services	185	
Section 4: Software as a Service (SaaS) Terms and Conditions (Only Applies to Proposed SaaS Solutions)		187
Attachment C: Agency Terms and Conditions	196	
Section 1: NCDHHS Department of Health Benefits (DHB)	196	
Section 2: NCDHHS Privacy and Security Office (PSO)	207	
Section 3: NCDHHS Development of Artificial Intelligence Systems	211	
Attachment D: Description of Offeror	217	
Attachment E: Cost Form	218	
Attachment F: Vendor Certification Form	221	
Attachment G: Location of Workers Utilized by Vendor	222	
Attachment H: Vendor References/Past Performance	224	
Attachment I: Financial Review Form	231	
Attachment J: Enterprise Architecture	233	
Attachment K: Vendor Key Personnel	235	
Attachment L: Service Level Agreements	245	
Attachment M: Contract Administrators	260	
Attachment N: Deliverables And Milestones Schedule	262	
Attachment O: Business Continuity Plan	301	
Attachment P: Disaster Recovery Plan	303	
Attachment Q: State Certifications	306	
Attachment R: Federal Certifications	309	
Attachment S: Business Associate Agreement	317	
Attachment T: Technical / Management Proposal	321	
Attachment U: Conceptual Architectural Diagrams	323	
Attachment V: Medicaid Integration Services Core Capabilities	324	
Attachment W: Work Products	330	
Attachment X: Request for Proposed Modifications to The Terms and Conditions	336	
Attachment Y: Minimum Qualifications	337	
Attachment Z: SUBCONTRACTOR IDENTIFICATION FORM	339	
Attachment AA: Reports	341	
Attachment AB: Interfaces	343	
Attachment AC: GenAI Disclosure and Fact Sheet	348	

1.0 GENERAL PROCUREMENT INFORMATION AND NOTICE TO OFFERORS

1.1 IMPORTANT NOTICES

Offerors are Cautioned to Read Carefully

1.1.1 READ, REVIEW, AND COMPLY

It shall be the Offeror's responsibility to read this entire document, review all enclosures and attachments, and any addenda thereto, and comply with all requirements specified herein, regardless of whether appearing in these Instructions to Offerors or elsewhere in this RFP document.

1.1.2 EXECUTION OF PROPOSAL

Failure to sign the Execution Page in the indicated space and return all attachments, tables, charts, exhibits, diagrams, and appendices completed and signed where required shall render the proposal non-responsive.

1.1.3 RESULTING CONTRACT

Under the State's procurement process, any contract resulting from this RFP will consist of the RFP and the Offeror's response, along with any addenda to the RFP, written Clarifications, Best and Final Offers (BAFO), and negotiation documents. The Contractor will be obligated to perform services as proposed in its offer, unless otherwise modified by Clarification, BAFO, negotiation, or Contract amendment, or superseded by a document with higher order of precedence. See *Attachment C: Agency Terms and Conditions, Section 1, Paragraph 14 Entire Agreement and Order of Precedence*, of this document for more information and the order of precedence of the contract documents. See section 1.3 Request for Proposal Functionality and Related Notices in this section for more information on the RFP, changes in specifications, and instructions regarding modifications to the terms and conditions.

1.1.4 POTENTIAL NEGOTIATIONS

The Department reserves the right to enter into negotiations with one or more Offerors to establish a contract that is in the best interest of the Department. Negotiations are specific to each Offer and shall be conducted to maximize the State's ability to obtain the most advantageous offer based on the evaluation factors set forth in the RFP. Such negotiations are at the Department's sole discretion and may result in modifications to the RFP and/or Offeror's proposal/response to the RFP.

1.1.5 EVENTS AND DEADLINES

- a. **Pre-proposal Conference** will be hosted by the Department on the date and time indicated in the RFP Schedule in Section 1.4.1.
- b. **Questions** concerning this RFP must be submitted in writing by the date and time indicated in the RFP Schedule in Section 1.4.1.
- c. **Submission of Proposals** will be accepted until the date and time indicated in the RFP Schedule in Section 1.4.1.

1.1.6 BIDDER'S LIBRARY

The Bidder's Library is a collection of documents, data, and reference materials that the Department provides to prospective Offerors during the Request for Proposal (RFP) process. Its primary purpose is to give Offerors access to relevant background information necessary to develop informed, accurate, and compliant proposals. The contents of the Bidder's Library are provided solely for informational purposes and will not be included as part of the final contract.

The documents contained in the Bidder's Library will be available only while the solicitation remains open in the Ariba Sourcing Tool. Offerors are strongly encouraged to review the Bidder's Library section found in the solicitation in the Ariba Sourcing Tool and download the documents for review and future reference. After the solicitation closes in the Ariba Sourcing Tool, the documents in the Bidder's Library will no longer be accessible.

The content of the Bidder's Library reflects the current state of information at the time the RFP is issued and is not guaranteed to be updated throughout the procurement process.

1.2 PROCUREMENT INFORMATION

1.2.1 INFORMATION AND DESCRIPTIVE LITERATURE

The Offeror shall furnish all information requested as part of this RFP. Each Offeror shall submit detailed information with their proposal (e.g., narratives, diagrams, exhibits, examples, sketches, descriptive literature, complete specifications) to support the services and products offered

1.2.2 RESERVED

1.2.3 MISCELLANEOUS

Pronouns, whether masculine, feminine, or gender-non-specific, shall be read to be inclusive of all genders and shall be read to include the plural and vice versa.

1.2.4 INFORMAL COMMENTS

The Department shall not be bound by informal explanations, instructions or information given at any time by anyone on behalf of the Department prior to or during the competitive process or after award, including but not limited to policy papers or any written or verbal statements whatsoever made outside of this RFP and any formal Addenda issued herewith. The Department is bound only by information provided in this RFP and in formal Addenda issued

1.2.5 OFFEROR'S REPRESENTATIVE

Each Offeror shall submit with its proposal the name, title, email address, physical address, and telephone number of the person(s) with authority to bind the Offeror and answer questions or provide clarification concerning the Offeror's proposal. This information must be included in the Offeror's proposal and response

1.2.6 DISCLOSURE OF ARTIFICIAL INTELLIGENCE (AI) USE–

The Offeror shall disclose whether Artificial Intelligence (AI), including generative AI tools, was used in the preparation of any portion of its response to this RFP. If AI tools were utilized, the Offeror affirms that it has reviewed and verified the accuracy, completeness, and appropriateness of all AI-generated content. The Offeror shall remain solely responsible for the content of its submission, including any errors, omissions, or misrepresentations resulting from the use of AI.

1.3 REQUEST FOR PROPOSAL FUNCTIONALITY AND RELATED NOTICES

1.3.1 RFP FUNCTIONALITY

- a. This RFP serves two functions:
 - i. Define the specifications of the Solution sought by the Department; and
 - ii. Provide the requirements and terms and conditions of any contract resulting from this procurement.
- b. All Terms and Conditions in this RFP shall be enforceable. The use of phrases such as “*shall*”, “*will*”, “*must*”, “*required*”, and “*requirements*” are intended to create enforceable Contract conditions. In determining whether proposals should be evaluated or rejected, the Department will take into consideration the degree to which the Offeror has proposed or failed to propose solutions that are responsive to the Department’s needs as described in this RFP.

1.3.2 NOTICES REGARDING RFP AND TERMS AND CONDITIONS

- a. It is the Offeror's responsibility to read all instructions, terms and conditions, specifications, requirements, attachments and appendices, and any other components made a part of this RFP and comply with all instructions and directives. The Offeror is responsible for obtaining and complying with all addenda and other changes that may be issued relating to this RFP.
- b. All questions and issues regarding any term, condition, instruction, or other component within this RFP must be submitted in accordance with Section 6.2.2. Questions Regarding this RFP. If the Department determines that any changes will be made because of the questions asked, then such decisions will be communicated in the form of an Addendum posted on the North Carolina electronic Vendor Portal (NC eVP). The Department may also elect to leave open the possibility for later negotiation and amendment of specific provisions of the Contract that have been raised during the question-and-answer period. Other than through this process, and except as provided in Section 1.3.3 Proposed Modifications to Terms and Conditions, the Department rejects and will not be required to evaluate or consider any additional or modified terms and conditions submitted with Offeror's proposal. This applies to any language appearing in or attached to the RFP document as part of the Offeror's proposal that purports to vary any terms and conditions, or Offeror's Instructions therein to render the proposal non-binding or subject to further negotiation.
- c. The Offeror's proposal to this RFP shall constitute a firm offer. **By execution and delivery of a proposal to this RFP, the Offeror agrees that any additional or modified terms and conditions, whether submitted purposely or inadvertently, or any purported**

condition to the offer, shall have no force or effect, and will be disregarded. Noncompliance with, or any attempt to alter or delete, this paragraph shall constitute sufficient grounds to reject the Offeror's proposal.

1.3.3 PROPOSED MODIFICATIONS TO TERMS AND CONDITIONS

- a. Offerors are urged and cautioned to inquire during the question period, in accordance with the instructions in this RFP, about whether specific language proposed as a modification is acceptable to or will be considered by the Department.
- b. Identification of objections or exceptions to the terms and conditions in the proposal itself shall not be allowed and shall be disregarded or the proposal rejected.
- c. If the Offeror wishes to suggest changes to any of the terms and conditions included in Attachments B and C of this RFP, those must be submitted in Attachment X: Request for Proposed Modifications to the Terms and Conditions. The Department, in its sole discretion, may consider any proposed modifications identified by the Offeror. Where necessary, any modification(s) to the terms and conditions agreed upon by the Department may be incorporated as part of an Addendum to the RFP, BAFO, negotiation document, Execution of Contract, or Contract Amendment after award. Other than through this process, the Department rejects and shall not be required to evaluate or consider any additional or modified terms, conditions, or instructions included in the Offeror's proposal.

1.3.4 CHANGES IN REQUIREMENTS AND SPECIFICATIONS

- a. The Offeror is cautioned that the requirements of this RFP can only be altered by written Addendum issued or other documents issued by the Department as described in this RFP, and that oral or emailed communications from whatever source(s) are of no effect.
- b. Any modification to specifications will be specified in an Addendum which shall be posted to the NC eVP prior to the opening of proposals or through Negotiation after opening the proposals.

1.4 SCHEDULE AND IMPORTANT EVENTS

1.4.1 ANTICIPATED PROCUREMENT SCHEDULE

The Department will make every effort to adhere to the schedule detailed below in Table 1.4 1-1: RFP Schedule. The Department reserves the right to adjust the schedule and will post an Addendum on the NC eVP website for any schedule changes occurring prior to the opening of proposals.

Action	Responsible Party	Due Date	Time (ET)
RFP Issued	Department	06/12/2026	
Register for Pre-Proposal Conference	Offeror(s)	06/16/2026	10:00 am
Pre-Proposal Conference	Offeror(s) and Department	06/17/2026	2:00 pm
Written Questions Deadline	Offeror(s)	06/26/2026	2:00 pm

Action	Responsible Party	Due Date	Time (ET)
Agency's Response to Written Questions / RFP Addendum Issued	Department	07/17/2026	
Proposals Due	Offeror(s)	08/21/2026	2:00 pm
Proposals Evaluation Begins	Department	08/24/2026	
System Demonstrations	Offeror(s)	1/5/2027	
Estimated Contract Award	Department	6/1/2027	
Protest Deadline	Responding Vendors	15 days after award	

Table 1.4 1-1 RFP Schedule

1.4.2 PRE-PROPOSAL CONFERENCE

- a. The Department will hold a Pre-proposal virtual Conference on the date and time indicated in the RFP Schedule in Section 1.4.1 for one hour via Microsoft (MS) Teams. No purchase is required to use the MS Teams app.
- b. The purpose of the conference is to allow the Department to review key priorities and objectives of the RFP and to review the submission requirements and instructions.
- c. While attendees may ask questions at the Pre-proposal Conference, the Department is not required to respond during the conference. The Department will respond to written questions per the process described in this RFP.
- d. Potential Offerors are not required to attend the Pre-proposal Conference in order to submit responses to this RFP; however, they are urged and cautioned to attend the Pre-proposal Conference to apprise themselves of the conditions and requirements of the submission.
- e. To ensure receipt of the video conference invite and instructions for participation, interested parties are required to pre-register for the conference by sending an email to Medicaid.Procurement@dhhs.nc.gov stating the name of the potential Offeror, the names and email addresses of representatives who will attend, the current title or role of each representative, and requests for a sign language interpreter or other accommodations. Interested parties must pre-register at this email address by the date and time indicated in the RFP Schedule in Section 1.4.1.
- f. The Department limits the number of representatives attending on behalf of each Offeror or organization to two (2) representatives to ensure adherence to videoconference capacity limits.
- g. Audio and video recording will not be permitted. Statements and materials discussed at the conference are informational only, are not binding upon the Department and do not replace reading, reviewing and complying with this RFP.

- h. Attendees will be required to announce their name or otherwise confirm their presence via a roll call during the Pre-Proposal Conference.

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The Purpose of this Request for Proposal (RFP) is the for the North Carolina Department of Health and Human Services (NCDHHS), Division of Health Benefits (DHB or Department), to solicit offers for the acquisition for the Provider Data Management Credentialing Verification Organization (PDM/CVO).

Medicaid Integrated Modular Solution (MIMS)

NCDHHS is replacing the Department's Medicaid Management Information System (MMIS) with a Medicaid Enterprise System (MES), also referred to as the Medicaid Integrated Modular Solution (MIMS). MIMS will be implemented through a multi-phase initiative, the MMIS Replacement Project. The MMIS Replacement Project will implement a series of interrelated modules. These modules will have functionality designated by the Centers for Medicare and Medicaid (CMS) in support of obtaining compliance with Medicaid Information Technology Architecture (MITA) 3.0 Framework and CMS certification for each module.

The future PDM/CVO solution is envisioned as a centralized Provider Data Management/Credentialing Verification Organization (PDM/CVO) solution that will support the Agency's provider data management functions including data intake, data management, enrollment, credentialing, data sharing and data archiving throughout the provider life cycle. The solution will also meet National Committee for Quality Assurance (NCQA) standards and enhance provider credentialing through centralized CVO features that include a Credentialing Committee and delegated enrollment and credentialing.

The PDM/CVO solution will consist of the below high-level items:

- Consolidate all provider data to reduce administrative redundancy for providers.
- Simplify enrollment, data maintenance and revalidation processes.
- Facilitate centralized credentialing on behalf of NCDHHS payers and health plans.
- Potentially mitigate reimbursement errors caused by outdated provider data.
- Allow for delegated enrollment and credentialing.
- Aligning North Carolina's credentialing process with NCQA standards.
- Establish a representative centralized Credentialing Committee with representatives from NCDHHS payers and health plans.

The NC MIMS system will modernize and transform North Carolina Medicaid and its sister divisions, including the Division of Mental Health (DMH) and Division of Public Health (DPH). NC MIMS will improve the Provider and Medicaid beneficiary experience across the enterprise.

2.2 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The initial term shall be five (5) years unless otherwise stated in the Notice of Award and unless otherwise terminated in accordance with the Contract.

2.2.1 OPTIONAL EXTENSIONS

After the initial term, the Department shall have the option to extend the Contract for two (2) additional one (1) year periods at its sole discretion. Each year that the Contract remains in effect shall be a "Contract Year." The Department will give the Contractor written notice of its intent whether to exercise each option year no later than thirty (30) Calendar Days before the end of the Contract's then current term.

2.2.2 Effective Date

This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the Department until the appropriate State purchasing authority / official, or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The Department shall not be responsible for reimbursing the Vendor for goods provided nor services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.3 CONTRACT TYPE

Definite Quantity Contract - This request is for a close-ended contract between the awarded Vendor and the State to furnish a pre-determined quantity of a good or service during a specified period of time.

The State reserves the right to make partial, progressive or multiple awards: where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; and where other factors are deemed to be necessary or proper to the purchase in question.

2.4 AGENCY BACKGROUND

NCDHHS manages the delivery of health- and human-related services for all North Carolinians, especially our most vulnerable citizens – children, elderly, disabled and low-income families. The Department works closely with health care professionals, community leaders and advocacy groups; local, state and federal entities; and many other stakeholders to make this happen. Within NCDHHS, the Division of Health Benefits is dedicated to providing access to physical and behavioral health care and services to improve the health and well-being of over 3 million North Carolinians.

NCDHHS is replacing the Department's Medicaid Management Information System (MMIS) with a Medicaid Enterprise System (MES), also referred to as the Medicaid Integrated Modular Solution (MIMS). MIMS will be implemented through a multi-phase initiative, the MMIS

Replacement Project. The MMIS Replacement Project will implement a series of interrelated modules. These modules will have functionality designated by the Centers for Medicare & Medicaid Services (CMS) in support of obtaining compliance with Medicaid Information Technology Architecture (MITA) Framework and CMS certification for each module.

The NC MIMS system will modernize and transform North Carolina Medicaid and its sister divisions, including the Division of Mental Health (DMH) and Division of Public Health (DPH) NC MIMS will improve the Provider and Medicaid beneficiary experience across the enterprise.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 SCOPE OF WORK

The Provider Data Management Credentialing Verification (PDM/CVO) solution will replace and modernize provider enrollment and management functionality provided by the legacy MMIS. The PDM/CVO solution will meet North Carolina's "to be" vision for the Provider Eligibility and Enrollment, Provider Management, Credentialing, as well as other applicable MITA business areas.

The PDM/CVO module will support a web-based self-service tool for providers to electronically sign and submit enrollment applications, complete periodic updates of their enrollment information, and revalidate provider record information. The self-service enrollment and maintenance portal must be configurable by provider criteria that include, at a minimum, provider role (e.g., OPR Rendering, Attending, Billing/Pay-to Providers), provider risk level, and provider classification (e.g., physician-family practice, physician-oncologist, hospital-acute care, nurse practitioner-pediatrics), as well as other required criteria detailed in Section 3.5 Business and Technical Requirements. In addition, the PDM/CVO module must also support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles.

The web-based application will collect, validate, and maintain the required data:

- To support decisions regarding a provider's enrollment request or continued participation.
- For provider directories, network adequacy analysis, federal and state compliance reporting, data analytics, claims processing, service authorizations, provider payment, tax and general reporting, use within other MES modules, and other purposes identified by the state.
- To associate providers with multiple networks, healthcare programs, and affiliations as directed by the state and governed by business rules.

The solution will leverage integrated, automated workflow to ensure that data and documentation are routed to the appropriate unit responsible for decisions on provider applications or findings.

A successful Provider Services solution will provide a variety of self-service options with a seamless end-user experience for North Carolina Healthcare Programs providers.

3.1.1 Business Operations

Self-Service Portal

The PDM/CVO module must include a Provider Self-Service Portal to support provider enrollment and maintenance activities. The Portal will solicit and receive data entry from applicants and providers according to Business Rules and shall be the primary point of interface between the provider and the PDM/CVO solution. The Portal must:

- Allow providers and potential applicants to learn and understand the process for submitting applications, viewing and updating their data, completing revalidations, and completing any activities required as part of the PDM/CVO solution.
- Allow enrolled providers to review and manage demographic data associated with their records.
- Include other self-service functions necessary to support day-to-day business functions, including but not limited to; a provider inbox, interactive chat functionality, and a provider locator for both public and authenticated users to find actively enrolled providers based on specified criteria.

The web screens that make up the Portal shall be efficient and concise, gathering all information required to complete steps in application processing, enrollment, and data management. Screens and their components will be subject to Department approval.

Refer to 3.1.2 Technical and Information Architecture Requirements for the technical architecture and associated technology requirements for enabling users to seamlessly navigate between the PDM/CVO Self-Service Portal and other MES modules.

Provider Maintenance

The PDM/CVO module must support provider maintenance activities for external and internal users that are founded on business process driven workflow automation principles. These activities include the collection, storage, and maintenance of all provider information identified for the operation of the MES. It also requires ongoing, automated provider monitoring necessary to support North Carolina Healthcare Programs business objectives and must be compliant with federal and state statutes, NCQA, policies and mandates.

Credentialing Committee

The Vendor is responsible for the operation of an NCQA-compliant Credentialing Committee to evaluate all applicants and providers, including initial enrollments, re-enrollments, revalidations, and data maintenance requests that may require credentialing, as well as ongoing monthly monitoring. The Credentialing Committee shall meet regularly (at least weekly) and make decisions regarding the credentialing status of the provider. The Vendor must provide IT solutions to manage all aspects of the process, provide staffing for operations, and coordinate with multiple payers, health plans, and other stakeholders.

The Vendor must employ a Medical Director, subject to Department approval, who is directly responsible for the operation of the Credentialing Committee and will serve as its chair and voting member, as well as appointing a proxy in their absence. The Medical Director will follow and enforce the Credentialing Committee Bylaws as approved by the Department. The Medical Director must participate in the review of the Credentialing Committee Bylaws, Credentialing Committee operating policy and procedures, recruitment of Credentialing Committee members, and coordination of peer reviewers.

The Vendor must prepare and make electronically available to all committee members a Provider Profile Package for each medium and high-risk provider under consideration, which contains all primary source verifications and supporting documentation. The package will include:

- Provider information - type/specialty, risk level, file ID, review type (application type/ongoing monitoring)
- A brief, objective description of any concerns or findings that elevate the file's risk status.
- A summary of each of the applicable primary source verification results
- Supporting documentation

Delegated Enrollment and Credentialing

Qualifying North Carolina hospitals, large health care systems, and the Cherokee Indian Hospital Authority (CIHA) shall be permitted to perform enrollment and credentialing activities for their own healthcare practitioners.

This will allow hospitals and large health care systems to better manage large volumes of individual providers, reduce administrative burden, accommodate program growth, expedite individual Provider Enrollment and Credentialing, improve efficiency in the credentialing process, increase practitioner satisfaction, remove the NC Application fee for their individual providers, and support centralized credentialing.

The Vendor must provide IT solutions to manage all aspects of allowing delegated entities to:

- Submit a new provider to the PDM.
- Submit a re-enrollment of a terminated provider to the PDM.
- Submit provider data updates to a provider on its roster.
- Identify existing active providers on its roster and the most recent Revalidation completion date.
- Remove a provider from its roster.

The solution must maintain and make affiliations between a delegated entity and its rostered providers viewable to the Department in real time and through standardized reports.

The Vendor is responsible for providing oversight and monitoring of each delegated entity, including:

- A pre-delegation audit that includes a performance and staffing assessment, a policy and procedure review, and a review of the entities understanding and adherence to NCQA, State, Federal enrollment and credentialing requirements and delegation tasks.
- Completion of an annual compliance audit to re-review all the components of the pre-delegation audit, audit 5% of the entity's credentialing and recredentialing files against NCQA, State, and Federal enrollment and credentialing requirements, and create corrective action plans for deficiencies in collaboration with the Department, including revocation recommendations for delegated entity participation.

- The Vendor must report results to the Department for each pre-delegation and annual compliance audit within 30 days of audit completion. If the entity is found to be out of compliance during the audit, the Vendor must report those results to the Department within 10 days of audit completion.

Conduct Federal Site Visit/Screening Verification

During the provider enrollment screening process for moderate and high-risk providers, there is a federally mandated requirement for the Agency to conduct an on-site evaluation of the provider. The Vendor's solutions and services shall include providing staff to act on behalf of the Agency to conduct pre- and post-enrollment on-site screening of the provider. The Vendor will upload the results of the site visit evaluation into the provider's profile within the PDM/CVO module.

The onsite screening includes:

- Conducting the initial assessment to verify the facility location, hours and personnel.
- Verifying operational status; and
- Confirming final determination of provider enrollment status.

Business Rules

The Vendor must create and maintain a business rules repository of requirements applicable to every combination of application classification that the State uses to set provider enrollment requirements. The rules in the repository shall be approved by the State and maintained by the Vendor. The repository sets a hierarchy of provider classifications (healthcare/non-healthcare, in-state/out-of-state/border, business type, provider type, application type, add-ons, etc.) and establishes criteria for the application process for office administration, required provider information, fees, addresses, NPES (National Plan and Provider Enumeration System) and other external registrations, affiliations, sanctions, care management and other licensing requirements, health plan selection, required attestations and signatures, specialty and supplemental information.

The Vendor must consider, for each business rule: the beginning and end dates for the application of the rule, the conditions that trigger the rule, the actions to be executed when the rule is invoked, any predecessor or successor rules, the sequence of the rule in relation to other rules and the business process as a whole, and the timing of rule invocation and execution. Rules may invoke other rules; the output from one rule may be an input (trigger or values) to other rules.

The Vendor's solution must control how changes to the rules are made, how rule versions are tracked, how rules are tested in an environment that does not impact production, how test results are presented to the State, how rules are implemented in production after approval by the State, and how rules may be rolled back if production errors occur.

The Vendor must work with the State to identify the specific Business Rules that will be included in the repository, and will develop the processes, logic, and data elements needed to support them. The Vendor must reference existing documentation from the State to create the initial business rules repository during the DDI phase. Business rule documentation can be found in the Bidder's Library and includes:

- State-approved business rules and job aids

- Most recent version of the legacy system's Provider Permissions Matrix (PPM) – This Excel file communicates provider enrollment requirements including fingerprinting, site visits, federal fees, licensures, accreditations, and certifications for enrollment participation
- State-approved Application Data files - These word documents detail data fields captured for provider enrollment based on provider enrollment type

The Vendor must add to the business rules repository all rules needed to support its solution and meet all contractual requirements.

The Vendor must provide real time access to the business rules repository, in an electronic format approved by the State, that documents all business rule logic used by the solution.

3.1.2 Technical and Information Architecture Requirements

The Vendor must provide a scalable, cloud-based solution that complies with all applicable federal, state, and Departmental security standards. The proposed solution must deliver the following:

- **Interoperability:** Support integration with existing enterprise systems and third-party applications through standard APIs and data exchange protocols.
- **Scalability:** Be architected to handle growth in users, data volume, and transaction load without degradation in performance.
- **Security:** Implement robust security measures aligned with industry best practices, including encryption, access controls, and vulnerability management.
- **Data Governance:** Provide mechanisms for data quality, lineage, and stewardship to maintain integrity and accountability across the lifecycle.
- **Compliance:** Ensure compliance with applicable federal and state regulations, such as NIST, Health Information Portability and Accountability Act (HIPAA), Fast Healthcare Interoperability Resources (FHIR) /Health Level 7(HL7), etc.

The infrastructure must support seamless integration across all components within the solution and with the modules of the MES. This integration must utilize tools that ensure high availability, confidentiality, and data integrity. Furthermore, these tools must be maintained in alignment with the latest technology standards.

Core components must include

- A Self-service provider portal that is easy to use for providers to initiate, track, and update enrollment applications and maintain their provider data.
- An operations portal for the Vendor's credentialing staff to conduct credentialing and data maintenance activities, and allow State resources, along with other authorized users, access to applications and provider data.
- A Credentialing component that is driven by a workflow that is highly automated and configurable to the Department's business rules.

- A document management solution integrated with the enrollment and credentialing workflows, ensuring secure storage and access control to uploaded documents and system generated forms.
- Correspondence management components capable of generating and tracking electronic and physical communications based on business rules.
- Audit trails and reporting shall be integrated throughout all components to capture logs and actions supporting regulatory compliance.

The application layer must incorporate business friendly, interactive, and intuitive user interfaces; dynamic dashboards; and flexible reporting tools for both standard and ad-hoc reporting needs, with access to current and historical data.

The data management and access layer must include role-based access control, prioritizing real-time and near-time access to data over batch feeds, enforcing data quality and validation in compliance with the State data governance policies and maintaining a single source of truth for providers across the MES.

The solution must integrate with external verification sources (e.g., CMS, SSA, National Plan and Provider Enumeration System (NPPES)) to automate provider credentialing and monitoring, enabling APIs in support of interoperability where available.

The integration layer must operate in full alignment as defined in Attachment V: Medicaid Integration Services Core Capabilities, with the Medicaid Integration Services (MIS) platform to:

- a. Provide single sign-on capabilities ensuring seamless user navigation between the PDM/CVO portal applications and other MES modules; and
- b. Facilitate secure data exchange with the NCDHHS systems and integration partners through supported mechanisms, including API-based integrations and MFT.

Security

The Vendor shall implement a configuration management policy that ensures all changes to the solution's hardware, software, and firmware components adhere to applicable security and privacy control requirements. Data must be classified based on sensitivity and protected accordingly, using encryption and access controls to prevent unauthorized access.

The Vendor's solution must integrate with the statewide identity management system (NCID) to manage user authentication and authorization in coordination with the Department's Medicaid Integration Services (MIS) module (see Attachment V: Medicaid Integration Services Core Capabilities).

The PDM/CVO solution must conform to the NCDHHS Acceptable Use Policy, which establishes baseline information security requirements. Additionally, the Vendor must comply with the Statewide Data Classification and Handling Policy and the High-Risk Applications Policy, which define mandatory security and data handling standards for all NCDHHS systems and vendors.

The Vendor shall support the establishment and maintenance of provider office administrators, who are responsible for managing user access across the MES. The PDM solution shall provision these roles and share updates with the MIS in real-time to ensure accurate and current access control information.

Data Management

The Vendor's proposed solution must incorporate robust data management practices. The Vendor shall implement comprehensive data lifecycle management to ensure the accuracy, completeness, and reliability of provider data. This data must be protected from unauthorized access through the use of encryption technologies and role-based access controls in compliance with federal and state security and privacy requirements.

The solution must include audit controls to maintain data integrity. These controls include audit trails, version control mechanisms, and other tools that enable traceability and accountability.

The scope of data management encompasses transactional data, current data, and historical data maintained within the PDM. The PDM must also support seamless integration with external sources such as managed care entities and credentialing sources. Combined, this data ensures a centralized and comprehensive provider data profile.

Content Management

The Vendor's solution must collect, manage, store, and preserve electronic documents associated with a provider and/or application. All electronic documents must be stored securely using encryption and access controls to prevent unauthorized access.

- Each document must be categorized and assigned a unique document identifier to be associated with the provider and/or the application.
- The provider's self-service portal's application workflow shall electronically collect documentation required from the provider based on the business rules for the type of provider and application.
- Authorized Vendor and Department users must have the capability to upload documentation required as part of primary source verification credentialing requirements.
- Authorized Vendor and Department users must be able to access stored documents in a timely and efficient manner.

In certain cases, documents may need to be physically mailed to the Vendor for association with a provider and/or application (e.g., transcripts). The Vendor must establish and implement standardized procedures for digitizing any paper documentation received by mail. The Vendor must integrate with the State's Centralized Medicaid Content Management System, when available.

Correspondence Management

The Vendor must configure and implement a Correspondence Management Solution capable of generating and managing provider communications. The Vendor must provide functionality to generate, store, and track all written communications to and from providers. All correspondence sent to a provider must be stored in the content management solution.

While most communications will be transmitted electronically (e.g. email, Provider Portal), certain communications must be sent via standard or certified mail in accordance with defined Business Rules. For example, all involuntary denials and terminations must be sent via certified mail. This solution must coordinate the printing and distribution of physical correspondence through a State-approved print and mail service.

The Correspondence Management Solution must operate in accordance with Business Rules provided by the State. Each communication, whether directed to a single recipient, a group of recipients with identical content, or a group using a templated message with variable fields, must be assigned to a unique identifier and a common name for reference and tracking purposes.

The solution must support the generation of scheduled, ad-hoc, and automated (system-triggered) communications. Supported formats include standard letters, notices, memos, form templates, and free-form letters. Correspondence content may include letterhead, images, tables, static text, variable-filled insert text, and formatting elements consistent with Microsoft Word capabilities. Variable data fields may be populated from any data element available within the Vendor's solution or provided by the State. Please see counts of prior year certified and non-certified correspondence.

Calendar Year	Certified	Non-Certified	Total
2023	33,109	1,052,971	1,086,080
2024	36,468	1,136,191	1,172,659
2025	19,637	671,011	690,648 (Amount through July 2025)
<i>Est Remaining</i>	<i>14,026</i>	<i>479,294</i>	<i>493,320</i>
<i>Est Total 2025</i>	<i>33,663</i>	<i>1,150,305</i>	<i>1,183,968</i>

Reporting

The Vendor must provide a Reporting Solution and capabilities to schedule the generation of data extracts, standard, and ad-hoc reports that support various user needs, module functions, and reporting needs that are required to satisfy State and federal guidance. The solution shall allow presentation of data through configurable dashboards, and monitoring of module performance through generation of service level agreements (SLAs) and OBC (Outcomes Based Certification)/KPI (Key Performance Indicators) reports as required by the state. The reporting solution shall include operational reports necessary to facilitate comprehensive oversight by the State, any summary "dashboards" that show current and trending activities, and a robust selection of enrollment, disenrollment, termination, re-enrollment, revalidation, recertification, and credentialing reports as defined and requested by the state including the following:

- Reporting needs to support module administration;

- Systems and application reporting;
- Enabling standard and ad-hoc reports in state-defined flexible formats;
- Role-based user access to reporting functionality and documentation; and
- Presentation of data, including configurable dashboards and key aggregated current and historical operational data for analysis.

Interfaces

The provider data management component of the PDM/CVO will serve as the authoritative source for provider information across the MES. The Vendor must ensure the solution supports timely, accurate, and secure standards-based inbound and outbound data exchanges to facilitate provider enrollment, credentialing, and ongoing maintenance, where data is shared real-time and in batch modes.

Data exchanges occur through two primary channels, within the MES or through direct integration with external sources. The Vendor shall utilize the State's integration solution, MIS, to exchange data with other MES modules, systems, and technical partners. All integrations must comply with State defined integration protocols, as outlined in Attachment V: Medicaid Integration Services Core Capabilities. The Vendor must establish and maintain direct interfaces with external credentialing and verification sources (e.g., national databases, licensing boards). These integrations must support real-time or scheduled data exchanges to ensure provider records remain current and accurate. All interfaces must comply with requirements defined in Attachment AB: Interfaces, including direct primary source credentialing integrations not listed in Attachment AB: Interfaces.

As the centralized repository for provider and provider entity data used across the MES for Medicaid Direct and Managed Care, the PDM/CVO shall validate provider enrollment and status for data sourced externally. For example, while Managed Care Plans maintain their own provider networks, the PDM must verify that contracted providers meet enrollment and credentialing requirements and make validated network data available for downstream processing.

The Vendor must ensure all data sharing activities comply with applicable federal and state privacy and security standards. The PDM integration layer shall include monitoring, logging, and reconciliation capabilities to track data transmissions and ensure data integrity across the MES.

3.1.3 Project Management and System Development Requirements

The Vendor must apply industry standard project management and system development methodologies (e.g. Waterfall, PMBOK, Agile, etc.) to the initial implementation of the proposed solution and to each subsequent enhancement or iteration of the solution. The Vendor must maintain communication with other contractors and NCDHHS management and staff as necessary to meet its responsibilities related to this RFP's scope of work and as defined in Section 7.11 Project Management.

System Development Methodology

The Vendor must follow an industry-standard system development methodology for the initial implementation of the proposed solution and throughout the Contract term. The Vendor must work with the NCDHHS MES Team to confirm the Vendor's understanding of the RFP

requirements and to reconcile the RFP requirements for the scope of work against the proposed solution. The Vendor shall conduct requirements-gathering sessions with the State to identify and discuss any solution gaps for the scope of work.

Design Configuration, and Build and Requirements Traceability

The Vendor shall, in the design sessions, recommend solutions for each configuration gap, as defined in requirements validation, that will produce the desired business outcomes. The Vendor must undertake activities to resolve gaps between the RFP requirements and the proposed solution. Once designs have been approved by NCDHHS, the Vendor shall configure and/or customize the software platform it uses to manage the credentialing and enrollment process. Such configuration/customization will be made in accordance with the needs of the State, PHPs, and the Credentialing Committee. The Vendor shall map all requirements to the work required to achieve the specific desired outcomes and ensure that requirements can be traced to work, testing, final outcome, and state approval.

Data Conversion, Cleansing and Migration

The Vendor is responsible for the end-to-end planning, execution, and validation of data conversion, cleansing, and migration activities necessary to transition provider data from legacy systems into the new Provider Data Management (PDM) solution.

The Vendor must conduct a comprehensive assessment of existing provider data sources, including legacy systems and third-party databases. The Vendor must develop a detailed data mapping document that aligns legacy data elements with the target data model of the PDM solution and addresses gaps between the legacy data model and the PDM/CVO. The canonical provider data model is available in the Bidder's Library.

The Vendor must perform data cleansing activities to ensure the accuracy, completeness, consistency, and validity of provider data prior to migration. Data must comply with the Department's data governance policy for data quality. This includes standardizing data formats, resolving data conflicts, deduplicating, and validating against authoritative sources.

The Vendor must convert and transform legacy data into the format required by the PDM solution. This includes applying business rules, formatting standards, and validation logic to ensure compatibility with the new system.

The Vendor must provide detailed documentation of the data conversion and migration process, including data mapping, cleansing rules, transformation logic, and validation results. Regular status reports shall be submitted to the State throughout the migration process. The Vendor shall develop a test plan specific to data conversion and migration that outlines the testing strategy, scope, test scenarios, and acceptance criteria. This applies to document migration in addition to data conversion.

For migration of documents, the Vendor shall conduct an inventory of existing documents to identify the different document types and formats. Document metadata shall be defined to ensure efficient indexing and retrieval of documents to be integrated as part of the provider's comprehensive record allowing access to documents using role-based access permissions. The Vendor shall perform a quality review of documents to identify duplicates and corrupt files for removal. The State shall approve the document mapping, document migration strategy and validation results. The Vendor can assume 24 different document types and a volume of approximately 4,250,000 documents to migrate.

The Vendor must map user roles and permissions from the legacy system to the equivalent roles in the PDM/CVO. This includes creating user accounts with the appropriate roles and links to appropriate provider records and documents. This will require NCDHHS cross functional

stakeholder engagement to validate role definitions and access needs. The Vendor must conduct a data quality review to identify inactive, duplicate, and unauthorized accounts for removal. The conversion plan and conversion test plan for user accounts must detail how automated tools are to be used to migrate the user accounts, preserving roles and access levels and where high-privilege accounts that need manual review and approval by the State are needed. The State shall approve the role mapping, conversion strategy, and validation results.

The Vendor must execute the migration of cleansed and validated data into the PDM solution using secure, auditable processes. Migration shall occur in phases (e.g., pilot, full load) and must include rollback and recovery procedures. A mock conversion of data, documents, and user roles are required prior to implementation. All data handling activities must comply with applicable federal and state privacy and security regulations, including HIPAA. The Vendor must ensure that all data in transit and at rest is encrypted and that access is restricted to authorized personnel only.

The Vendor must work with the State to identify a cutover plan to convert provider data from applications that are in progress during the transition to the PDM/CVO. This plan shall include the approach for coordination with the legacy vendor when new applications are no longer accepted and considerations for short-term dual processes where necessary.

The Vendor must collaborate closely with the State throughout all phases of data conversion, cleansing, and migration. The State shall review and approve key deliverables and activities prior to execution. The Vendor must not proceed with data migration activities until the State has formally approved the associated data/document mapping, cleansing, and transformation documentation. The Vendor must provide opportunities for the State to participate in validation and reconciliation activities to ensure data quality and integrity post-migration.

Testing

Testing is a critical component of successful implementation of any system configuration/development effort; therefore, in depth, process driven, fully documented testing processes are required for all implementations and configuration changes within the North Carolina Medicaid enterprise. The testing activities shall include planning, managing, and executing a comprehensive testing effort that includes unit, system, regression, parallel, integration, UAT, and enterprise End-to-End Testing. North Carolina Medicaid enterprise testing expectations and definitions are fully documented in Section 7.17 Testing.

During DDI and prior to implementing a new release during O&M, the Vendor is responsible for ensuring that all required tests are performed and evidence that each component meets or exceeds all relevant functional, technical, security, and performance requirements is provided.

Training

The Vendor must provide training to designated NC MES team members, NCDHHS staff, Vendor staff, internal and external users (including providers and applicants), and other staff as needed to explain how users in each role should use the solution to accomplish tasks assigned. Training must be developed and published in advance of the transition to the Vendor's solution and any significant system or process modifications. The Vendor must use the Department approved training media, including, but not limited to teleconferencing, Web-based training, and computer-based training. Users must become proficient in using and viewing information in the Vendor's solution to ensure effective and efficient business operations and service delivery.

Implementation and Acceptance

Prior to implementation, the Vendor must demonstrate readiness to implement the solution and provide operational support and maintenance of the proposed solution(s) for the remainder of the Contract term. The Vendor is responsible for managing the end-to-end implementation of the proposed solution. The Vendor must actively participate with NCDHHS in the development of strategies for a successful transition.

NCDHHS must formally approve the implementation of the solution based on predefined acceptance criteria. NCDHHS's acceptance of the solution will initiate the Operations, Maintenance, and Configuration phase of the contract.

Staffing support

The Vendor must fill any staffing needs to ensure a sufficient level of support upon Program implementation. The Vendor must provide a timetable for filling all position(s) not already designated to existing staff.

3.1.4 Certification

The Vendor must work with NCDHHS and other Contractors as necessary to ensure that all solutions provided by the Vendor meet requirements specified in the relevant federal certification requirements as described in the most current version of the Streamlined Modular Certification, available at <https://cmsgov.github.io/CMCS-DSG-DSS-Certification/>

The Vendor is responsible for providing and maintaining a solution that meets all applicable checklist items in the most current version of the Streamlined Modular Certification (SMC), and for supporting the review and validation of those items by the Department, and CMS. The Vendor must become knowledgeable of all SMC-related items associated with the solution offered.

The Vendor must provide staff and other resources to support and participate in SMC milestone reviews and other Certification activities that occur before, during, and after implementation of the proposed solution(s).

3.1.5 Customer Relationship Management and Provider Call Center

Customer Relationship Management

The Vendor's solutions and services will include providing and utilizing a Customer Relationship Management (CRM) tool to manage correspondence with providers. The CRM tool will capture interactions with providers through free-form text, pre-defined data elements, and be capable of searching logged correspondence on command. The CRM tool will support attachments; linking of documents and information within the tool; and routing of correspondence and captured information through the workflow to specific individuals. All correspondence from providers and sent to providers must be stored in the content management solution.

Provider Call Center

The Vendor's solutions and services must include a call center for providers inquiring about enrollment in NCDHHS programs, applicants, and existing providers regarding their enrollment records via a toll-free telephone number, email address, online mechanisms (chat features and contact us form), fax number, and mailing address.

The Vendor will be fully responsible for providing support for providers without additional assistance from the State. This support includes:

- Application Support:
 - Help providers complete the online enrollment applications (initial enrollment, re-enrollment, re-validation, and provider-initiated change requests).
 - Answer questions about required documentation (e.g., licensure, credentialing).
 - Guide users through the self-service portal.
- Application Status Updates
 - Clarify issues related to missing or incorrect information in applications
 - Provide updates on the status of a submitted application
- Questions related to changes in provider information, such as:
 - Notifications sent to providers
 - Provider status updates
- Troubleshoot technical issues the users may be experiencing with the self-service portal

Interactive Voice Response System

The Vendor's solution shall include an Interactive Voice Response (IVR) System to welcome and route incoming provider calls, convey educational alerts during hold times, and intelligently queue providers until Vendor staff are available. The IVR system will include the ability for the provider to leave a message during or outside of normal business hours.

3.1.6 Operations, Maintenance, and Configuration Requirements

The Vendor shall provide Operations support, Maintenance, and ongoing Configuration of the provided Solution(s) throughout the life of the Contract. This includes providing Operations support as described in the scope of work, as well as providing Maintenance and Enhancements to the provided Solution(s). The Vendor will follow project management and system development processes throughout the life of the Contract.

Throughout the life of the contract, there are two distinct classifications of work that all NC MES Module Contractors will perform: maintenance and system enhancements.

Maintenance Enhancements

NCDHHS defines maintenance for each NC MES module as follows:

1. Making configuration updates as requested by NCDHHS. Configuration includes changes to table values, parameters, codes, and business logic, including hardcoded business logic.
2. Correcting deficiencies (defects) found in the solution(s) based on detailed requirements described in the scope of work and published design specifications.
3. Correcting deficiencies (defects) found in the solution(s) based on a failure to meet the detailed requirements in completed enhancement, configuration, or maintenance requests.
4. Conducting research requested by NCDHHS or required to support the Department. For example:

- a. System behavior and results
- b. New healthcare initiatives
- c. Best practices research across states and industry
- d. Impacts of new State and federal legislation
5. Performing mass adjustments or mass changes as requested by NCDHHS or required to support North Carolina Healthcare Programs (for example, errors in pricing, eligibility, cost share, and financial code assignments, TPL discovery, and provider reimbursement changes).
6. Performing all maintenance activities necessary to ensure continued functionality, security, and integrity of the system and its associated components. Examples of maintenance include, but are not limited to:
 - a. Performance optimization.
 - b. Database management.
 - c. Software, hardware, and tools (e.g., patches, upgrades, and replacement).
 - d. Interface, report, and correspondence changes.
 - e. Making corrections or changes to maintain the integrity of the system or the data within it (e.g., backing out changes, correcting duplicate records, cleansing corrupt data, adding security measures, adding redundancy).
7. Using appropriate testing, configuration, and changing control procedures.
8. Updating system, user, and training documentation and online help to reflect changes that have been made to the solution.
9. Performing the activities above to maintain customizations implemented as part of an approved enhancement.
10. Perform incremental integration services via configuration. Incremental integration services should be included in the DDI costs.

If incremental integration can be handled using configuration, the integration will fall under the definition of maintenance. If the incremental integration requires system development and testing efforts, the integration will fall under the definition of enhancement.

All maintenance activities will be performed at no additional cost to the State in the Vendor's response. The Vendor will be required, at no additional cost, to add resources necessary to complete all activities by the required due date. Maintenance activities and any associated hours will not be applied to the system enhancement hourly pool.

System Enhancements

NCDHHS defines system enhancements as follows:

1. System enhancements exclude any activities defined in "Maintenance" above.
2. New features or functionality that fall outside the scope of all RFP requirements, Offeror's RFP response, the contract, or agreements of any supplemental negotiations.

The State must approve both the design and level of effort prior to the start of development or configuration for system enhancements. NCDHHS must approve any changes to the design or level of effort that occur after the original approval. The level of effort billed cannot exceed the level of effort approved by NCDHHS. The level of effort incurred to complete an enhancement will be applied to the Necessary System Change (NSC) hours once the enhancement is implemented and approved by the Department. If the level of effort exceeds the NSC hours remaining, the Department may choose to utilize hours from the next Contract operations year or have the Vendor invoice the Department for the balance at the rates defined in Attachment E: Cost Form.

The Vendor must provide an estimate of any impact to annual operations cost for the enhancement during the operations phase of the Contract, if applicable. Reimbursements for any additional operations costs must be addressed in a contract amendment.

3.2 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.2.1 REQUIREMENTS

A requirement is a function, feature, or performance that the system must provide.

3.2.2 SPECIFICATIONS

A specification documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, will mean that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.2.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency with complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modifications in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor, and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.2.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturers or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.2.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a. Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
- b. Identify and explain any components that are missing from the State's existing license agreement.
- c. If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.
- d. Explain the transportability and transferability of the proposed license agreements.

3.2.6 ENTERPRISE ARCHITECTURE STANDARDS

The Department maintains a comprehensive set of Enterprise Architecture artifacts that must be created and maintained by vendors. The Department's Enterprise Architecture is based on the Federal Enterprise Architecture framework and is aligned with the MITA framework. The Department's framework will leverage the MITA standards and additionally use standard conventions such as Unified Modeling Language (UML) 2 and Business Process Modeling and Notation (BPMN). The Department maintains the right to add or change its Enterprise Architecture artifacts as its needs change. The Vendor will be required to provide and maintain standard documentation. The details are referenced in *Attachment J: Enterprise Architecture*.

3.3 SECURITY SPECIFICATIONS

3.3.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE - RESERVED

3.3.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The PDM/CVO Solution will be required to receive and securely manage data that is classified as High Risk. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding this data classification. The policy is located here: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using National Institute of Standards and Technology (NIST) 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solution which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

- a. Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located here: <https://it.nc.gov/documents/vendor-readiness-assessment-report>
- 1) Vendors shall provide a current independent 3rd party assessment report in accordance with subparagraphs i)-iii) at the time of offer submission.
 - i. Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

- ii. A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.
- iii. An IaaS vendor cannot provide a certification or assessment report for a SaaS vendor UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.
- c. Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

3.3.3 VULNERABILITY RISK RATINGS AND REMEDIATION

Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 “Qualitative Severity Rating Scale” for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a common vulnerability and exposure, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above “info”, or a score of 0, may be used after appropriate review.

The risk ratings and remediation timelines are assigned to vulnerability follows:

- a. Critical-level Risk (Priority/CVSS 9.0-10.0): A vulnerability that could cause grave consequences and potentially lead to leakage of sensitive data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner. Critical-level risk vulnerabilities must be, at a minimum, remediated within seven (7) days.
- b. High-level Risk (Priority/CVSS 7.0-8.9): A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. High-level risk vulnerabilities must be mitigated or remediated within thirty (30) days.
- c. Medium-level Risk (Priority/CVSS 4.0-6.9): A vulnerability that should be addressed within the established timelines. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner. Medium-level risk vulnerabilities must be mitigated or remediated within sixty (60) days.
- d. Low-level Risk (Priority/CVSS 0.1-3.9): A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Low-level risk vulnerabilities must be mitigated or remediated within ninety (90) days.

3.4 ENTERPRISE SPECIFICATIONS

3.4.1 ENTERPRISE STRATEGIES, SERVICES, AND STANDARDS

Agencies and vendors should refer to the Vendor Resources Page for information on North Carolina Information Technology enterprise services, security policies and practices, architectural requirements, and enterprise contracts. The Vendor Resources Page can be found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

3.4.2 ARCHITECTURE DIAGRAMS

The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. Diagrams, required at offer submission, should be created using the template that can be found at the following link: <https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192>.

There may be additional architectural diagrams requested of the Vendor after contract award. This will be communicated to the Vendor by the agency as needed during the project.

Please review *Attachment U: Conceptual Architectural Diagrams* for a detailed architecture of the future state.

3.4.3 IDENTITY, Credential, and Access Management (ICAM)

Identity, Credential, and Access Management is a crucial component of modern IT security strategies, providing a robust framework to protect an organization's digital assets while enabling efficient and compliant business operations. The State provides an Identity and Access Management Solution (NCID) and requires all inter-agency and external facing solutions/applications to use NCID. NCID enforces policies for identity management such as:

- a. Common user ID and passwords;
- b. Central, delegated ID management;
- c. Central repository of IDs and authentication policies;
- d. Self-registration and password recovery; and
- e. Tooltips to verify new passwords meet the State's password policy.

Documentation and resources are available from the State to provide guidance for using the NCID solution to individuals, business users, government employees, and contractors.

- [NCID resources - Individual and Business users](#)
- [NCID resources – Government employees and Contractors](#)

A solution's ICAM integration to the NCID solution is accomplished by one of the following protocols:

- Security Assertion Markup Language (SAML v2)
- OAuth/OIDC

The State has developed a Medicaid Enterprise System Portal (MES Portal) which provides an entry point into the NC MES Medicaid system and displays the MES modules to which a user has access based on the coarse-grained authorization. When linking and signing into an MES module's application, the MES module will provide fine-grained authorization to give the user the appropriate access within the application.

Multi-Factor Authentication (MFA) will be provided by NCID and will be used when logging in by MES Modules to provide enhanced security in addition to the use of a username and password. The MES Modules will make available to users State documentation and guidance for installing MFA options to work with NCID.

- [NCID MFA Documentation and Guidance](#)

Please review *Attachment V: Medicaid Integration Services Core Capabilities* for additional information on ICAM and the MES Portal.

3.5 BUSINESS AND TECHNICAL REQUIREMENTS

The Vendor must provide a response in their offer to all requirements as part of the technical proposal as defined in *Attachment T: Technical / Management Proposal*. If any of the RFP requirements cannot be met, the State will disqualify the Vendor from further evaluation.

Note: The number assigned to each requirement in the following tables may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

3.5.1 REQUIREMENTS

Table R1. Architecture

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-ARCH-001	The Vendor must provide multiple sessions /environments/applications/areas/views simultaneously. This includes providing sufficient environments and configurations (e.g., multiple environments, multiple application layers, hub architecture) necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery).	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-ARCH-002	The Solution's user interfaces must be compliant with Section 508 of the Rehabilitation Act and 45 CFR part 170, subpart B.	
PDM-REQ-ARCH-003	The Solution must provide an isolated, secure, scalable, and highly available Production (PROD) environment for live business operations.	

Table R2. Business Operations

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-001	The Solution must receive provider applications through a web-based provider self-service tool. The Solution must allow for the enrollment, re-enrollment, revalidation, and provider-initiated change requests (e.g. voluntary disenrollment/termination, updates to required licensure, adding/removal of affiliations).	PIC-01
PDM-REQ-BO-002	The Solution must provide automated verification and validation of provider information and credentials for enrollment, screening as well as monthly monitoring eligibility. At a minimum, the following screening processes must be automated: •National Plan and Provider Enumeration System (NPPES) •Social Security Administration's Death Master File •List of Excluded Individuals/Entities (LEIE) •Excluded Parties List System (EPLS) as maintained by System for Award Management (SAM) •National Practitioner Databank (NPDB) •NC State Bureau of Investigation (SBI) •NC Provider Penalty Tracking Database (PPTD) •Criminal Background Checks	BR-08-001, BR-08-026, BR-01-008, BR-06-005, BR-06-007, BR-06-013, BR-06-012
PDM-REQ-BO-003	The Solution must assign a system generated provider ID for providers without NPIs (atypical providers).	BR-13-001, APP-13, APP-02

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-004	The Solution must allow providers to enroll in sub programs respective to each NCDHHS division during the enrollment process when the provider's qualifications meet the criteria as established in the respective business rules. For example, enrollment in Medicaid with Primary Care Provider qualifications allows the provider to enroll in managed care programs as a primary care provider or primary care management provider.	BR-08-006, APP-02, APP-03, APP-04, APP-05, APP-11, APP-13
PDM-REQ-BO-005	The Solution must allow a provider to use a single application to enroll in multiple programs, locations, taxonomy codes, and services.	APP-02, APP-03, APP-01, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-11, APP-12, APP-13
PDM-REQ-BO-006	The Vendor must provide the capability for a consolidated, centralized provider enrollment and credentialing system to enroll/reenroll/credential/revalidate health care practitioners, organizations and facility providers (taxonomy driven) and non-health care entities (with no taxonomy) into NCDHHS programs following criteria and business rules that are Department specific. The NCDHHS programs supported include Medicaid, Mental Health, Developmental Disabilities, Substance Use Services, Department of Public Health, and Division of Child and Family Wellbeing, or any programs as defined by the Department.	APP-02, APP-03, APP-01, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-11, APP-12, APP-13
PDM-REQ-BO-007	For enrolling and actively enrolled providers electing to participate in specific programs, the Solution must collect and maintain the supporting data (e.g., geographic locations, number of preferred assigned members, and capacity to accept additional members), present the program agreement/contract for review, and acceptance (i.e., digital signature).	BR-08-006, APP-02, APP-03, APP-01, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12, APP-13, PIC-01

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-008	The Solution must be configurable to allow or prevent provider enrollment based on provider eligibility criteria.	
PDM-REQ-BO-009	The Solution must collect, validate, and maintain all information needed to complete provider enrollment in compliance with all State and federal policies and regulations following department business rules.	BR-08-005, BR-08-008, BR-13-002
PDM-REQ-BO-010	The Vendor must determine provider eligibility in accordance with State and Federal policies and regulations, following Department Business Rules.	JA-001
PDM-REQ-BO-011	The Solution must be capable of suspending or terminating provider participation in specific programs/taxonomy codes while maintaining participation in other programs/taxonomy codes.	
PDM-REQ-BO-012	The Solution must maintain the provider's effective date including retroactive effective dates to begin administering services according to the business rules.	BR-08-019
PDM-REQ-BO-013	The Vendor must monitor Centers for Medicare and Medicaid Services (CMS) notifications received directly or from the Department (e.g. Denial of Payment for New Admissions (DPNA), Change of Ownership (CHOW), Imposition and Compliance, etc.) and must take automated or manual action per Department approved processes or business rules	BR-03-001
PDM-REQ-BO-014	The Solution and the Vendor must adhere to all NCQA credentialing standards.	BR-06-009, BR-06-006
PDM-REQ-BO-015	The Vendor must obtain via electronic signature all required attestations and agreements wherever a signature is required. The Vendor must ensure the electronic signature belongs to an authorized individual listed on the application and/or provider's record.	BR-08-016, BR-01-004

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-016	The Vendor must reconcile State Bureau of Investigation (SBI) results to pending provider applications requiring fingerprinting when the case number, last name, first name, Social Security Number (SSN) or date of birth are not an exact match.	BR-07-007
PDM-REQ-BO-017	The Vendor must be certified by the National Committee for Quality Assurance (NCQA) in Credentialing. Certification includes all core credentialing standards and all credentialing certification standards. If the Vendor is not currently certified in Delegation, as it is not required to be a CVO, the Delegation standard must be applied for with successful certification at the next NCQA certification renewal.	
PDM-REQ-BO-018	The Vendor must review and evaluate enrollment requirements against NCQA updates and submit any recommended updates to the Department for review and approval prior to implementation.	
PDM-REQ-BO-019	The Solution must include a process to complete revalidation of providers following Department business rules.	BR-22-001
PDM-REQ-BO-020	The Vendor must perform the federally mandated screening site visit of Medicaid providers classified as moderate and high risk per federal regulations 42 CFR § 455.432 Site visits and 42 CFR 455 Subpart E and NCGS 108C-3 following Department business rules.	BR-08-009
PDM-REQ-BO-021	The Vendor must notify the credentialing decisions of all applications and determination decisions to the provider per the business rules.	BR-08-024

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-022	The Vendor is responsible for the operation of an NCQA-compliant Credentialing Committee to evaluate and make credentialing decisions for applicants and providers for NCDHHS. The Credentialing Committee is composed of a Vendor-employed Medical Director, designated voting members, non-voting members, and Vendor-coordinated peer review experts who represent key stakeholders across NCDHHS, contracted entities, and managed care organizations. All members will carry out their responsibilities in accordance with the Bylaws and Policies and Procedures. The Credentialing Committee must review and render decision on credentialing files classified as medium or high risk; files may include: · initial enrollments · re-enrollments · revalidations · provider submitted data change requests · active providers with actions found during the Vendor's ongoing monitoring.	BR-06-003
PDM-REQ-BO-023	The Vendor must meet with the Department and other stakeholders as needed, to assist in the maintenance and continual improvement of the credentialing process.	
PDM-REQ-BO-024	The Vendor must prepare and make electronically available to all committee members a Provider Profile Package for each medium and high-risk provider under consideration which contains all primary source verifications and supporting documentation. The package will include: · Provider information - type/specialty, risk level, file ID, review type (application type/ongoing monitoring) · A brief, objective description of any concerns or findings that elevate the file's risk status. · A summary of each of the applicable primary source	BR-06-003

Requirement #	Requirement Description	Business Rules/Application Data Files
	verification results · Supporting documentation	
PDM-REQ-BO-025	The Vendor must provide administrative and customer service support to the Credentialing Committee. This will include: · Scheduling Credentialing Committee meetings, developing agendas, and distributing materials for the meetings in advance; · Flagging specific provider records or files for review; · Attending and keeping minutes of the Credentialing Committee decisions; · Enact the Credentialing Committee's credentialing decision in the provider's enrollment record; · Answering Credentialing Committee questions about the PSV file or its contents; · Answering Credentialing Committee questions about any aspect of the primary source verification work; and · Performing follow-up or supplementary research, as required, to enable to the Credentialing Committee to render a credentialing decision.	
PDM-REQ-BO-026	If the provider submits the application and does not supply any of the required documentation within a timeframe determined by the Department, the Vendor must abandon initial enrollment, re-enrollment, provider-initiated change request, and re-validation. For abandoned revalidations, terminate the provider.	BR-08-024, BR-22-001
PDM-REQ-BO-027	The Vendor must conduct a search at initial enrollment, re-enrollment, revalidation, as well as ongoing monitoring of the Provider Penalty Tracking Database (PPTD) to identify providers, owners, subcontractors, and managing	BR-06-013

Requirement #	Requirement Description	Business Rules/Application Data Files
	relationships who have violations that have resulted in penalties or serious administrative actions against their license.	
PDM-REQ-BO-028	The Vendor must notify Office of Inspector General (OIG), National Provider Data Bank (NPDB), Provider Penalty Tracking Database (PPTD), CMS Data Exchange System (DEX) or other appropriate agencies of providers terminated 'for cause'.	BR-11-002.
PDM-REQ-BO-029	The Vendor must terminate a provider's participation in Medicaid in accordance with section 1902(a)(39) (Adverse Action Report) of the Social Security Act as amended by Section 6501 of the Affordable Care Act and business rules defined by the Department.	BR-13-004
PDM-REQ-BO-030	The Vendor must exclude providers from the revalidation process based on business rules determined by the Department.	BR-22-001
PDM-REQ-BO-031	The Vendor must include in all denial and termination notices the state approved appeal rights to which providers are entitled, per State Business Rules.	BR-01-005
PDM-REQ-BO-032	The Vendor is responsible to provide oversight and monitoring of each delegated entity to include: A pre-delegation audit that includes a performance and staffing assessment, a policy and procedure review, and a review of the entities understanding and adherence to NCQA, State, Federal enrollment and credentialing requirements and delegation tasks. Completion of an annual compliance audit to re-review all the components of the pre-delegation audit, audit 20% of the entity's credentialing and recredentialing files against NCQA, State, and Federal enrollment and credentialing requirements, and create corrective action plans on deficiencies in collaboration with the Department to include revocation recommendations of delegated entity participation. Vendor must report results to the Department on each pre-delegation and annual compliance audit.	BR-10-001

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-033	The Vendor must provide additional workflows that allow for attestations in managed care programs for providers credentialed by a delegated entity.	BR-10-001
PDM-REQ-BO-034	The Solution must support Department defined needs concerning provider Change of Ownership, to include at minimum the collection of Department required documentation, notification and dispersion to the Department, and the support of provider-initiated enrollment and record maintenance modifications.	BR-12-001, APP-02, APP-03, PIC-01
PDM-REQ-BO-035	The Vendor must accept data exchanges with the delegated credentialing entities that include provider data as defined by the Department.	BR-10-001
PDM-REQ-BO-036	The Vendor must uniquely identify and track providers who are credentialed by a delegated credentialing entity in order to exclude them from standard credentialing processes and/or other delegated entities credentialing processes.	BR-10-001
PDM-REQ-BO-037	The Solution must reconcile discrepant data received across multiple delegated entities.	BR-10-001
PDM-REQ-BO-038	The Vendor must maintain an affiliation between the delegated credentialing entity and its rostered providers.	BR-10-001
PDM-REQ-BO-039	The Solution must be used to track the status of an appealed application denials and appealed provider terminations.	BR-01-005
PDM-REQ-BO-040	The Solution must allow for an individual rendering/attending provider to affiliate to a group's (organization's) locations or servicing counties where the individual renders services. The system must apply these locations or servicing counties to the individual provider's record per the State's business rules.	BR-08-021, APP-12, APP-04, APP-05

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-041	The Solution must include an automated process to receive, validate, update provider license, accreditation, and certification data from the primary source at a frequency determined by the state (monthly or more often). At a minimum, the Solution must automate with the following boards: · NC Medical Board · NC Dental Board · NC Board of Nursing · NC Optometry · NC Pharmacy Board · Clinical Laboratory Improvement Amendment (CLIA) · Drug Enforcement Agency (DEA) · NCDHHS Division of Health Service Regulation	
PDM-REQ-BO-042	The Vendor must assess and validate the qualifications of the Provider, including all primary source verifications (PSV) at no additional cost to the Department (e.g. NPPES, license, malpractice), for initial enrollment, re-enrollment, re-validation, and change request applications following NCQA Credentialing standards, federal and state regulations, and Department business rules. Vendor must make at least three (3) attempts to verify each required credentialing data element if the initial attempts are unsuccessful. If all attempts fail, the source must be marked as Unable to Verify" (or a similar message) on the Provider record.	BR-08-001; BR-08-009; BR-12-003; BR-22-001; BR-08-022; BR-08-023
PDM-REQ-BO-043	The Vendor's workflow technology must be used to automate the organization and flow of all application processes, credentialing events and provider notifications. The workflow must integrate seamlessly across intra Solution modules for access to current and historical provider data, credentialing and verification sources and stored documents.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-044	The Vendor must continuously monitor adverse actions about all actively enrolled providers, managing relationships, subcontractors, and owners as applicable and as defined in the Business Rules. Vendor must document, terminate, take no action on the provider, or present provider with adverse actions to the Credentialing Committee as defined in the Credentialing Committee Bylaws.	BR-12-002
PDM-REQ-BO-045	The Solution must automatically deny locations/applications (initial enrollment, re-enrollment, revalidation, and provider-initiated change requests) and terminate locations/providers when a provider fails (including failing to complete) the federal screening and/or site visit.	BR-08-009
PDM-REQ-BO-046	The Vendor must ensure all new providers complete the New Medicaid Provider Enrollment training as required with NCGS § 108C-9 following Department business rules. The Vendor must automatically deny an initial enrollment application if the provider fails the required training.	BR-06-004
PDM-REQ-BO-047	The Vendor must retain untouched applications for 90 calendar days and allow the provider to return and resume the application process. The Solution must automatically purge untouched applications following Department business rules.	BR-08-024
PDM-REQ-BO-048	The Solution must capture ownership information in accordance with 42 CFR 455.104 and 42 CFR 455.106 and corroborate ownership information, disclosed and non-disclosed, for every organizational provider as per the State's defined business rules.	BR-08-003, APP-02, APP-03, APP-04, APP-05, APP-08, APP-09, APP-10, APP-11
PDM-REQ-BO-049	The Solution must maintain a provider's overall enrollment status and statuses at more detailed levels to include programs, locations, taxonomy, and service levels as defined in State Business Rules. The Solution must identify the status (active, suspended, terminated)	

Requirement #	Requirement Description	Business Rules/Application Data Files
	and a detail reason for the suspended or terminated status.	
PDM-REQ-BO-050	The Solution must set application status and provide the capability for authorized provider/applicant, Vendor, and Department users to view a detailed status of a submitted application. The application status information must otherwise be protected from viewing by any other party.	BR-08-024
PDM-REQ-BO-051	The Solution must support the capability for the Department to set CMS and State-imposed temporary moratoria on new providers or provider types following CMS or State directed timelines.	
PDM-REQ-BO-052	The Vendor must collect, store, maintain and display servicing counties for providers who don't have a physical location.	BR-08-021, APP-01, APP-03, APP-02, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12
PDM-REQ-BO-053	The Solution must provide the ability to electronically collect, accept, and track the NC application fee from a provider as defined by the Department's Business Rules.	BR-08-004
PDM-REQ-BO-054	The Solution must identify when the NC fee and/or the Federal Fee are required based on department business rules. The Solution must provide the capability to collect the Federal fee and NC Application fee in one transaction when required. The Solution must integrate with the State's preferred payment service.	BR-08-004
PDM-REQ-BO-055	The Solution must allow for organizations to request an affiliation from individuals, notify the individual of the added affiliation, and allow the individual to authorize or decline the affiliation. The Solution must allow for individuals to affiliate to organizations, must notify the organization of the added	BR-08-017, APP-01, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-11, APP-12

Requirement #	Requirement Description	Business Rules/Application Data Files
	affiliation, and allow for the organization to authorize or decline the affiliation.	
PDM-REQ-BO-056	The Vendor must generate a public facing version of the Business Rules associated with Provider Enrollment that is accessible from the public portal for provider reference.	
PDM-REQ-BO-057	The Solution must create a Maintain Eligibility process for providers who have no claims or encounter activity within the past year following Department business rules, allowing for exclusions. The process will allow the provider to confirm continued participation or terminate the provider for no claim's activity. The Solution must accept data from external sources to identify providers who meet the criteria to maintain eligibility.	BR-13-005
PDM-REQ-BO-058	The Vendor must make updates to provider agreements, attestations, template letters, or notifications, static text and/or exclusion sanction questions, as directed by the State.	
PDM-REQ-BO-059	The Solution must ensure the primary provider office administrator and any secondary provider office administrators included in the application are designated as the provider, managing employee, or an owner of the organization.	BR-01-001, APP-01, APP-02, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12, APP-13

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-060	The Solution will support eligible providers' ability to enroll in Primary Care Case Management (PCCM) programs. - Providers must be given the option to self-select to participate in Carolina Access (CA) as part of their NC Medicaid initial, re-enrollment, revalidation, or data maintenance provider applications, regardless of their current CA status, if their taxonomy is eligible to participate. - The applicant will be required to answer CA specific enrollment questions - The Vendor must review the provider's request and approve CA participation based upon department business rules. Upon approval, the Solution will set the enrollment date as the first of the following month and default the provider as an Advanced Medical Home Tier 2 provider with the same enrollment date.	BR-08-006, APP-11, APP-04, APP-03, PIC-01
PDM-REQ-BO-061	The Solution must allow credentialing information to be collected and linked to the Physical Locations of Organizations/Facilities for the credentials found in the License and Accreditation types provided by the Department.	APP-01, APP-02, APP-03, APP-08
PDM-REQ-BO-062	The Solution will have the ability to systematically terminate a provider's Provider Enrollment record when the provider's Revalidation application is denied or incomplete for any reason; following Department Business Rules.	BR-22-001
PDM-REQ-BO-063	The Solution will support the provider's ability to request to terminate their participation in the Primary Care Case Management (PCCM) program. The Solution will set the termination date to the end of the month to allow member reassignment.	BR-08-006, PIC-01
PDM-REQ-BO-064	The Solution must allow a provider to change any information on the initial and re-enrollment application and/or revalidation and provider-initiated change	BR-08-03, PIC-01

Requirement #	Requirement Description	Business Rules/Application Data Files
	requests, including the Tax ID and SSN information within the application prior to submission.	
PDM-REQ-BO-065	The Solution must allow providers to view their current enrollment status and current data on file. The Solution must allow organization and individual providers to change any enrollment information, including the Tax ID and SSN information, within an application without requiring them to disenroll and reenroll, as stated in the Department Business Rules. The Solution must create a document of changes made to the provider's record for each submitted change request; the document must be attached to the application and the provider's record.	BR-0803, PIC-01

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-066	The Solution must provide a role-based interface design that is easy to use and encourages provider engagement. The design must: · Provide real-time validation against available, acceptable primary sources · Prompt users to correct data entry errors, missing data or inconsistencies · Provide a user-friendly Graphical User Interface supported with interactive workflows that lead the user through steps associated with the application type, capturing information needed to support appropriate business process events · Engineer workflows to support and manage automated process events throughout the lifecycle of each application type · Breakdown complex tasks into manageable steps · Pre-populate data from acceptable sources where applicable to reduce keystrokes and keying errors · Offer pre-checked conditions to encourage engagement with training and communication · Strategically offer prompts to request providers to review and update their data · Offer additional features that further improve provider engagement	BR-08-006
PDM-REQ-BO-067	The Vendor must pose all questions as required in the enrollment process to identify the health plan(s) and benefit plan(s) enrollment for each provider.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-068	The Solution must allow the ability to manage many types of affiliations between providers and other entities.	BR-08-027, BR-08-023, BR-24-001
PDM-REQ-BO-069	The Solution must have the ability to designate a few of the Vendor's Management Level Staff Members to be super users. This super user role must allow these users to make changes directly to a provider's record at the sole written direction of State Leadership, within 48 hours of notification. Super users and State Leadership will be identified and documented in change control process documentation.	BR-13-008
PDM-REQ-BO-070	Two hundred and ten (210) days prior to the CMS re-validation due date, the Vendor must start the revalidation process, by opening the re-validation application to the providers due and sending an electronic invitation. The provider will be given seventy (70) days to complete and submit the re-validation application with applicable fee payments. The Vendor must send reminders to providers that have not submitted the re-validation application with applicable fee payments at fifty (50), twenty (20), and five (5) days prior to the provider's due date. If the provider has not submitted the re-validation application with applicable fee payments by the due date, the following day the Vendor will suspend the provider's record. The suspension will stay on the record until the re-validation is satisfied, or termination date comes. If the provider has not satisfied the revalidation fifty 51 days after suspension was applied the provider will terminate. The Vendor will have the remaining timeline, of the two hundred and ten (210) days left to process the revalidation to completion prior to the CMS re-validation due date.	BR-22-001
PDM-REQ-BO-071	The Vendor must have the ability to transfer or copy data about the provider as directed by the State. This includes the ability to complete mass updates.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-072	The Vendor must have the ability for a provider to initiate the merge of provider records into one existing record per State business rules.	BR-13-003
PDM-REQ-BO-073	The Vendor must ensure all categorical high-risk NC Medicaid providers and owners with 5% or greater ownership interest undergo Fingerprint-Based Criminal Background Checks (FCBC) as required by Centers for Medicare and Medicaid (CMS) and NC Medicaid regulations following Department business rules.	BR-06-007
PDM-REQ-BO-074	The Vendor must use an environment that facilitates quick response to changes in policy, such as rules repositories, work-flow management systems, table-driven logic, automated letter (and other communication) generation, and configuration to allow basic changes to be made quickly.	
PDM-REQ-BO-075	The Solution must allow a submitted application to be returned to the provider for correction as needed during the credentialing process, as stated in the Department Business Rules.	BR-0803
PDM-REQ-BO-076	The Solution must validate certain qualifying organizations (e.g. multi-Specialty (193200000X), Single-Specialty (193400000X, 261QP2300X (Primary Care)) have the required qualifying individual providers affiliate per the State's business rules.	BR-08-010
PDM-REQ-BO-077	The Solution must develop a process to identify required expiring licensure, accreditation, and certification to include suspension and termination following department business rules.	BR-06-010
PDM-REQ-BO-078	The Vendor must provide a HIPAA, state and federal compliant Solution that supports electronic signatures for all required agreements and attestations in accordance with applicable business rules.	BR-08-016, BR-01-004

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-079	The Vendor must query the National Practitioners Databank (NPDB) on all individual providers (to include enrolling each provider in NPDB's continuous query), review the NPDB data, receive updates from the continuous query, and identify negative results (malpractice claims, state and Medicare sanctions and exclusions, license and certification actions, etc.) which require review by the Credentialing Committee (as defined in the bylaws) during initial enrollment, re-enrollment, re-validation, and ongoing monitoring. The data from the NPDB query and the updates from the continuous query must be stored with the provider's record in PDF format.	BR-06-005, BR-06-002, BR-06-011
PDM-REQ-BO-080	The Vendor must create a process to receive and process the information from the NPDB in an ongoing process by utilizing the Continuous query option for any notifications of any new reports for a provider.	BR-06-005
PDM-REQ-BO-081	The Vendor must use the state defined contract for delegated credentialing and must require each hospital system and CIHA to sign the contract to assure that their own credentialing process meets state, federal, and National Committee of Quality Assurance (NCQA) standards applicable to NC Medicaid enrollment and credentialing.	BR-10-001
PDM-REQ-BO-082	The Vendor must generate a response to the delegated credentialing entity confirming the results of the data exchange.	BR-10-001
PDM-REQ-BO-083	The Vendor must develop methods for the Department to monitor the delegated credentialing process throughout – including but not limited to reporting and/or dashboards that allow real-time access to the status of each contract, as well as each data exchange, throughout the process.	BR-10-001
PDM-REQ-BO-084	The Vendor must implement a Corrective Action Plan (CAP) in collaboration with the Department, on the deficient delegated entity, to improve performance if findings warrant.	BR-10-001

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-085	The Solution must provide the ability to electronically collect, accept, and track the federal fee from the provider or confirm payment completed with a previous application, Medicare, or another State Medicaid Agency as defined by the Department's Business Rules.	BR-08-004, APP-02, APP-03, APP-08, APP-13
PDM-REQ-BO-086	The Solution must provide an expedited enrollment process for health care professionals to become an NC Medicaid provider due to a natural disaster following Department business rules.	BR-08-025, APP-01
PDM-REQ-BO-087	The Vendor must process disaster enrollment applications following department business rules.	BR-08-025
PDM-REQ-BO-088	The Vendor must obtain an electronic signature attestation from each individual practitioner through the Provider Portal following Department business rules. The attestation must be signed directly by the individual provider and may not be delegated.	BR-08-014
PDM-REQ-BO-089	For new provider applicants, the Solution must allow a user, with an authenticated NCID, to initiate a new enrollment application, self-designate themselves to become the primary office administrator and submit the application for processing. The user must be able to save an incomplete application then return to the application at a later time to continue the enrollment process. Upon approval of the application, the user is granted the role of the primary office administrator with full access and rights to the provider record.	BR-01-001
PDM-REQ-BO-090	The Solution must require all provider records to be managed by an office administrator as the legal authority for the provider provided the office administrator does not fail a background check or applicable fingerprint verification.	BR-01-001
PDM-REQ-BO-091	The Solution must prompt and encourage the primary office administrator to include and maintain a secondary office administrator with the same access and rights to a provider record as the primary. The secondary office	BR-01-001, APP-01, APP-02, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09,

Requirement #	Requirement Description	Business Rules/Application Data Files
	administrator is subject to the same credentialing requirements as the primary office administrator.	APP-10, APP-11, APP-12, APP-13
PDM-REQ-BO-092	The Solution must allow a provider user to be provisioned as a user to one or many provider accounts using the same NCID. The user role for each provider account can vary. For example, a provider user may be a primary office administrator for one provider yet a provider enrollment specialist for a different provider.	BR-01-001
PDM-REQ-BO-093	The Solution must revoke access to all providers in which the Office Administrator (OA) is provisioned when directed by the Department or the OA fails background or fingerprint verification. The background check and fingerprint verification can be triggered through an application or monthly monitoring. When available, the secondary OA assumes the role of primary. The Solution must notify the provider(s) and all owners of this event, or others as determined by Business Rules.	BR-01-001
PDM-REQ-BO-094	The Solution must communicate the NCID of the primary office administrator, and secondary office administrator where applicable, to the MES modules using the Office Admin API following application approval. Thereafter, any change to any information managed by the API for an NCID for a provider or providers must also be communicated immediately in accordance with the design of the NCID coarse-grained authorization and SAML flow described in Attachment V: Medicaid Integration Services Core Capabilities.	BR-01-001
PDM-REQ-BO-095	The Solution must allow a transfer of the role of a primary Office Administrator (OA) from one user to another user for one, many or all provider accounts the original OA is provisioned.	BR-01-001

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-096	Under the direction of the State, the Vendor must work with NCDHHS Hearings Office for denial and termination appeals submitted by providers. The Vendor must: · Receive appeals from the NCDHHS Hearing Office · Research the submitted appeal to determine if the adverse decision was proper · Outreach to the provider who submitted the appeal · Create and submit a Summary of Factions and supporting documentation · Attend and represent the State during NCDHHS Hearings · Document provider appeals in the provider's application/record to including attaching all receiving and outgoing correspondence related to the appeal · Update the provider's application/record with the final decision of the appeal The Vendor must provide guidance to DHB for formal denial and termination appeals submitted to the Office or to the Office of Administrative Hearings (OAH).	BR-01-005
PDM-REQ-BO-097	The Vendor must complete one hundred percent (100%) of pre- and post-enrollment onsite screening of moderate and high-risk providers within ten (10) business days according to Agency onsite screening protocols and federal onsite screening regulations, including at a minimum: · Conducting the initial assessment to verify the facility location, hours and personnel; · Verifying operational status; and · Confirming final determination of provider enrollment status.	BR-08-009
PDM-REQ-BO-098	The Vendor must verify the TIN and provider legal name for new enrollment, name and Tax ID changes, revalidation, re-enrollment, and CHOW following department business rules.	BR-08-013

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-BO-099	The Solution must allow the Primary or Secondary OA to add users with limited access to a provider's record per department business rules.	BR-01-001

Table R3. Business Rules Repository

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-BRR-001	The Vendor must have a Solution to configure, support and maintain a business rules repository (e.g., add, modify, or remove/retire rules).	
PDM-REQ-BRR-002	The Vendor must provide real time access to the business rules repository, in an electronic format approved by the State, that documents all business rule logic used by the solution.	
PDM-REQ-BRR-003	The Solution must evaluate the impact of business rules in a testing environment prior to deployment. The Vendor must share the results of business rules testing with the department.	
PDM-REQ-BRR-004	The business rules repository must provide the ability to prioritize, sequence, and must identify the predecessor(s) and successor(s) to identify rules in a chain with access to the historical rules	
PDM-REQ-BRR-005	Where applicable, the business rules repository must use State-defined business rules definitions.	
PDM-REQ-BRR-006	The Vendor must use the Business Rules Repository (BRR) as the source for data input and credentialing, which complies with State and Federal requirements for provider-initiated Change Requests, Enrollment, Re-enrollment or Re-validation processes per State Business Rules.	
PDM-REQ-BRR-007	The Vendor must establish a process or update an existing process for any new primary source of credentialing interface to update a provider's record with new data, as directed by the State within an agreed upon timeframe.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-BRR-008	The Vendor must add a new taxonomy including all associated business rules and exceptions, and end-date or modify criteria for an existing taxonomy, as directed by the State.	
PDM-REQ-BRR-009	The Vendor must create and maintain a business rules repository of requirements applicable to every combination of application classification that the State uses to set provider enrollment requirements. The repository must be informed and approved by the State and maintained by the Vendor. The repository sets a hierarchy of provider classifications (healthcare/non-healthcare, in-state/out-of-state/border, business type, provider type, application type, add-ons, etc.) and establishes criteria for the application process for office administration, required provider information, fees, addresses, NPPES and other external registrations, affiliations, sanctions, care management and other licensing requirements, health plan selection, finance, required attestations and signatures, specialty and supplemental information. The Vendor must work with the State to identify data elements for the Business Rules, referencing the Business Rules Data Elements documentation (the Provider Permissions Matrix PPM, PPMP documentation, the Provider Data Entities and Attributes documentation) any sources provided by the State.	
PDM-REQ-BRR-010	The Vendor must make changes to the business rules repository at the direction of the State of a required change.	

Table R4. Call Center

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-CC-001	The Vendor must establish, operate, and maintain the call center and associated Service Lines.	BR-23-001
MES-REQ-CC-002	Vendor must staff the Call Center and maintain staff at the level agreed upon in the contract.	BR-23-001
MES-REQ-CC-003	The Vendor must submit their agent competency test to the Department for review and approval thirty (30) days prior to the start of the agent training class.	
MES-REQ-CC-004	All service lines must be staffed with agents specifically trained on the requirements, policies and procedures of the North Carolina market and pass an agent competency test with an 85% or greater.	BR-23-001
MES-REQ-CC-005	The Vendor service lines must be accessible via a toll-free telephone line.	
MES-REQ-CC-006	The Vendor must acquire the necessary phone number(s) to support the Call Center requirements within ninety (90) calendar days after Contract Award. · The Vendor must relinquish ownership of the toll-free number(s) upon contract termination or expiration, at which time the Department must take title of these telephone numbers. · All costs accrued, due, and owing on the toll-free numbers, upon termination or expiration of the Contract, including any taxes, penalties or fines must be the sole obligation of the Vendor and must be paid prior to the Department taking title of these telephone numbers.	
MES-REQ-CC-008	The Vendor must provide educational messages or other applicable messages which improve the customer experience (e.g., announcement of new program changes or reminders) while callers are on hold, with the ability to create and make changes as directed or approved by the Department.	
MES-REQ-CC-009	All Vendor service lines must be able to transfer calls via warm transfer to the Department's Fee-for-Service Provider and Medicaid call centers, Enrollment Broker, Ombudsman, county DSS or EBCI PHHS offices, and all participating Health Plans or LME/MCOs when appropriate and without impacting the capacity to handle in-bound calls simultaneously.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-CC-010	The Solution must provide online interactive chat functionality as a reliable transaction channel that allows users to chat directly with a customer care representative.	
MES-REQ-CC-011	The Vendor must use Computer Telephone Integration (CTI) to provide personalized routing and work-object handling based upon identifiers received from the caller regarding inquiry area, ability to produce reports on both electronic and voice transactions.	
MES-REQ-CC-012	The Vendor must provide and maintain secure and user-friendly interactive voice response (IVR) solution with scripts approved by the State to respond to inquiries using a telephone menu and response solution.	
MES-REQ-CC-013	The Vendor's call center solution must include backup and disaster recovery capabilities to limit service disruption and provide for business continuity.	
MES-REQ-CC-014	The Vendor must provide, configure and maintain an automated telephone solution.	
MES-REQ-CC-015	The Vendor must provide a contact tracking system (CRM tool) for all calls and correspondence received.	
MES-REQ-CC-016	Vendor's Call Center staff must document, in the Customer Relationship Management (CRM) system, all the information they provide to callers during first contact and any subsequent follow-ups for example, the caller checking the status of a previous call, an outbound call made by the Vendor, and virtual meetings held with the caller.	
MES-REQ-CC-017	The Vendor's CRM tool must have the ability to provide State resources or designated resources local and remote access to the CRM solution.	
MES-REQ-CC-019	The Vendor must provide assistive listening devices, computer assisted real-time captioning, and qualified sign language interpreters during presentations and other events with audiences.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-CC-021	The Vendor must record and retain all inbound and outbound calls for all service lines and chats for the 12-month retention period. The recordings must capture the entirety of each call, including any hold times, transfers, and interactions with automated systems. The Vendor must implement and maintain a secure solution for the storage and retrieval of call recordings, ensuring compliance with all applicable federal and state laws and regulations regarding data privacy and security, including but not limited to HIPAA and relevant North Carolina General Statutes. The Vendor must provide these recordings to the Department upon request and on a monthly cadence.	
MES-REQ-CC-022	The Vendor must implement and maintain a secure system for the storage and retrieval of call recordings, ensuring compliance with all applicable federal and state laws and regulations regarding data privacy and security. The Vendor must provide these recordings to the Department upon request and on a monthly cadence.	
MES-REQ-CC-023	The Vendor must allow the Department real time remote access via SFTP or API upon request or on an ongoing basis to all call recordings and must provide all call recordings, including video and audio, with the Department having ownership and control of these recordings.	
MES-REQ-CC-024	The Vendor must provide a performance dashboard reporting associated with Call Center correspondence.	
PDM-REQ-CC-025	The Vendor must provide a voice messaging solution for after-hours callers indicating the hours of operation.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-CC-026	The CRM tool must log and track information for each call that includes at a minimum the following elements: · time of call · date of call · identifying information on caller · representative ID · call type · call category · inquiry description, free form text · ticket status · response description · call reference number	
PDM-REQ-CC-027	The Vendor's CRM tool must have the ability to link related CRM tickets.	
PDM-REQ-CC-028	The Vendor's CRM tool must allow users to view related correspondence records from a single correspondence record.	
PDM-REQ-CC-029	The Vendor's CRM tool must have the ability to upload or associate attachments to correspondence records.	
PDM-REQ-CC-030	The Vendor's telephone solution must provide quality monitoring tools and processes to enable a continuous improvement cycle for toll-free call center services that includes: · Plug-in/double-jack monitoring, · Silent monitoring, · Record and review, · Voice and screen/multi-media monitoring, for call center supervisors, State resources or designated resources.	
PDM-REQ-CC-031	The Vendor's call center must operate during Business Days and Business Hours as defined in the RFP.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-CC-032	The Vendor must respond to telephone and written inquiries with a researched response within two (2) business days.	
PDM-REQ-CC-033	The Vendor must provide training to State staff in the use of the Customer Call Center System, initially and on an ongoing basis, as defined by the Department.	
PDM-REQ-CC-034	The Vendor must, if the requestor is not the provider whose eligibility is being requested, require two pieces of the following verification information: NPI, Atypical Provider ID, Address and Phone Number, Provider Name, Primary Email at full credentialing.	
PDM-REQ-CC-035	Vendor must provide sufficient call center staff, accessible from the IVR system, to support the anticipated volume of credentialing and recredentialing applications as reflected in the CVO Plan.	
PDM-REQ-CC-036	The Vendor's call center staff must respond to provider inquiries on provider enrollment processes, data and documentation required, use of the portal, and how to assess status as the application progresses through various stages and all pertinent PDM/CVO processes.	
PDM-REQ-CC-037	The Vendor must thoroughly investigate each Provider complaint using applicable statutory, regulatory and contractual provisions, collecting all pertinent facts from all parties and applying Vendor's written complaint policies and procedures, as approved by the Department. The Department maintains corrective action authority in all instances.	BR-23-002
PDM-REQ-CC-038	The Vendor must allow Providers or Provider's representatives to file a written complaint based on the date of the alleged action, as defined by the Department's Business Rules.	BR-23-002

Table R5. Certification

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-CERT-001	The Solution must comply with the CMS seven conditions and standards.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-CERT-002	The Solution must meet the conditions for enhanced federal funding and other federal regulations required for Centers for Medicare and Medicaid Services certification as defined in Section 7.14.6.	
MES-REQ-CERT-003	The Solution must meet all federal Medicaid Information Technology Architecture (MITA) requirements.	
MES-REQ-CERT-004	The Vendor must provide evidence, including business process mapping, to show how the Solution achieves the state-defined Medicaid Information Technology Architecture (MITA) maturity level AND achieves at least MITA Maturity Level 3.	
MES-REQ-CERT-005	The Vendor must support the Department with CMS Reviews, including but not limited to, planning activities, meetings, presentations, demonstrations, required artifacts, and development of evidence packaging to meet CMS and State-specific outcomes.	
MES-REQ-CERT-006	The Vendor must prepare system documentation for submission to the Department and CMS in a secured location in conjunction with the state for review no later than one month prior to CMS certification milestone reviews.	
MES-REQ-CERT-007	The Vendor must provide the data required for the Intake Form and supporting evidence for CMS reviews. This data must be accessible to the State on an ad-hoc basis through reports in the Solution, the functionality of which can be updated as directed by CMS. When completing the Intake Form, the Department will use the latest template published by CMS at https://cmsgov.github.io/CMCS-DSG-DSS-Certification-Staging/ .	
MES-REQ-CERT-008	The Vendor must enable the development of an Operational Reporting Workbook through a flexible Solution that can be updated as directed by CMS that allows the state to pull the reports as needed for system performance oversight that demonstrates the continuous	

Requirement #	Requirement Description	Business Rules/Application Data Files
	achievement of required and desired outcomes and metrics.	
MES-REQ-CERT-009	The Vendor must participate and support, as needed, the CMS certifications of the other modules.	
PDM-REQ-CERT-010	The Vendor must promptly correct all remediation activities required as a result of certification findings, in accordance with a schedule approved by CMS and the State.	
PDM-REQ-CERT-011	The Vendor must use appropriate testing, configuration and change control procedures for all changes made to the Solution during the CMS certification process.	
PDM-REQ-CERT-012	The Vendor must conduct an Operational Readiness Walkthrough with the Department to validate the operational readiness of the Vendor, the Solution, and the Department. The Department must formally sign off on the Operational Readiness Checklist prior to proceeding to implementation.	
PDM-REQ-CERT-013	The Vendor must allow the Department access to the Solution and data to conduct audits of the Quality Assurance process to ensure enforcement of standards and maintenance of certification.	
PDM-REQ-CERT-014	The Solution(s) must produce transaction data, reports, and performance information that contribute to program evaluation, continuous improvement in Business Operations, and transparency and accountability in accordance with the CMS Standards and Conditions (Reporting Condition) in force during the period of the contract.	

Table R6. Content Management

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-CM-002	The Solution must allow State authorized users to access electronic documents.	BR-21-002
MES-REQ-CM-003	The Solution must support role-based control and access of electronic documents, including the following: a. Granular authorizations for access, preview, editing and sharing. b. Automatic access expirations for documents deemed sensitive by the Department. c. Content security policy enforcement, such as unusual document access activity and sharing of documents with sensitive information of uploads/downloads of prohibitive data.	
MES-REQ-CM-004	The Solution must support all common document types (i.e., Word, PDF, Visio, Excel, PowerPoint, etc.) and integrate with the common document viewing and editing tools used by the Department. (i.e., Microsoft and Adobe products)	
MES-REQ-CM-005	The Solution must store all sent or received electronic documents for future download.	BR-21-002
MES-REQ-CM-006	The Solution must scan all uploaded electronic documents for viruses prior to storage.	
MES-REQ-CM-007	The Solution must include a flexible search capability, including electronic document and content search capabilities.	
MES-REQ-CM-008	The Solution must support integration with scanning Solutions and support for bulk-scanning.	
MES-REQ-CM-009	The Solution must support version control of electronic documents.	
MES-REQ-CM-010	The Solution must support electronic document workflows with review/approval ability with digital signature support (e.g., scan notifications).	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-CM-011	The Solution must be able to index, link and display incoming correspondence or uploaded documentation with the entity record.	BR-21-002
MES-REQ-CM-012	The Solution must allow users to associate metadata with electronic documents.	BR-21-002
PDM-REQ-CM-013	The Vendor must convert electronic documents identified by the Department in a format approved by the Department.	
PDM-REQ-CM-014	Vendor must ensure all incoming documents received and/or other applicable documentation must be scanned into the system within five (5) business days. The Vendor must conduct internal quality checks on the documents scanned.	BR-01-007
PDM-REQ-CM-015	The Solution shall collect and retain electronically all provider documentation (e.g., original application and copies of correspondence) for actively participating providers. For terminated providers, records shall be retained electronically according to record retention requirements (i.e., ten (10) years).	
PDM-REQ-CM-016	The reporting Solution must provide the ability to store system generated reports in the content management solution.	
PDM-REQ-CM-017	The reporting Solution must allow a user to manually save report output to the content management solution.	
PDM-REQ-CM-018	The Vendor must configure, support and maintain a configurable content management and workflow solution that meets the State's requirements.	BR-21-001
PDM-REQ-CM-019	The Vendor must create a complete backup of all historical data migrated from the legacy system into the Solution before any transformations are applied. This backup must reflect the data exactly as received and must be stored in secure object storage in a read-only state.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-CM-020	The Solution must use a Git-based tool for version control for all code artifacts—including notebooks, pipelines, configuration files, and infrastructure definitions, leveraging branching strategies agreed on with the state during DDI phase.	

Table R7. Communications

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-COMM-001	The Solution must provide the ability to create materials for various audiences written between a sixth and eighth grade reading level.	BR-21-001
MES-REQ-COMM-003	The Solution must send documents and the necessary indexing metadata for storage of documents in a content management solution.	
MES-REQ-COMM-004	The Vendor must manage all published communications and must maintain version control to ensure that the original published communication and any published revisions are retained in history.	BR-11-001
MES-REQ-COMM-005	The Vendor must provide a way for the State to directly enter parameter data for communications, automated telephone responses, and letters, including standard paragraphs and messages that may be applied to any particular communication.	BR-21-001

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-COMM-006	The Vendor must configure, support and maintain a correspondence Solution to generate correspondence and coordinate the email, print, and distribution through a State approved print and mail service, using certified mail as defined in the Business Rules.	BR-21-001
MES-REQ-COMM-007	The Vendor's correspondence management Solution must be configurable to allow automatic insertion of variable data into provider communications, including letters, email notifications, Solution-based communications, and other approved correspondence. The Solution must support insertion of names, addresses, specific or aggregated data elements from provider, status, reporting, and State-supplied datasets, as well as approved static text and images.	BR-21-001
PDM-REQ-COMM-008	The Correspondence Management Solution must be able to generate scheduled, ad-hoc, and automatic correspondence to providers, applicants, and other entities (e.g. specific events, license expiration, revalidation, enrollment/disenrollment notices, requests for information, and program information) using standard letters or forms, letter/notification templates, and free-form letters using the Department Business Rules. The Solution must be able to generate correspondence based upon actions taken by the Vendor, the provider, the Department, and as a result of data received on interface files.	JA-002, BR-21-001
PDM-REQ-COMM-009	The Solution must support official approval and denial notifications to the provider. The notification will support consolidated communication for multiple taxonomies, services, locations, and Carolina Access in the case of split approval and denial of provider enrollment service determinations.	BR-21-001, BR-08-024

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-COMM-010	The Vendor must implement, communicate, and apply new or revised policies, outside of the revalidation timeframes as needed, to currently enrolled providers, notifying providers in advance whenever possible.	
PDM-REQ-COMM-011	The Vendor must attend annual and quarterly meetings and provider association meetings when requested by the Department.	BR-11-001
PDM-REQ-COMM-012	Changes to any communication will be completed without additional charge within 5 business days of receipt of approved final copy from the State.	BR-11-001
PDM-REQ-COMM-013	The Vendor must send approval, denial, and termination letters within one (1) State business day of provider participation approval, denial, or termination.	BR-08-011, BR-08-024, BR-11-002
PDM-REQ-COMM-014	The Vendor must date stamp, image, and process all incoming mail based upon department business rules.	BR-01-007
PDM-REQ-COMM-015	The Solution must include an automated process to review returned mail and process based upon department business rules (e.g. suspend providers for bad addresses, terminate for bad addresses).	BR-01-007
PDM-REQ-COMM-016	The Solution must support, track (with date and time of receipt), and monitor communications (e.g., email, SMS, correspondence) to and from providers.	BR-21-001

Table R8. Conversion

Requirement #	Requirement Description	Business Rule
PDM-REQ-CONV-001	The Vendor must collaborate with the Department and the existing Call Center Vendor to optimize and migrate legacy Call Center-related functionality and data to the Vendor's Provider Call Center solution.	
PDM-REQ-CONV-002	The Vendor must perform a conversion of user data requiring a one-time identity management task to verify the user with their NCID account assuming a minimum of 2 users per provider.	

Table R9. Data

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-DATA-001	The Vendor must apply validation and appropriate business rules for all data fields being entered, imported to, and exported from the Solution. The Vendor and the Department must agree on a standard for valid values.	
MES-REQ-DATA-002	The Solution must have a means to deal with data received from other sources that fall outside of the validations: to reject a file or record based on business rule validations, or accept the data but report an error, or a combination of these means as approved by the Department.	
MES-REQ-DATA-003	The Solution must facilitate data processing including data cleansing, data loading, data brokerage, integration, validation, reconciliation, and synchronization with the MES.	
MES-REQ-DATA-004	The Solution must capture and maintain the data needed for applicable State or Federal reporting requirements	
MES-REQ-DATA-005	The Solution must provide the ability to import/export data in generally accepted formats.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-DATA-006	The Vendor must provide access to archived data to the Department within 48 hours of request.	
MES-REQ-DATA-007	The Vendor must ensure that 99% of all data being converted is correctly mapped as defined in the Data Migration Plan.	
MES-REQ-DATA-008	The Vendor must perform one or more trial conversions as necessary prior to System Integration Testing (SIT), User Acceptance Testing (UAT), and the final conversion, and present the results to the State for review and approval.	
MES-REQ-DATA-009	The Vendor must convert all applicable operational provider data for any provider that has been active/suspended within the past ten (10) years. This includes all current data plus all historical data that is expired or no longer active for the provider. All data for providers terminated within the past 10 years must also be converted.	
MES-REQ-DATA-010	The Vendor must provide Department designated staff access to an environment to provide support or validate converted data.	
MES-REQ-DATA-011	The Vendor must participate in ongoing data governance meetings and processes as required by the Department.	
MES-REQ-DATA-012	The Solution must maintain its own reference data. This includes ongoing management, validation, and updating reference data within the Solution.	
MES-REQ-DATA-013	The Solution must consume the reference data from the State designated systems of record and enforce its consistent use across all business domains.	
MES-REQ-DATA-014	The Solution must not maintain independent or conflicting versions of the State designated system reference data and must remain aligned with the systems of record.	
MES-REQ-DATA-015	The Solution must provide all its reference data to other State systems via the Medicaid Integration Services (MIS).	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-DATA-016	The Solution must expose data lineage metadata to third-party open source and off the shelf metadata governance tools (e.g., OpenLineage, Amundsen, OpenMetadata).	
MES-REQ-DATA-017	The Solution must expose canonical business definitions and calculation logic for metrics that are published as Single Version of Truth to the third-party open source and off the shelf metadata data catalog/governance tools.	
MES-REQ-DATA-018	The Solution's data must align with data classification standards as mutually agreed upon by the State and Vendor to ensure that appropriate controls are applied to each category of data before it is accessed or used.	
MES-REQ-DATA-019	The Vendor must identify the specific data elements required for inclusion in the Operational Data Store (ODS) and subsequently support the development of appropriate file extracts and/or API integrations to enable data transfer.	
MES-REQ-DATA-020	All current and historical data, including electronically imaged documents for records (providers, members, cases, etc.) for any entity or case that has been active within the last ten (10) years must be retained by the Solution following implementation. For data and documents for entity or case records inactive ten (10) years or greater may be purged only with the Department's written approval, and in accordance with applicable federal and state data policies. Historical data and documents for active entity or case records may only be purged with the Department's written approval, and in accordance with applicable federal and state data policies	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-DATA-021	The Vendor must develop and maintain a process to archive and access archived data (including legacy MMIS component data).	
MES-REQ-DATA-022	The Vendor is responsible for backups and the retention of backups to include: · Daily incremental backups with retention of ninety (90) days. · Weekly incremental backups with retention of twelve (12) weeks. · Monthly full backups with retention of eighteen (18) months. · Annual full backups with retention of ten (10) years.	
MES-REQ-DATA-023	The Vendor must maintain an automated audit trail of all update transactions, both batch and online, including date and time of change, before and after data field contents, and operator identifier or source of the update.	
PDM-REQ-DATA-024	The Vendor must work with the State to identify the data elements that will be converted into the Solution, including data where there is not data mapping in the Solution. For legacy data elements that cannot be converted into the Solution, the Vendor must work with the State to achieve desired business outcomes using the data elements in the Solution. The Vendor must work with the State to define conversion rules achieving desired business outcomes by identifying and defining rules for: · Data elements that will be converted into the Solution · Data elements or fields in the Solution that are not available to be converted from the legacy system, and whether the conversion programs should fill them with default or initial values · Legacy data elements that cannot be converted into the Solution	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-DATA-025	The Solution must provide a configurable workflow process for resolving near matches for providers that can link, void or end date extraneous records (i.e., duplicate provider records) and manage a cross reference to historical provider identification as determined by the Department.	BR-13-006
PDM-REQ-DATA-026	The Solution must provide the ability to store and apply updates to all applicable codes upon new release at an interval appropriate for the data or when requested by the Department.	
PDM-REQ-DATA-027	The Solution must have the ability to void or reverse data changes by rolling back to prior configurations.	
PDM-REQ-DATA-028	The Solution must provide a flexible search capability for all state authorized users including the ability to search by entity type, entity name, entity address elements, entity phone number(s), unique identifier for entity type, any alternate identifiers including EIN, SSN, TIN and any elements defined by the Department.	
PDM-REQ-DATA-029	The Solution must be configured and maintained to validate and standardize addresses in real-time during enrollment, re-enrollment, revalidation, or provider-initiated change process (add or change address) according to United States Postal Service (USPS) validation and standardization rules. When a physical address cannot be validated at initial enrollment, the Vendor's Solution must provide a means for a provider to self-confirm their address with an indication, visible to all system users, that the address has not been validated. The Vendor's Solution shall continue attempting validation for any self-confirmed address during revalidation and/or each provider-initiated change process until the address is successfully validated.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-DATA-030	The Solution must provide, at minimum, ten (10) years of operational data accessible for queries, report generation and online views. Operational data needed beyond ten (10) years that is archived must be accessible within twenty-four (24) hours. Operational data and archive data is the data necessary to maintain the provider's eligibility and participation in managed care programs as defined in the data model.	
PDM-REQ-DATA-031	While the Department prefers real-time/event driven processes, the Vendor must provide a tool to easily administer and execute scheduled events (e.g. reports, file transfers, processes, notifications) to be performed on a regular basis (e.g. daily, weekly, monthly).	
PDM-REQ-DATA-032	The Solution must maintain online access to reports for the life of the contract.	
PDM-REQ-DATA-033	The Solution must assign standardized unique internal identifiers for all entities to use as a secondary identifier for internal system processing.	
PDM-REQ-DATA-034	The Solution must maintain online access to all reference tables with an option to search and display by reference data type and code.	
PDM-REQ-DATA-035	The Solution must allow the enrollment of one or multiple locations, to include specifying servicing counties for each location, on a single application.	BR-08-021, APP-01, APP-02, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12, APP-13
PDM-REQ-DATA-036	The Solution must support retrieval and presentation of data associated with geographic indicators such as state, by county, by zip code, by peer group, or other geographical indicators specified by the Agency.	

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-DATA-037	The Solution must generate and maintain a locator code associated with every location where the locator code represents a unique address for the provider. Locator codes assigned must be sequential and cannot be duplicated for an NPI. If the address for a given locator code becomes inactive for the provider, the locator code cannot be used for another location address. In the event a duplicate address is found, the Solution must facilitate the provider through an address merge to reduce keystrokes when merging appropriate location data from one locator code to the other such as office hours or preventative ancillary services. The Vendor must also allow the ability to reinstate an end dated location.	
PDM-REQ-DATA-038	The Solution must carry over the Legacy NCTracks Locator code field to PDM/CVO during conversion for the purpose of continued use as described in PDM-REQ-DATA-037.	
PDM-REQ-DATA-039	The Solution must ensure that all physical locations entered on an application are not a PO Box, a Commercial Receiving Agency, a Virtual Mailbox, a Virtual Address, or a Private Mailbox (PMB), not a PO Box. The correspondence and/or financial address may be a physical address or a non-physical address. Any address entered on an application must be validated by the Vendor's Solution according to related address validation requirements.	
PDM-REQ-DATA-040	The Solution must allow the provider to select and modify their primary location from their approved locations.	APP-13, APP-04, APP-03, APP-02, APP-11, PIC-01

Requirement #	Requirement Description	Business Rule/Application Data Files
PDM-REQ-DATA-041	The Solution must allow an individual provider the ability to enroll as a rendering/attending only, sole proprietor or a combination where all locations are defined by the provider's billing affiliations. The sole proprietor must declare the locations in which the provider will operate as a sole proprietor and allow the provider to maintain billing affiliations. This includes when the provider changes their business structure from sole proprietor to rendering only and vice versa.	APP-12, APP-05, APP-04
PDM-REQ-DATA-042	The Solution must not allow providers the ability to edit an existing address for a location, thereby forcing the provider to instead create a new location.	PIC-01
PDM-REQ-DATA-043	The Solution must automatically generate, store, and display a geocode for each location using a reliable geocoding service. For providers who use servicing county, the Solution must provide a geographical way to specify the service area such as through the use of centroid geocoding or boundary mapping.	
PDM-REQ-DATA-044	The Solution must have the ability to automatically exclude providers from the provider directory and to allow providers to elect to be included or not in the provider directory, per business rules.	BR-09-001
PDM-REQ-DATA-045	The Solution shall provide real-time access to transactional data for all module components.	

Table R10. Integration

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-INT-001	The Solution must interface through Medicaid Integration Services (MIS) using APIs for real-time and secure file transfer for batch data exchanges.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-INT-002	The Solution must integrate with other MES modules as needed utilizing Medicaid Integration Services (MIS) via batch or real-time data exchanges.	
MES-REQ-INT-003	The Solution must send and receive real-time discrete transactions between modules and other entities designated by the Department through the State's Medicaid Integration Services (MIS) integration platform, where necessary, using the provided standards and protocols to reduce the need for bulk data transfers and duplicate communications. Direct data entry into the Vendor's web Solution is exempt.	
MES-REQ-INT-004	The Vendor must identify and provide all tools and software intended to maintain interfaces, code, versions, environments, and data models as a component of its Information Systems Development Methodology (ISDM).	
MES-REQ-INT-005	The Vendor must provide inbound and outbound interface raw data files when requested by the State on a mutually agreed timeline.	
MES-REQ-INT-006	The Solution must provide the functionality to access raw daily interface files for up to sixty (60) calendar days. Archive raw daily interface files after sixty (60) calendar days and maintain for up to six (6) months.	
MES-REQ-INT-007	The Solution must provide the ability to access raw weekly, monthly, and quarterly interface files for up to one year (365 calendar days). Archive raw monthly and quarterly interface files for two years (730 calendar days) and maintain for up to two (2) years.	

Table R11. Provider Maintenance

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-PMAIN-001	The Vendor must a) add or remove a taxonomy on the provider's record or b) change the providers risk level on the provider's record or c) add additional licensure, accreditation, or certification on the provider's record, as directed by the State.	BR-06-001
PDM-REQ-PMAIN-002	The Vendor must make exceptions to established business rules that require manual intervention, as directed by the State.	
PDM-REQ-PMAIN-003	The Solution must identify providers who are under review or investigation as identified by the State. These providers may be excluded from manual and automated suspension and termination processes as defined by department business rules.	BR-13-005, BR-22-001, BR-06-010
PDM-REQ-PMAIN-004	The Solution must require, capture and maintain the 10-digit National Provider Identifier (NPI) for all healthcare providers required to have an NPI.	BR-08-001, APP-01, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-11, APP-12
PDM-REQ-PMAIN-005	The Solution must provide the functionality to: · Collect, store, maintain, and display provider ownership data by tax identification number (TIN) · View real-time and via standard reporting all provider records associated with a TIN	
PDM-REQ-PMAIN-006	The Solution shall allow for the collection, storage, and maintenance of information related to site visit, training, fingerprinting, background, and all other required credentialing checks. The information shall be displayed to state-authorized users.	
PDM-REQ-PMAIN-007	The Solution must reactivate terminated providers within twenty-four (24) hours without requiring a complete re-enrollment, as directed by the Department.	
PDM-REQ-PMAIN-008	The Solution must accept, validate and store new and updated provider information entered by state-authorized users.	BR-08-028
PDM-REQ-PMAIN-009	The Solution will collect, store, maintain, display, and provide reporting on provider business relationships (e.g., ownerships, subVendors, and managing entities).	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-PMAIN-010	The Solution must capture subpart NPIs.	BR-08-012
PDM-REQ-PMAIN-011	The Solution must collect, validate, verify, and maintain Clinical Laboratory Improvement Amendments (CLIA) certification information for all active and suspended providers including the level of certification, the specific procedures each laboratory is authorized to perform, effective and end dates, and location of the certification for use in claims adjudication.	BR-08-007
PDM-REQ-PMAIN-012	The Solution must identify providers who are suspended, a method for indicating the reason for the suspension, and historical information on suspension to include dates and reason(s).	BR-11-003
PDM-REQ-PMAIN-013	The Solution must have the ability to suspend the provider record for providers that fail to respond to requests per State Business Rules and in compliance with all federal and State policies and regulations.	BR-01-007, BR-06-010, BR-08-010, BR-11-003, BR-22-001
PDM-REQ-PMAIN-014	The Solution must allow for mass updates to provider status based on criteria defined by the department (e.g., group practice changes) and initiate notification to the providers and appropriate programs.	BR-01-003
PDM-REQ-PMAIN-015	The Solution must have the ability to end date provider participation in specific programs while maintaining participation in other programs and initiate notification(s) to the provider, agency staff, and modules.	BR-11-002
PDM-REQ-PMAIN-016	The Solution must require and capture reasons for all provider terminations and denials.	BR-11-002, BR-08-011, PIC-01
PDM-REQ-PMAIN-017	The Solution must have the ability to assign classifications (e.g., provider type and specialty) to all providers including atypical providers, that fall within the scope of their practice.	APP-01, APP-02, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12, APP-13

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-PMAIN-018	The Solution must provide application workflows to collect enrollment and maintenance data from the provider that is conditional to and configurable by provider entity type (e.g., individual, organization), provider role (e.g., Ordering, Prescribing or Referring (OPR), Medicare Lite, rendering, attending, managed care health plan) and provider classification (e.g., case manager, physician, home health agency) following business rules established by the respective NCDHHS agencies. This includes workflows accommodating atypical providers and entities enrolling or registering without a taxonomy as well as traditional healthcare providers with taxonomy codes.	BR-08-002, BR-08-018, BR-08-020, BR-08-25, JA-001, APP-13, APP-12, APP-11, APP-09, APP-10, APP-08, APP-07, APP-06, APP-05, APP-04, APP-02, APP-03, PIC-01
PDM-REQ-PMAIN-019	The Solution must support the ability to compare provider information (ownership, screening/site visit, federal fee, fingerprinting, Medicare Lite/Disaster Relief/Out-of-State enrollment) with Provider Enrollment, Chain, and Ownership System (PECOS) if the provider is enrolled with Medicare, in accordance with State Business Rules.	BR-06-001, BR-06-007, BR-08-003, BR-08-004, BR-08-015, BR-08-020, BR-08-025
PDM-REQ-PMAIN-020	The Solution must provide an application workflow to collect information from the provider based on the provider's entity type, role, application type and provider classification configurable following business rules for health care providers as well as atypical entities necessary for supporting NCDHHS agencies.	APP-01, APP-02, APP-03, APP-04, APP-05, APP-06, APP-07, APP-08, APP-09, APP-10, APP-11, APP-12, APP-13
PDM-REQ-PMAIN-021	The Solution must have configurable workflow to present for validation, updates submitted online/electronically by specific criteria (e.g., program type, data type, risk level).	
PDM-REQ-PMAIN-022	The Solution must support manual and automatic classification of a provider risk level status (limited to moderate to high) which must trigger additional steps and screening as applicable. The Vendor must notify the provider within five (5) calendar days when the provider's list level has been adjusted.	BR-06-001, BR06-014

Table R12. Operations and Maintenance

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-OM-001	The Vendor must perform operations and maintenance on all solution environments (i.e. production and pre-production environments), following change control, defect management, configuration management, release management, and testing processes that are approved by the Department.	
MES-REQ-OM-002	The Vendor must provide comprehensive system maintenance which will include, at a minimum: service changes, system upgrades, correction of deficiencies, performance enhancements, script changes, system parameters, configuration changes, patching, and other activities required to meet the solution operations requirements.	
MES-REQ-OM-004	Vendor must request any planned Downtime due to scheduled upgrades or Maintenance, outside the normal Maintenance Window, to the Department 5 Business Days prior to Downtime. Unless the Department consents, it does not qualify as approved Downtime.	
MES-REQ-OM-005	The Vendor must submit its notice within ninety (90) days of any system upgrades, new versions of product, or new APIs, to the Department for approval. The Vendor must provide an impact analysis to the Department on how the changes or upgrades will impact the operation and functionality of the Solution and provide the documented testing results.	
MES-REQ-OM-006	The Vendor must provide solution configuration changes to the Department for approval prior to deployment. The Department reserves the right to request changes to the proposed configuration changes.	
MES-REQ-OM-007	The Vendor must include documentation of solution components and procedures such that the solution could be operated by a variety of Vendors or other users.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-OM-008	Vendor must maintain Solution documentation to include configuration, system design, enterprise architecture, user manual, operations procedures manual, training manual, and data dictionary within 10 business days of an implementation change to the Solution.	
MES-REQ-OM-009	The Vendor must comply with the Department's reporting and resolution timelines for standard production incident and problem turnaround times as outlined in the Bidder's Library.	
MES-REQ-OM-010	Vendor must provide initial recommended production issue severity and incident priority levels that address both the business impact and business urgency. Production issues will be categorized based on the Department's urgency, severity, and priority definitions. The Department reserves the right to elevate the Vendor's recommendations.	
MES-REQ-OM-011	The Vendor must utilize and report into the IT Service Management tool that is designated by the Department to track all Incidents, Problems and Changes (including Service Requests).	
MES-REQ-OM-012	The Vendor must resolve all service defects and service disruptions. Defects are not considered resolved until approved by the State.	
MES-REQ-OM-013	The Vendor must collect, prioritize, manage, and report on all defects and must include defect aging information to track how long defects are taking to resolve throughout the Software Development Lifecycle.	
MES-REQ-OM-014	The Vendor must provide a report for all Critical and High-Level incidents, as defined in RFP Section 3.3.3 Vulnerability Risk Ratings and Remediation, on a monthly basis for the previous month and must provide a Root Cause Analysis for each of the Critical and High-Level incidents.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-OM-015	The Vendor must report metadata on the status of all interfaces as defined by Tech Ops procedures to the department, on a daily basis, unless otherwise defined. Tech Ops provides processes related to the submission of this information.	
MES-REQ-OM-016	The Vendor must provide authorized users access to all environments as required for transition activities and throughout the lifecycle of the contract.	
MES-REQ-OM-017	Vendor must ensure maintenance of licenses and appropriate permitted usage with all licensing agreements, including software licensing, to support the proposed Solution and services.	
MES-REQ-OM-018	The Vendor must provide licenses to the Solution as required by the Department to allow users access to perform all necessary business functions.	
MES-REQ-OM-020	The Vendor must transition all licenses, services, and accounts procured for the solution to the State in the event of a transition.	
MES-REQ-OM-021	All transfers of software licenses and subscriptions must be completed 4 weeks after the notification of transfers as provided by NCDHHS to the Vendor.	
PDM-REQ-OM-022	The Vendor must provide labor for Necessary System Change (NSC) for the duration of the DDI phase of the contract. The cost of this annual not to exceed cost for the effort related to NSC are included in the Offeror's fixed price and included in Attachment E Cost Form. The NSC hours include personnel cost for all staff supporting the system enhancement effort.	
PDM-REQ-OM-023	The Vendor will provide labor for Necessary System Change (NSC) during the Operations phase per operations year. The cost of this annual not to exceed cost for the effort related to NSC are included in the Offeror's fixed price and included in Attachment E Cost	

Requirement #	Requirement Description	Business Rule/Application Data Files
	Form. The NSC hours include personnel cost for all staff supporting the system enhancement effort.	
PDM-REQ-OM-024	The Vendor must submit a monthly Necessary System Changes report that details tickets invoiced and must include funds used and funds remaining for the Department's approval.	
PDM-REQ-OM-025	In the event of Contract transfer or termination, the Vendor must provide transition assistance in the migration of the cloud-based PDM/CVO solution from the Vendor provided cloud environment to a State provided cloud environment. Such assistance must include a complete transfer of all solution assets such as source code, configuration details, data pipelines, transformation logic, any new models and reports, documentation, IaC scripts, code repository assets, and all data in usable formats.	

Table R13. Project Management

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-PM-001	The Vendor must participate in key project/program milestones such as: System Integration Testing (SIT), User Acceptance Testing (UAT) Sign-Off, End to End Testing (E2E), Operational Readiness Review (ORR), and Go-Live.	
MES-REQ-PM-002	The Vendor must coordinate module milestone walkthroughs and participate in other module walkthroughs as required by the Department.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-PM-003	The Vendor must provide a written acknowledgment of any potential compliance issues formally communicated by the Department, its Vendors, or other stakeholders. Formal communication must be submitted through documented channels such as email or official correspondence. The Vendor's acknowledgment must be submitted to the Contract Administrator within two (2) business days of receiving the formal notification.	
MES-REQ-PM-004	The Vendor is responsible for obtaining licenses, services, and accounts required by any local, State, or Federal entities for the project and maintaining them throughout the duration of the contract.	
MES-REQ-PM-005	The Vendor must conduct a weekly status meeting to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and service level agreements), utilizing the Department-provided status deck template.	
MES-REQ-PM-006	The Vendor must organize and participate in project-related meetings with the Department as required by the Department.	
MES-REQ-PM-007	The Vendor must distribute meeting agendas to invitees at least one business day before the start of a scheduled meeting involving project stakeholders. Scheduled meetings include any reoccurring project meetings; meetings identified in the Work Plan or any meeting requested by the Department with at least two (2) business days' notice. Vendor must distribute meeting minutes to meeting attendees within two business days of the scheduled meeting.	
MES-REQ-PM-008	The Vendor must follow the Department processes and tools for the escalation of risks, issues and decisions during the project implementation and operations phases.	
MES-REQ-PM-009	The Vendor must include a risk mitigation strategy for all risks and issues identified during the projects' implementation and operations.	

Requirement #	Requirement Description	Business Rule/Application Data Files
MES-REQ-PM-010	The Vendor must draft and execute Department approved mitigation strategies for logged project risks and issues, within defined timeframes, throughout the project lifecycle. These plans must be maintained and monitored until risk/issue closure. The Vendor also must participate in the development and execution of risk/issue mitigation strategies owned by the Department.	
MES-REQ-PM-011	The Vendor must include the following in risk/issue mitigation strategies: · Risk Assessment: An evaluation of the likelihood and impact of each identified risk. · Mitigation Strategies: Specific strategies and actions the Vendor is taking to resolve/close identified risks, including contingency plans. The Vendor must also include their plans for monitoring progress. · Timeline: when the Vendor expects certain mitigation activities occur and when the risk/issue overall is expected to be resolved.	
MES-REQ-PM-012	The Vendor must manage requirements and demonstrate requirements traceability throughout the life of the contract, to include providing product demonstrations, sprint reviews (post-development/configuration reviews), and Requirement Traceability Matrix (RTM) maintenance, to support project implementation, operations, certifications, contract close out, and audits.	
MES-REQ-PM-013	The Vendor must provide the Department with 24x7, real-time, view-only access to their RTM tool and export its contents upon request in an excel/CSV.	
MES-REQ-PM-015	The Vendor must provide a Deliverable Expectation Document (DED) for deliverables as requested by the Department, using the Department's preferred template as applicable.	
PDM-REQ-PM-016	The Vendor must work with the State to finalize the design of the credentialing and enrollment process. This must include but not be limited to: · Collaborating to agree upon a single set of data elements to be credentialed for each provider type. This collaboration	

Requirement #	Requirement Description	Business Rule/Application Data Files
	may be done in phases of provider types. The State desires that the credentialing and enrollment platform will be rolled out by provider type, beginning with managed care providers. · Collaborating to agree upon a standard format for the Primary Source Verification (PSV) files · Collaborating to agree upon any needed customization or configuration of the credentialing platform software · Collaborating to agree upon standard provider communications regarding credentialing · Collaborating to agree upon standard reports, their contents and frequency · Collaborating with the State to ensure the enrollment function meets State and Federal requirements	
PDM-REQ-PM-017	The Solution must manage multiple payers for multiple state agencies and departments. Each entity may have different eligibility and enrollment requirements, different workflows, different security profiles, and different reporting requirements.	
PDM-REQ-PM-018	The Vendor must work with the Department to confirm the Vendor's understanding of the requirements and to clarify and/or elaborate requirements where necessary to achieve desired business outcomes.	

Table R14. Reporting

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-REP-001	The Vendor must ensure that all narrative descriptions of codes and abbreviations are available for reporting.	
PDM-REQ-REP-002	The Vendor must ensure complete transparency of all data fields in reports generated by the solution including providing the Department with SQL, pseudo code, narrative description, analytic protocols and assumptions to document the logic and formulas used in all calculations.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-REP-003	The Vendor must provide summary and detailed level Operational Performance Reports delivered to the Department, at agreed upon intervals, pertaining to provider enrollment, disenrollment, termination, re-enrollment, revalidation, recertification, provider-initiated change request and credentialing status as well as Service Level Agreements (SLAs) and other provider maintenance and credentialing activities as specified.	
PDM-REQ-REP-004	The Solution must include a query tool that allows all state-authorized users to easily query data necessary to support state healthcare programs business needs. This includes all in-flight, historical, and source data from all tables used for all provider enrollment and credentialing.	
PDM-REQ-REP-005	The Solution must have the ability for all State-authorized users to selectively retrieve, view, export, and print reports (or portions of reports).	
PDM-REQ-REP-006	The Vendor must update dashboards in real-time or on a schedule approved by the State.	
PDM-REQ-REP-007	The Solution must provide an established library of standardized operational reports as well as the ability to create a wide array of configurable detail level and summary level reports, dashboards and queries. This includes all in-flight and source data from all tables used for all provider enrollment and credentialing.	
PDM-REQ-REP-008	The reporting Solution must support initiation of reports through various methods including on-demand, scheduled requests (including non-business hours), and event-driven requests with distribution of the report results to specified secure locations.	
PDM-REQ-REP-009	The reporting Solution must display standard report header and footer information (e.g., report number, report title, page number, date) on all reports.	

Table R15. Security

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-001	The Vendor and its subcontractors must comply with the Federal, State and Department Security Policies and Standards.	
MES-REQ-SEC-002	The Vendor must provide weekly status updates for each Corrective Action Plan (CAP) until the CAP is complete and the finding is remediated in accordance with the State IT Security Policies.	
MES-REQ-SEC-003	The Vendor must implement the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks.	
MES-REQ-SEC-004	The Solution must ensure that all data exchanges including inbound and outbound interfaces must comply with industry standards where applicable (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), HIPAA-compliance standards, Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR)).	
MES-REQ-SEC-005	The Solution's services and infrastructure must adhere to best practices and use open security standards and frameworks, such as: · Policy: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL) · Federation: WS-Secure Conversation, WS-Federation, WS-Authorization, XML Key Management (XKMS) · Mechanism: Extensible Access Control Markup Language (XACML), XML Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML), X.509 certificates	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-006	The Vendor must implement the risk management framework in compliance with the NIST Risk Management Framework or equivalent.	
MES-REQ-SEC-007	The Vendor must implement the Web Application Firewall (WAF) to mitigate the application security vulnerabilities such as OWASP TOP 10.	
MES-REQ-SEC-008	The Vendor must run weekly vulnerability scans on all Vendor and subVendor networks and systems that will access or host State data and information.	
MES-REQ-SEC-009	The Vendor must implement encryption for data in transit and data at rest using FIPS 140-2 or FIPS 140-3 compliant crypto material.	
MES-REQ-SEC-010	The Vendor must ensure encryption of email transmissions, including attachments, that contain sensitive and confidential information.	BR-11-001
MES-REQ-SEC-011	The Vendor must make its facilities reasonably available for inspection by NCDHHS PSO security staff, or a third party acting on NCDHHS's behalf when requested.	
MES-REQ-SEC-012	The Vendor must comply with privacy and security related assessments or audits conducted by NCDHHS, the State of NC, and Federal, including security audits, third party security assessments, and annual audits.	
MES-REQ-SEC-013	The Vendor must perform internal risk assessment annually and share the assessment findings and corresponding CMS Information Security Program Plan of Action and Milestones (POA&M) / Corrective Action Plans (CAPS) with the Department.	
MES-REQ-SEC-014	The Vendor must cooperate fully and completely with all Quality Assurance audits, evaluations, studies, investigations, surveys, reviews, and findings conducted by the Department, State, Centers for Medicare and Medicaid Services, or other auditing entities	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-015	The Vendor and its subcontractors must provide access (network connectivity and system credentials) for Department, Federal, and State auditors, including the execution of outside audit tools and audit test software for auditors from the U.S. Department of Health and Human Services (HHS) Office of the Inspector General, the State of NC or NCDHHS Internal Audit, or any other authorized auditors as determined by Department.	
MES-REQ-SEC-016	The Vendor must remediate findings from security audits and assessments as per the guidelines described in the State Security Policies and must adapt to evolving controls as standards change.	
MES-REQ-SEC-017	Audit logs must be maintained online, behind a front-end presentation toolset that is accessible by the Department (or Department authorized users) and provides queries, reports and analytics on any log, in support of typical control questions required by the latest NIST 800-53.	
MES-REQ-SEC-018	The Solution must integrate audit logs with enterprise Security Information Event Management (SIEM).	
MES-REQ-SEC-019	The Vendor must produce and maintain for ten (10) years, robust audit trails and audit logs of all applications and engineering activities (including inquiry transactions) on the environments wherever the production data is accessible.	
MES-REQ-SEC-020	The Vendor must retain all records, electronic documents, and reports relating to this Contract for a period of ten (10) years after final payment is made under this Contract. When an audit, litigation, or other action involving or requiring access to records is initiated prior to the end of said period, records must be maintained for a period of ten (10) years following resolution of such action or longer if such action is still ongoing.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-021	The Solution must retain all Solution data, logs, correspondence, and reports of the past 180 calendar days of activity. Access to this data should be online, secure, and readily available to authorized State personnel during this period.	
MES-REQ-SEC-022	The Vendor must conduct a Business Impact Analysis (BIA) to identify hierarchy of critical services and infrastructure to determine the order that services will be restored for developing the detailed Business Continuity and Contingency Plan (BCP) and Disaster Recovery Plan (DRP).	
MES-REQ-SEC-023	The Vendor must coordinate disaster recovery activities with the Department, application business owner, system owner and division Business Continuity Plan Coordinator.	
MES-REQ-SEC-024	The Vendor must restore the Solution availability, in the event of unscheduled downtime, following the protocols and timing provided in the Disaster Recovery Plan.	
MES-REQ-SEC-025	As part of Go-Live/Operational Readiness Review, the Vendor must execute a disaster recovery test and provide testing results (After Action Report) to the Department that demonstrates the ability to recover the Solution in accordance with the Disaster recovery Plan and in support of all Service Level Agreements.	
MES-REQ-SEC-026	The Vendor must perform Disaster Recovery testing each year. In the event the Vendor's test is deemed by the Department to be unsuccessful, the Vendor must resolve the identified issues and continue to perform the test, at the Vendor's expense, until satisfactory results are received and approved by the Department.	
MES-REQ-SEC-027	The Vendor must submit an After-Action Report that includes the Disaster Recovery (DR) testing results and issues experienced during DR testing.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-028	The Vendor must obtain approval from the Department's Privacy and Security Office before storing or processing production data in lower environments such as development, test, User Acceptance Testing (UAT), and End-to-End testing (E2E).	
MES-REQ-SEC-029	The Vendor must incorporate Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) in their SDLC.	
MES-REQ-SEC-030	The Vendor must incorporate Interactive Application Security Testing (IAST) and Runtime Application Self Protection (RASP) techniques to improve the security posture of the application.	
MES-REQ-SEC-031	The Vendor must provide the necessary access to the systems and required support to the Department or its authorized contractors to conduct an annual third-party privacy and security assessment including Whitebox penetration testing.	
MES-REQ-SEC-032	The Vendor must provide the necessary access to the systems and required support to the Department or its authorized contractors to conduct third-party privacy and security assessments including Whitebox penetration testing for Operational Readiness Review (ORR).	
MES-REQ-SEC-033	The Vendor must conduct annual independent third-party penetration testing and submit the test results and reports to the Department.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-034	The Vendor must maintain dedicated test environments adequate to support multiple testing workstreams concurrently, for example multiple concurrent cycles of internal testing and End-to-End testing (E2E). In addition, for the E2E environment and testing specifically, the Vendor must maintain a test environment provisioned with the same privacy and security controls that are required by the Federal, State, and Department privacy and security requirements. As part of E2E testing, this environment must support and secure production data including production volumes.	
MES-REQ-SEC-035	The Vendor must maintain or otherwise arrange for a disaster recovery site for its system operations in the event of a disaster that renders the production site inoperable.	
MES-REQ-SEC-036	The Vendor must provide a disaster recovery (DR) site that is geographically separated from the primary site by at least 100 miles and not reliant on the same power or network utilities.	
MES-REQ-SEC-037	The Vendor must provide back-up processing capability at a DR site such that normal processing can continue in the event of a disaster or major hardware problem at the primary site. All operations at the remote back-up (DR) site must meet established contractual performance and SLA requirements.	
MES-REQ-SEC-038	In the event the Solution's production environment becomes unavailable due to a disaster, the Vendor must move operations to the disaster recovery site and remain operational at the disaster recovery site until the Department approves a return to normal operations.	
MES-REQ-SEC-039	The Vendor must determine when the primary production site is inoperable due to a disaster and execute the Disaster Recovery Plan.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SEC-040	The Vendor Solution must integrate identity and access management with NCID and support one of the following protocols: · Security Assertion Markup Language (SAML v2) · OAuth/OIDC	
MES-REQ-SEC-041	The Vendor Solution must leverage Multi-Factor Authentication (MFA) provided by NCID when logging into the module system applications.	
MES-REQ-SEC-042	The Vendor Solution must provide links to users of the State MFA documentation and guidance for installing MFA options to work with NCID.	
MES-REQ-SEC-043	The Vendor must review privileged access accounts with the Department and provide the summary report on a quarterly basis.	
MES-REQ-SEC-044	The Vendor must provide at least two Department individuals with administrative accounts to provide continuity of operations.	
MES-REQ-SEC-045	The Vendor must provide the ability to have different access levels using role-based access controls. The access levels must be configurable by the Vendor.	
MES-REQ-SEC-046	The Vendor must certify that all Confidential (PHI/PII) and sensitive Department data will reside in data centers located in the continental United States. Additionally, this data will only be accessible by resources within the continental United States that have completed the necessary HIPAA and Security Awareness training.	
MES-REQ-SEC-047	The Solution's disaster recovery environment must fully support production-level availability, capacity, and capabilities while maintaining adherence to all contract SLAs.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-SEC-048	The Solution must provide audit trail of changes made by a user or Solution initiated to allow information on all transactions to be traced from receipt of the transaction through the completion of the transaction, capture at a minimum date/timestamp, data source, user, action taken, and log any errors encountered for reporting. This includes changes that were made in error and subsequently backed out.	
PDM-REQ-SEC-049	The Solution must maintain a history of provider information (i.e., full audit history or equivalent capabilities). All transactions, including the execution of database scripts, before and after values, need to be recorded in the full audit history.	
PDM-REQ-SEC-050	The Vendor must ensure all hardware, software, and communication components installed for use by State staff are compatible with the State currently supported versions of the Products and current technologies for data interchange.	
PDM-REQ-SEC-051	The Vendor must not collect or use information from the providers not authorized by the State.	
PDM-REQ-SEC-052	The Solution must provide the capability for managing provider ids, including the capability to capture, identify, and report suspected duplicate provider identifiers, to update records to reflect changes such as merging or decoupling of provider IDs, and to maintain a cross-reference to historical provider identifications as defined by the Department.	BR-13-001, BR-13-006. BR-13-003
PDM-REQ-SEC-053	The Vendor must limit access to fingerprinting negative findings/results to users authorized by the North Carolina State Bureau of Investigation (NC SBI).	BR-07-007
PDM-REQ-SEC-054	The Solution must allow the provider's authorized users, as designated by the provider's office administrator, to enter, view, and update (including retroactively) all provider data.	BR-01-001, PIC-01

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-SEC-055	The Solution must validate email addresses associated with the provider account through a confirmation and/or activation email process that requires the user to respond to activate the email account for agency communication.	BR-01-001
PDM-REQ-SEC-056	The Solution must provide tools (e.g., alerts or reports), which identifies usage anomalies or users who may have misused the Solution.	
PDM-REQ-SEC-057	The Solution must automatically maintain an audit trail of users, including database administrators, who pass through or view a record, regardless of whether data is changed.	
PDM-REQ-SEC-058	The Solution must ensure that the audit trail cannot be modified and includes documentation of users who completed each change and why the change was made.	

Table R16. Solution

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SOLN-001	All Vendor websites must be accessible using mobile phones and tablets using Android OS and Apple iOS.	
MES-REQ-SOLN-002	The Vendor must ensure website form fields are validated on the client side as well as on server side.	
MES-REQ-SOLN-005	The Vendor's website shall provide online, context-sensitive help that provides current and accurate information that is in a format and structure approved by the Department.	
MES-REQ-SOLN-006	The Vendor's operations Portal must implement standard policies and practices to ensure the security and integrity of the information to be exchanged.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SOLN-007	The Vendor must have processes in place to restrict access when inappropriate Solution access or misuse is detected.	
MES-REQ-SOLN-008	The Vendor must prohibit concurrent logins to the Solution's website by an individual user or by a single user ID.	
MES-REQ-SOLN-009	The Vendor must ensure all website users are notified in advance of five (5) days of any scheduled maintenance on the website's main page as per the timelines approved by the State.	
MES-REQ-SOLN-010	The Vendor must provide a notification web page that displays when the Solution is unavailable for scheduled maintenance or unscheduled outages.	
MES-REQ-SOLN-011	The Solution must provide functionality to notify users of the reason for any Solution component or content reason for non-availability and provide an expected service resumption time.	
MES-REQ-SOLN-012	The Vendor must display error messages that explain why the user could not reach the production system and must include a link back to home page or the origin page.	
MES-REQ-SOLN-013	The Solution must provide links to relevant web resources (e.g., State and Federal websites, and other entities determined by the State to be appropriate for the self-service portal).	BR-11-001
MES-REQ-SOLN-014	The Solution must provide an online self-service Frequently Asked Questions (FAQ) tool that is easily navigable and searchable. The FAQ must be updated quarterly or as directed by the State.	BR-11-001
MES-REQ-SOLN-015	The Vendor's solution must integrate with the MES landing page as described in Attachment V.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-SOLN-016	The Solution must support the preferred stakeholder communication methods: email, on screen notification, and bulk email blasts.	
MES-REQ-SOLN-017	The Solution must support role-based configurations.	
MES-REQ-SOLN-018	The Solution must receive, translate, and process data to support batch and real-time integrations for secure exchanges.	
PDM-REQ-SOLN-019	The Vendor must display error messages, interactive help views and tables, and hypertext links.	
PDM-REQ-SOLN-020	The Solution must allow enrolled providers, and other State-authorized users access to the user's authorized secure areas (e.g. call center, document management, provider application data, provider data, reporting tools) of the Solution through single sign-on.	
PDM-REQ-SOLN-021	The portal Solution must support a framework that includes a public facing portal and a secured portal for registered providers and approved state-authorized users.	
PDM-REQ-SOLN-022	The Vendor's portal Solution must include useful links, including but not limited to, access to educational information about the credentialing program, access to MES systems (such as the Medicaid Integration System (MIS), Pharmacy Benefits Administrator (PBA), Enrollment Broker (EB), Interoperability (IO), NCTracks), FAQs, access to DHB and sister NCDHHS agency websites and managed care health plan websites.	BR-11-001
PDM-REQ-SOLN-023	The Solution must provide the capability for providers to review all data on enrollment, re-enrollment, revalidation, and user-initiated change request applications prior to final submission.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-SOLN-024	The Solution must provide an online self-service tool for providers to access messages and notices. The Solution must provide the ability to send, receive messages, and respond to messages.	BR-21-002
PDM-REQ-SOLN-025	The Solution must provide an online self-service tool for providers to add or remove provider account users and change user roles for all self-service functions, according to business rules.	BR-01-001
PDM-REQ-SOLN-026	The Solution must allow authorized users to view all aspects of a provider's record based on the user's assigned rule.	BR-01-001, BR-13-008
PDM-REQ-SOLN-027	The Solution must provide a public facing provider directory that updates real-time and includes a provider search feature to allow users, at minimum, to search by provider name (including phonetic search), network, location(s) (including city, state and zip code), provider classification(s), all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), accessibility, gender, and whether or not a provider is accepting new patients. At a minimum the results display must include; provider name, network(s) location(s), phone numbers, provider classifications, all languages spoken/language accommodations (e.g., English, Spanish, American Sign Language (ASL)), office hours, accessibility, whether or not a provider is accepting new patients, and any restrictions on the freedom of choice among providers in the public provider locator (e.g., ages served, gender).	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-SOLN-028	The Vendor must create, update, and maintain a public (no login required) Provider Portal. The Vendor is responsible for posting provider-related material to the Provider Portal and making updates to the material as needed and directed by the Department. The following provider material must be made available on the Provider Portal: · Provider announcements · Provider publications and instructions · User guides · Frequently Asked Questions (FAQs) · Links to relevant web resources (e.g., State and Federal websites, and other entities determined by the State)	BR-11-001
PDM-REQ-SOLN-029	The Solution must create and present a tracking or confirmation number when provider information is updated via the self-service portal.	
PDM-REQ-SOLN-030	The Solution must allow for a provider to save a draft version of their application at points throughout the enrollment process per the business rules.	BR-08-024
PDM-REQ-SOLN-031	The Vendor must ensure all platforms supporting or hosting browser accessible components or content shall be scanned for known vulnerabilities no less frequently than once a month, with scan results shall be sent to the State's Privacy and Security Officer.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-SOLN-032	The provider enrollment Solution must support comprehensive historical data management by fulfilling the following capabilities: Data Retention: The system must record and retain all historical changes to provider data, including data elements with associated date spans (e.g., effective and end dates), including but not limited to demographic information, addresses, credentialing status, affiliations, and enrollment statuses. · User Interface Accessibility: · Historical data must be readily accessible through the user interface for both providers (via self-service portals) and operational staff (via operational portals and dashboards). · The interface must clearly display a timeline or audit trail of changes, including the date/time of each change, the data element modified, the previous and updated values, and the user or system that made the change. · Filtering and Search: Users must be able to filter and search historical records by date range, data field, or change type to efficiently locate specific updates. · Audit Compliance: The historical data view must support audit and compliance needs, ensuring that all changes are traceable and immutable.	

Table R17. Solution Technical Approach

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-STA-001	The Solution must notify other Medicaid Enterprise System (MES) modules and external entities, such as the PHPs, about changes in a providers' enrollment status. The Solution must support both real-time automated updates and scheduled batch submissions based on the business need and integration capability of the receiving entities.	
PDM-REQ-STA-002	The solution must support the ability to exchange credentialing related data directly without integration through the MIS only as approved by the Department (e.g., NPPES, Fingerprinting agency)	
PDM-REQ-STA-003	The Vendor must perform provider data matches on any inbound primary source interfaces, (e.g. State Bureau of Investigation (SBI), Clinical Laboratory Improvement Amendments (CLIA)) using matching criteria following the Department's business rules.	BR-06-007, BR-06-010
PDM-REQ-STA-004	The Solution must be capable of receiving managed care provider network data from the Health Plans, PIHPs, Primary Care Case Management Entity (PCCME) and Integrated Care Model (ICM) entities and maintaining the validated provider contracts as part of each provider's record. The rejected contract records must be retained separate from the provider's record for State monitoring on PHP network compliance.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-STA-005	The Solution must integrate with the Medicaid Enterprise System (MES) Interoperability module to support the Department's requirements for maintaining a Provider Directory API that complies with NCQA requirements and CMS interoperability standards. The Vendor is responsible for managing the data necessary to meet or exceed the Provider Directory Requirements set forth in the CMS Interoperability and Patient Access Rule. See 42 CFR Parts 431, 435, 438, 440, and 457 and https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index and http://hl7.org/fhir/us/davinci-pdex-plan-net/STU1/	
PDM-REQ-STA-006	The Solution must integrate with the Medicaid Integration Services (MIS) platform to perform data exchange functions with other systems, as directed by the Department.	

Table R18. Staffing

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-STAF-001	The Vendor must provide sufficient personnel to administer and execute required project activities during the development, implementation, and operations phases of the project. This includes completing the project within the required timeframe, meeting the quality standards outlined in this RFP, and maintaining the adequate staffing levels throughout the life of the project.	
MES-REQ-STAF-002	The Vendor is solely responsible for and incurs all the costs related to recruiting, hiring, training, monitoring the performance of, and managing qualified professional and other staff to meet contractual requirements.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-STAF-003	The Vendor must work with the Department to plan for and identify any policy, programmatic, and technology changes to ensure the success of the program.	
MES-REQ-STAF-004	The Vendor's staff, working remotely, must be available to work in the State's primary project location at the Department's request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, user acceptance testing, implementation, and production deployment).	
MES-REQ-STAF-005	For any work performed at a location other than the primary Project site, the Vendor must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.	
MES-REQ-STAF-006	The Department reserves the right to request removal of any Vendor key personnel, assigned to the project, and the Vendor must comply with any such request immediately.	
MES-REQ-STAF-007	The Vendor may not fill two key personnel roles with the same resource.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-STAF-008	The Vendor must employ a Medical Director who is directly responsible for the operation of the Credentialing Committee and serves as its chair and voting member, as well as appointing a proxy in their absence. The Medical Director is subject to Department approval. The Medical Director will follow and enforce the Bylaws of the Credentialing Committee as approved by the Department. The Medical Director must participate in the review of Bylaws, credentialing committee operating policy and procedures, recruitment of credentialing committee members, and coordination of peer reviews. The Medical Director must meet the qualifications specified by NCQA. The Medical Director must have a valid, current Medical Doctor degree; be North Carolina licensed, and board certified within their specialty; have a minimum of 5 years' experience in medical practice; and have a minimum of 3 years' experience in supporting policy and claims solution services in commercial or government health insurance programs.	
PDM-REQ-STAF-009	The Vendor must provide staffing to perform all provider enrollment and credentialing required tasks, per Business Rules.	

Table R19. Testing

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-001	The Vendor must coordinate testing processes, activities and schedules with the State.	
MES-REQ-TST-002	The Vendor must build and maintain a testing schedule as part of the overall project schedule that accurately reflects all testing activities linked	

Requirement #	Requirement Description	Business Rules/Application Data Files
	with the appropriate dependencies between predecessors and successors.	
MES-REQ-TST-003	The Vendor must update the Master Test Plan, which is a living document, throughout all DDI phases within thirty (30) calendar days of a change being implemented prior to System Integration Testing (SIT), change in scope, and changes to access to testing tools.	
MES-REQ-TST-004	The Vendor must schedule, coordinate and support all testing activities to ensure that each test is prepared and performed in accordance with the Master Test Plan.	
MES-REQ-TST-005	The Vendor must lead, support and report status for all applicable test phases and all associated environments. This includes the test phases listed in Section 7.17 Testing.	
MES-REQ-TST-006	The Vendor must thoroughly test the Solution and demonstrate proof of successful Vendor testing for each testable requirement by providing all Vendor test results for State review and approval before testing is considered complete. In addition, Vendors should perform Solution demonstrations after each sprint showing the State what was completed and successfully tested during that Sprint.	
MES-REQ-TST-007	The Vendor must ensure it meets the State's Exit and Entrance criteria set for each phase of testing.	
MES-REQ-TST-008	The Vendor must support all testing efforts with other Solutions (both internal and external).	
MES-REQ-TST-009	The Vendor must utilize a Department approved automated testing tool.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-010	The Vendor must participate in verification of non-system elements of the overall Solution, such as manual processes, as directed by the State.	
MES-REQ-TST-011	The Vendor must make time-sensitive recommendations to support the specific Software Development Life Cycle (SDLC) activities (e.g., recommending for or against deployment of a new increment of functionality).	
MES-REQ-TST-012	The Vendor must make recommendations concerning test execution activities based on the results of testing.	
MES-REQ-TST-013	The Vendor must employ a testing escalation process that allows for criticality classification to determine frequency of reporting and/or meetings with the Department.	
MES-REQ-TST-014	The Vendor must support the Department in all testing activities by providing support staff and technical expertise.	
MES-REQ-TST-015	The Vendor must provide the Department access, as needed, to all test management software and test data including defect tracking, test execution status, test results and test traceability.	
MES-REQ-TST-016	The Vendor must propose Solutions for all issues, problems, and defects for the Solution identified through Operational Readiness Review.	
MES-REQ-TST-017	The Vendor must identify test configurations and environment.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-018	The Vendor must submit and obtain approval from the Department, of a Requirements Traceability Matrix (RTM) to ensure that all requirements are met with the appropriate evidence and artifacts. The RTM is a living document that will be submitted on a schedule approved by the Department.	
MES-REQ-TST-019	The Vendor must design and document detailed test cases for each sub-phase of testing.	
MES-REQ-TST-020	The Vendor must develop test cases that include positive and negative scenarios, and the negative scenarios must include error handling and stressing the system with bad or invalid data to ensure it is rejected correctly. Test cases must provide step-by-step instructions for executing test cases, including the identifications, expected results and actual results.	
MES-REQ-TST-021	The Vendor must present all test cases to the Department for review and approval by the Department prior to the start of testing execution. The Department may provide additional test cases as agreed to by both parties.	
MES-REQ-TST-022	The Vendor must test all data transmissions with the Department and the Department's agents and subcontractors to validate connectivity, format, and data. This may include data exchanges between the Department and the Vendor, or between the Vendor and other Department subcontractors.	
MES-REQ-TST-023	The Vendor must utilize a well-established and Department approved or supplied defect tracking tool and process for the management and reporting of all defects identified during testing.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-024	The Vendor must provide a functional demonstration of the Solution including any changes or enhancements prior to user acceptance testing.	
MES-REQ-TST-025	The Vendor must perform System Integration Testing (SIT) Sprint Demos to the Department for each completed sprint. Additional demos can be requested as needed.	
MES-REQ-TST-026	The Vendor must implement version control in all environments.	
MES-REQ-TST-027	The Vendor must provide authorized users access to necessary testing environments as required for testing during DDI and throughout the life of the Contract.	
MES-REQ-TST-028	The Solution's test environment(s) must mirror the production Solution in its size, files, databases, processing, and reporting. Any exceptions must be Department-approved and documented.	
MES-REQ-TST-030	For E2E testing, the test environment(s) data refresh must be scheduled per the Department approval.	
MES-REQ-TST-031	The Solution improvements or enhancements must be deployed to test environments before they are deployed to the production environment.	
MES-REQ-TST-032	The Vendor must plan and execute testing for all inbound and outbound interfaces, ensure accurate and secure data transmission between the Solution and the Medicaid Integration Services (MIS) or an interface protocol determined by the department. They must also validate the file names, file format, and data integrity within the file.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-033	The Vendor must perform regression testing for changes to the application, including defects and enhancements.	
MES-REQ-TST-034	The Vendor must automate and/or script their regression suite and provide those results to the state at agreed-upon intervals.	
MES-REQ-TST-035	The Solution must provide the ability to execute performance tests of a simulated user load consistent with the actual load projected or used in production.	
MES-REQ-TST-036	The Vendor must have a process for and the capability to mask, sanitize, scramble, or desensitize sensitive data (e.g., PII/PHI) when extracting data from the Solution's production environment for use in non-production environments.	
MES-REQ-TST-037	The Vendor must manage security, ad hoc, or other specialized testing	
MES-REQ-TST-038	The Vendor must perform Operational Readiness Testing (ORT) that includes a test of actual data processing in a fully operational environment.	
MES-REQ-TST-039	The Solution must provide the ability for the tester to perform temporal testing within all testing environments by manipulating the system date.	
MES-REQ-TST-040	The Vendor must provide training for all testing participants that includes: the system, processes, procedures, and tools used to execute testing.	
MES-REQ-TST-041	The Vendor must support all aspects including resources, scheduling, data, environments, and defect remediation as appropriate, for State-led testing.	

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TST-042	The Vendor must support State-led User Acceptance Testing (UAT) testing during planning and execution to include: · Assist the Department in developing User Acceptance Testing (UAT) test cases. · Refresh data, execute processes, and migrate releases or code fixes as requested or on an agreed-upon schedule. · Provide User Acceptance Testing (UAT) test data including masked production data.	
MES-REQ-TST-043	The Vendor must ensure that User Acceptance Testing (UAT) is conducted on a fully tested and operations-ready module component, including all software features.	
MES-REQ-TST-044	The Vendor must participate in all End-to-End testing with other Department partners as directed by the Department. This will include End-to-End testing prior to launch and may include periodic End-to-End testing as other technical processes and systems are modified or brought online.	
MES-REQ-TST-045	The Vendor must document test results and provide them to Department prior to implementing any changes in the production environment.	

Table R20. Training

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TRN-001	The Vendor must coordinate all training activities through the Department.	BR-01-002
MES-REQ-TRN-002	The Vendor must design and conduct all training in collaboration with the department and in accordance with the approved solution Training Plan.	BR-01-002

Requirement #	Requirement Description	Business Rules/Application Data Files
MES-REQ-TRN-003	The Vendor must conduct training at times and locations mutually agreed upon between Department and Vendor, which may include virtual options when approved by the Department.	BR-01-002
MES-REQ-TRN-004	The Vendor must create and maintain all training materials in such a way as to account for any system, policy, and operational modifications that are made throughout operations and maintenance.	
MES-REQ-TRN-005	The Vendor must provide training that describes the features, functions, limitations, standards and governance processes, tools, and other relevant items.	BR-01-002
MES-REQ-TRN-006	The Vendor must analyze, define, and tailor training to each specific user role and group.	BR-01-002
MES-REQ-TRN-007	The Vendor must ensure that the end users (state authorized users, Applicant users, Provider users, Vendor users) receive the training, education and technical assistance necessary for successful implementation, integration, and downstream operations. This training activity will be measured using the training evaluation and end user experience as included in the Training Plan. Post implementation training must be performed by the Vendor.	BR-01-002
MES-REQ-TRN-008	Vendor must provide, maintain, and update a training environment to design training and conduct training for each user, role, and group during DDI and O&M. Users and Department staff must have access to this environment.	BR-01-002
PDM-REQ-TRN-009	The Solution must document training attendance to a provider's record to include the training date, attendee name, and title of the training.	BR-01-002

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-TRN-010	The Vendor must conduct dry run reviews of new training sessions or major updates with the Department prior to conducting provider training sessions.	BR-01-002
PDM-REQ-TRN-011	The Vendor must furnish and maintain appropriate hardware, software and telecommunications to support the development, maintenance and presentation of training program(s).	BR-01-002

Table R21. Workflow

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-WKF-001	The Vendor must implement an automated process within the Solution to transmit provider applications and associated data to the Department for review and approval, when required by State business rules.	BR-01-006, BR-06-008
PDM-REQ-WKF-002	The Solution must accommodate NC Specific program workflows and data management. Further defined in State Business Rules, this includes but is not limited to: -Primary Care Case Management (PCCM) program affiliations; -NC Minority Health Program, -Health Information Exchange (HIE), -Tailored Care Management assignment and data collection; -Systematic assignment of AMH Tier 2 status with the capability for providers to initiate an upgrade or downgrade of their AMH Tier status.	BR-08-006; BR-13-007; APP-02, APP-03, APP-04, APP-05, APP-11, APP-12, APP-13
PDM-REQ-WKF-003	The Solution must have configurable event-based workflow to instantiate information requests, correspondence or electronic notifications throughout the provider lifecycle.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-WKF-004	The Vendor must support and assist the Department in mapping all business processes and subprocesses to the workflow application and in transitioning from manual to automated process execution, as applicable.	
PDM-REQ-WKF-005	The workflow Solution must support work-type processing that includes internal and external dependencies.	
PDM-REQ-WKF-006	The workflow Solution must provide the ability to set and view alerts and/or reminders by user, by work-type.	
PDM-REQ-WKF-007	The workflow Solution must automatically update the state of the work item, based on the processing steps when completed to provide transparent, accurate status of the work at all times.	
PDM-REQ-WKF-008	The workflow Solution must provide supervisors access and control of work by type and by user.	
PDM-REQ-WKF-009	The workflow Solution must provide configurable work distribution and redistribution based on business rules that consider the nature of a required task, the various user roles, the status and age of the task, the priority and schedule, and any other data elements in the Solution. The workflow Solution shall include all tasks relevant to the operation of the contract, including provider enrollment, provider screening, primary source verification, credentialing committee operations, provider communications, reporting, compliance, monitoring, and all other functions of the Vendor's operation. Workflows and Business Rules are subject to approval by the Department.	

Requirement #	Requirement Description	Business Rules/Application Data Files
PDM-REQ-WKF-010	The Vendor must provide secure links within the workflow tool to all required screening and monitoring databases (e.g., Office of Inspector General (OIG) SAM, National Practitioner Database (NPDB), National Plan and Provider Enumeration System (NPPES), List of Excluded Individuals and Entities (LEIE)) when the data is not available through an automated interface.	

3.6 BUSINESS AND TECHNICAL SPECIFICATIONS

The Vendor must provide a response in their offer to all specifications as part of the technical proposal as defined in *Attachment T: Technical / Management Proposal*. The categories of specifications are listed in descending order of importance.

Note: The number assigned to each specification in the following tables may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

3.6.1 SPECIFICATIONS

Table S1. Business Operations

Specification #	Specification Description
PDM-SPC-BO-001	Describe how the system will handle duplicate records. Include screenshots where available.
PDM-SPC-BO-002	Describe how the solution will allow a provider to identify what Hospital(s) they have admitting privileges for without having to enter the hospital(s) NPI number. Include screenshots where available.
PDM-SPC-BO-003	Describe how your solution manages voided transactions to maintain history but disregard its impact on the record. For example: • Provider was approved in error by the Vendor, and the provider's enrollment needs to be voided. • A Prepaid Health Plan (PHP) affiliation record was sent in error. The provider to the PHP affiliation needs to be voided. • Provider is terminated, appeals the termination, wins the appeal, and the provider needs to be reinstated. The termination needs to be voided. Include screenshots where available.

Specification #	Specification Description
PDM-SPC-BO-004	Describe how your solution will interact with providers in-between revalidation periods to encourage providers to update their provider record. Include Key Performance Indicators (KPI) for how to measure engagement. Include screenshots where available.
PDM-SPC-BO-005	Describe how your solution will: • uniquely identify a rendering service location address for a provider • standardize and validate physical addresses • identify and prevent duplicate addresses across multiple locations for a provider • prevent a provider to overwrite an address for a service location unique identifier • allow providers to enroll a servicing county in lieu of a physical location Include screenshots where available
PDM-SPC-BO-006	Describe how your company will present business rules in a way that enables state users to visualize the rules. Include screenshots where available.
PDM-SPC-BO-007	Describe how the solution will configure, support and maintain business rules (i.e., add, modify, or remove/retire rules) and the type of resource and necessary skill set(s) required for business rule configuration. Include screenshots where available.
PDM-SPC-BO-008	Describe your reporting solution capabilities available to state-authorized users to include: • The solution for a library or repository or reports and ways to locate reports in the library/repository • The variety of formats of reports available for viewing, exporting, and printing – real-time dashboards, scheduled reports, HTML, Excel, TXT. CSV, PDF, etc. • Capabilities to query, including use of wild cards and date ranges, and display data in a variety of formats • Query templates for all state-authorized users to modify and reuse Include screenshots where available.

Table S2. Security

Specification #	Specification Description
MES-SPC-SEC-001	Describe how your proposed solution complies with applicable security standards identified by the State in this document and describe how compliance can be achieved and verified during Design, Development, and Implementation (DDI) and Operations of the solution.
MES-SPC-SEC-002	Describe how your Solution supports the State's Identity and Access Management protocols referenced in section 3.4.3 Identify, Credential, and Access Management (ICAM).
MES-SPC-SEC-003	Describe how the proposed solution manages user provisioning process to access the system functionalities.
MES-SPC-SEC-004	Describe the audit capabilities of the proposed solution related to management of the application.
MES-SPC-SEC-005	Describe the frequency and test procedures for end-to-end disaster recovery testing.

Specification #	Specification Description
MES-SPC-SEC-006	Describe the capabilities of the proposed solution to support the agency's continuity of operations and incident responses.
PDM-SPC-SEC-007	Describe how the solution will perform identity proofing of all users and their NCID to secure access to the provider's record and where the application submission is restricted to the Office Administrator (OA) NCID. User roles for individuals who are not the OA must have limited access to the provider's data as defined by data security.
PDM-SPC-SEC-008	Describe how the solution will interface with the NCID system to ensure required information from the NCID record is reconciled with the Office Administrator OA user account in the PDMCVO. Required information at minimum is the NCID, first name and last name, user email address.
PDM-SPC-SEC-009	Describe how the solution will manage the primary and secondary status for an Office Administrator (OA) when the primary is no longer an active user for the provider and keep the provider officers informed of changes to these roles.
PDM-SPC-SEC-010	Describe your approach to system-based performance auditing. Specifically: A schedule to assess at least annually the key systems used to process, store, archive, access, and present data that is critical to the success of the PDM/CVO Solution. The criteria used in the assessment to classify components as to their criticality to operations and the risk of failure or substandard performance. (Data Criticality Analysis - HIPAA requirement) The frequency and methods that will be used to audit critical systems and report results to the State. The approach to conducting audits to assure capacity, throughput, data integrity, data accuracy, and data control. The vendor's commitment to a systems-oriented approach that will focus on the proper functioning of the vendor's management systems.
PDM-SPC-SEC-011	Describe how the solution enables authorized state users to view changes made to a provider's record, including the date of the update, the specific data that was modified, the user who made the change, and the values before and after the change.

Table S3. Certification

Specification #	Specification Description
MES-SPC-CERT-001	Describe your company's experience with the MITA framework, and how that supports the State's achievement of MITA Level 3 or higher capability levels. Include in your narrative the information and technical architectures that support the solution while conforming with both the MITA Framework and Seven Standards and Conditions.

Table S4. Data

Specification #	Specification Description
MES-SPC-DATA-001	Data conversion often encounters risks and issues related to the complexities in defining the relationship between source and target data structures, differences in the data required for processing between legacy and new systems and the historical changes to processing requirements and valid codes that may result in data inconsistencies and missing data conditions. Describe approaches available for data conversion and/or data migration to load current data into proposed solution.
MES-SPC-DATA-002	Describe how the Vendor will provide real-time access to transactional data for integration with other MES Modules.
MES-SPC-DATA-003	Describe the tools and methods that will be used to support, provide, and maintain a comprehensive data dictionary.
MES-SPC-DATA-004	Describe how the solution would provide context sensitive help to view definitions of all data on system.
PDM-SPC-DATA-005	Describe how the solution will validate addresses as defined in Requirements PDM-REQ-DATA-029 and PDM-DATA-REQ-039. Include how your solution validates physical addresses and not PO or other non-physical addresses.

Table S5. Solution

Specification #	Specification Description
PDM-SPC-SOLN-002	Describe how your company will continually improve your solution to respond to changes in the Medicaid and healthcare industry, changes in state policy, customer-focused enhancements, and general product improvements as approved by the state.
PDM-SPC-SOLN-003	Describe how your approach embraces innovation and change, allowing for better services while maintaining good stewardship of State and Federal resources, and developing the solution with the express goal to reduce redundant data entry, make the process more efficient for end users, improve reception in the provider community, speed throughput, and improve the user experience.
PDM-SPC-SOLN-004	Describe how business process workflows are documented. Include the tools used and how the information is made accessible to the Department.
PDM-SPC-SOLN-005	Describe how your design strategy includes accommodating both design for integration partners and the solution development design for review by the state.
PDM-SPC-SOLN-006	Describe how your solution presents the homepage to users that lets them see the latest broadcast messages and helps them prioritize their work
PDM-SPC-SOLN-007	Describe how the solution will exchange notices and messages with providers
PDM-SPC-SOLN-008	Describe how the solution provides chat assistance outside of business hours.

Table S6. Workflow

Specification #	Specification Description
PDM-SPC-WKF-001	Describe the solution's capacity to configure, support and maintain a workflow solution (i.e., add, modify, or remove/retire existing workflow configurations) and the type of resource and necessary skill set(s) required for workflow management. Describe how the Vendor's solution will provide configurable work distribution and redistribution based on work type, user role, priority, and age of work.

Table S7. Communications

Specification #	Specification Description
PDM-SPC-COMM-001	Describe how your company will track and maintain the lifecycle of each application and related notifications will be traced to support auditing and reporting purposes. These should be accessible by department staff. Include screenshots where available.
PDM-SPC-COMM-002	Describe how your company will approach correspondence management, including if you will use a correspondence management system or other processes. Include screenshots where available.

Table S8. Architecture

Specification #	Specification Description
MES-SPC-ARCH-001	Describe the approach to how the Solution can be hosted on: • A State hosted environment. Refer to State hosting capabilities at https://itservices.nc.gov/services/hosting/cloud-services • A Vendor hosted environment. A narrative for both hosting options listed above must be included in your response.
MES-SPC-ARCH-002	Describe how the proposed solution monitors and reports the metrics on system performance.
MES-SPC-ARCH-003	Describe the future roadmap for your solution for the next 1-3 years.
PDM-SPC-ARCH-004	Describe how the contractor will set up interfaces used for primary source verification. Include how they will add additional sources as they may be required by the department

Table S9. Conversion

Specification #	Specification Description
PDM-SPC-CONV-001	Describe how you will convert existing Office Administrators from the legacy system into your system.

Specification #	Specification Description
PDM-SPC-CONV-002	The scope of data to convert is available from the canonical provider data model. Describe your approach to converting NC specific data not included in your solution's data model. Describe how all provider data, current and historical, is made accessible and viewable through provider and operational user displays, reports, dashboards, query tools and integrations.

Table S10. Integration

Specification #	Specification Description
MES-SPC-INT-001	Describe any import/export and/or extraction translation and load tools included in your solution.
MES-SPC-INT-002	Describe how the Vendor solution's technical capabilities will support the services, protocols, standards, capabilities, and functionality of the core MIS Services referenced in Attachment V: Medicaid Integration Services Core Capabilities.
MES-SPC-INT-003	Describe the proposed Solution capabilities to integrate with other systems. Identify the standards supported, integrations Solutions, adaptors, APIs, etc.
MES-SPC-INT-004	Describe how the Solution's data exchanges (including inbound and outbound interfaces) comply with industry standards (such as NIEM, NIST, HIPAA, HL7, FHIR, CCDA, and CSV) where applicable. Include in the narrative how non-standard formats required by State are covered.

Table S11. Testing

Specification #	Specification Description
MES-SPC-TEST-001	Describe the testing environments you will maintain in order to support all appropriate testing phases as listed in Section 7.17 Testing.
MES-SPC-TEST-002	Describe how your Solution's test environment mirrors the production environment in its size, files, databases, processing, data protection, and reporting. Include how this state of the environment is maintained in the response.
MES-SPC-TEST-003	Describe the defect management process and how abnormal results that arise during the execution of identified test cycles (e.g., DDI, Operations, UAT) are resolved, in alignment with the Defect Management and Master Test Plans.
MES-SPC-TEST-004	Describe the approach to ensuring independence and separation between the development and testing organizations.
MES-SPC-TEST-005	Describe how the solution will create and load test data and utilize it during the testing process. Include how PHI and PII data is protected or masked during testing and how participants are notified if testing involves confidential, PHI, or PII data.

Specification #	Specification Description
MES-SPC-TEST-006	Describe how your company conducts testing using automation testing tools, level of test automation, interactive testing, and interactive debugging available in the test environment.
MES-SPC-TEST-007	Describe how your company would develop, maintain, and automate your regression suite. Include pertinent details on the tools that will be used.
MES-SPC-TEST-008	Describe how your solution provides performance tests, and reporting of a simulated load consistent with the actual load projected or used in production.
PDM-SPC-TEST-009	Describe how your company will evaluate and report to the State the impact of business rules in a testing environment prior to deployment.

Table S12. Project Management

Specification #	Specification Description
MES-SPC-PM-001	Describe your requirement management methodology during the DDI and O&M phases based on the RTM deliverable. Include in your response the approach to connecting requirements to their evidence and vice versa (bidirectionality).
MES-SPC-PM-002	The Solution will become one module in the State's Medicaid Enterprise Solution (MES), where multiple vendors and the State may need to coordinate activities during development and as the different modules are prepared, tested and implemented. Describe your approach to this coordination and your availability for onsite meetings during DDI or special circumstances if requested by the State.
MES-SPC-PM-003	Describe your approach to managing the Software Development Life Cycle, describing how they will design, develop, and test software and operational processes to meet or exceed Department expectations and deliver promised components within time and cost estimates. Please address the different phases of the project. - Planning: Defining the scope and purpose of the project. - Analysis: Gathering requirements and analyzing them. - Design: Creating the architecture and design of the software. - Testing: Test Planning and Test Execution of the code - Implementation: Implementing the code. - Maintenance: Updating and fixing the software post-deployment.
MES-SPC-PM-004	Describe your company's quality management policies procedures, and practices it will implement to ensure quality, completion, and validation of the accuracy of the documentation and services required in the RFP.

Specification #	Specification Description
MES-SPC-PM-005	Describe how you will measure, track and document the quality of deliverables.
MES-SPC-PM-006	Describe the approach for participation in Department initiated deliverable reviews and incorporation of feedback and recommendations.
MES-SPC-PM-007	Describe your company's approach to production implementation and cutover.
MES-SPC-PM-008	Describe your company's approach to collaborating with the existing vendor to identify interfaces, capabilities, and processes, for seamless cutover.
MES-SPC-PM-009	Describe how your company will identify and acquire the licenses necessary for any software, services, and accounts to support the requirements defined in the RFP. Include in your narrative how the State can own or be named on the license of any software that is designed, developed, installed, improved, or configured with enhanced Federal Funding Participation (FFP), in accordance with § 433.112(b)(5).
PDM-SPC-PM-011	Describe any special plans to monitor the system in the days following go-live to ensure programs are not negatively impacted and are operating as expected.
PDM-SPC-PM-012	The PDM/CVO will become one module in the state's Medicaid Enterprise Solution (MES), where multiple vendors and the state may need to coordinate activities during development and as the different modules are prepared, tested and implemented. Describe your approach to this collaboration and your availability for onsite meetings during DDI or special circumstances if requested by the state.
PDM-SPC-PM-013	Describe your agile approach and sprint demo processes.

Table S13. Operations and Maintenance

Specification #	Specification Description
MES-SPC-OM-001	Describe your plan to provide NCDHHS the ability to transition from the Vendor solution to State/New Vendor and maintain the continuity of operations.
MES-SPC-OM-002	Describe your approach to ensure the solution and all included portals and interactions are available for NC users with an annual availability of 99.99% uptime. Describe your approach to monitoring, measuring, and reporting.

Specification #	Specification Description
MES-SPC-OM-003	Describe your approach to address and resolve customer support and technology disruptions impacting the ability to maintain a fully working Solution. Include in your narrative: · The timeframe required to accomplish full recovery from the point of interruption. · Strategies for addressing longer disruptions resulting from natural disasters or cyberattacks. · A detailed communication strategy to ensure stakeholders are informed during disruptions.
MES-SPC-OM-004	Describe how the Solution promotes sharing, leveraging, and reuse of healthcare technologies and systems within and among states in accordance with the CMS Standards and Conditions (Leverage Condition) in force during the period of the contract.

Table S14. Staffing

Specification #	Specification Description
MES-SPC-STAF-001	Describe how your company will hire and retain staff and Key Personnel with the qualifications and experience necessary to perform the requirements of this RFP.
MES-SPC-STAF-002	During the Operations and Maintenance phase, describe the physical locations where the main office and satellite offices (if satellite offices are applicable) are or will be located in North Carolina.

Table S15. Call Center

Specification #	Specification Description
PDM-SPC-CC-001	Describe how your tool will enable the State and your users to view and monitor call activity.
PDM-SPC-CC-002	Describe any Computer Telephony Integration (CTI) your solution will use to auto-populate screens and make customer service interactions more efficient.
PDM-SPC-CC-003	Describe how your company will staff the call center to ensure calls that cannot be resolved on the first call will be tracked and resolved to meet SLAs.
PDM-SPC-CC-004	Describe your staffing model that includes the ratio of staffing to Call Center operation volume (including, for example: total Call Center volume, average call wait time, rate of abandoned calls, length of call, open vs. closed trouble tickets

Specification #	Specification Description
PDM-SPC-CC-005	Describe how your solution allows authorized State and PDM/CVO staff real-time access to a provider-applicant's record during the enrollment application data entry process by the provider-applicant.

Table S16. Training

Specification #	Specification Description
MES-SPC-TRN-001	Describe the curriculum and training documents used for training external users. Include in your narrative help screens, descriptions of online or printable materials, use of knowledge bases, etc.
MES-SPC-TRN-002	Describe the type of training offered in your training program to meet the needs of users with different learning styles. Include how you determine the effectiveness of your training via such methods as surveys and real-time feedback sessions.
PDM-SPC-TRN-003	Describe how the Contractor's solution links to training modules within the enrollment process.

3.7 OPTION REQUIREMENTS AND SPECIFICATIONS - RESERVED

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must provide a complete cost proposal that is inclusive of all of the costs associated with the solution and services outlined in this RFP, including all direct and indirect costs. The Cost Proposal must be submitted using the Microsoft Excel Cost Proposal Workbook referenced in *Attachment E: Cost Form*. The Cost Proposal will contain the following:

Total Implementation Costs: The deliverables associated with planning, development, and implementation effort necessary to deliver the solution and services outlined in this RFP.

In addition to the Total Implementation Costs, describe how the Vendor can also provide a schedule reflecting a request for payment for satisfactory performance of the remaining scope (Non-Implementation or Steady State) of the contract.

Each deliverable within a Phase must have a cost unless otherwise noted by the Department within the Cost Proposal Workbook.

Operations and Maintenance Costs: The ongoing services, support, deliverables, and cloud hosting necessary to provide the solution and services outlined in this RFP after the initial implementation.

- a. Costs must be provided for each year of the Contract term.

- b. Operations and Maintenance Costs will begin after Solution Implementation is complete and approved by the Department.
- c. Operations and Maintenance Costs will be billed monthly:
 - i. Services and Support for the functionality of Items in *Attachment E: Cost Form* will be billed as one-twelfth (1/12th) of the annual cost for the item for the upcoming month.
 - ii. Ongoing Maintenance deliverables will be billed by the Vendor upon delivery and approval by the Department.
 - iii. Cloud Hosting will be billed as one-twelfth (1/12th) of the annual cost for the upcoming month.
- d. Fully Burdened Hourly Labor Rates for all Key Personnel and other project staff must be provided.
- e. Additional Costs – The Vendor may provide any additional costs that are specific to the implementation of their solution that are not outlined in the Cost Proposal Workbook referenced in *Attachment E: Cost Form*. Vendors may submit written questions in accordance with *Section 6.2.2 Questions Concerning The RFP*.
- f. Assumptions – The Vendor must provide any assumptions made in their cost proposal.

4.2 PAYMENT SCHEDULE

The Vendor must propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables.

5.0 EVALUATION

5.1 SOURCE SELECTION

A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value to the State, recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when price is considered with or traded off against non-price factors.

- a. Evaluation Process Explanation: The State will establish an evaluation committee to review each Vendor's response to this RFP and make award recommendations. The State will designate employees, independent contractors, or other individuals to serve on the evaluation committee or assist the evaluation committee as a subject matter expert during the evaluation process. The State reserves the right to alter the composition of the evaluation committee and to designate individuals and subject matter experts to assist in the evaluation process. All offers will be initially classified as being responsive or non-responsive. If an offer is found to be non-responsive, it will not be considered further. All responsive offers will be evaluated based on the stated evaluation criteria.

- b. To be eligible for consideration, the Vendor's offer must conform to all requirements and must substantially conform to the specifications provided in this RFP. Compliance with requirements and specifications will be determined by the State. Offers that do not meet all requirements listed in this RFP may be deemed deficient.
- c. The State reserves the right to reject any offer if the evidence submitted by, or investigations, reviews or validations of, the Vendor and its proposal fail to satisfy the State that the Offeror is properly qualified to carry out the obligations of the Contract and to provide the required services.
- d. The evaluation committee may request clarifications or presentations from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or in part, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer as part of the negotiation process, if applicable.
- e. Vendors are advised that the State will not ask for or accept data that is essential for a complete and thorough evaluation of the offer after the closing date for receipt of offers.
- f. The evaluation committee will make a recommendation to award to the Vendor meeting the RFP requirements and whose offer is determined to be most advantageous and provide the Best Value in accordance with N.C.G.S. § 143-135.9, to the State, based on the evaluation criteria described in the RFP, and the evaluation committee's ranking of proposals and the basis and reasons for the selection decision. Upon approval of the recommendation by the State, the notice of award will be issued, with the State executing a Contract with the successful Vendor.

5.2 EVALUATION CRITERIA

Evaluation shall include Best Value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in descending Order of Importance. While all responsive proposals will be evaluated in accordance with the stated criteria, consideration will be given to the impact on the State's technical and business resources and environments.

- a. Business and Technical Specifications of this RFP. Within the business and technical specifications listed in Section 3.6.1 the major categories listed by table are further listed in descending order of importance as provided in Attachment T. For example, the Business Operations category is more important than the Testing category. The specifications listed within a major category, such as Business Operations, are all of equal importance. In addition to the business and technical specifications, vendors will be required to perform a system demonstration based on use cases provided by the Department once a competitive range has been established. System demonstrations will be scheduled by the assigned Contract Specialist during the evaluation phase of the solicitation. System demonstrations will be limited to two (2) hours and shall be provided by the vendor staff performing the day-to-day work vs the

sales/marketing team. The System demonstrations will be evaluated and included as part of the business and technical specifications evaluation.

- b. Corporate background and experience, and strength of references (see Attachment H: Vendor References/Past Performance), relevant or material to technology area(s) or Specifications. The Vendor may be disqualified from any evaluation or award if the Vendor or any Key Personnel proposed (see Attachment K: Vendor Key Personnel), has previously failed to perform satisfactorily during the performance of any contract with the State (e.g., unresolved vendor complaint forms on file with the State or contracts terminated for default) or violated rules or statutes applicable to public bidding in the State;
- c. Cost: Total Cost of Ownership in the formatted cost tables provided in this RFP.

Only those proposals that substantially conform to the RFP will be considered for award.

5.2.1 EVALUATION OF OPTIONS - RESERVED

5.3 BEST AND FINAL OFFERS (BAFO)

The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendor(s) within this range, e.g., "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers consistent with the stated evaluation criteria to determine the final rankings.

5.4 POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, and to the committee responsible for participating in the evaluation. The Vendor submitting a proposal (including its representatives, subcontractors, and suppliers or other pilot partners or affiliates) is prohibited from having any communications with any person inside or outside the using agency, issuing agency, other government agency office, or body (including the purchasing agency, department secretary, agency head, members of the General Assembly and Governor's office), or private entity, if the communication refers to the content of Vendor's proposal or qualifications, the content of another Vendor's proposal, another Vendor's qualifications or ability to perform the contract, and/or the transmittal of any other communication of information that could be reasonably considered to have the effect of directly or indirectly influencing the evaluation of proposal and/or the award of the contract. Vendors who attempt to gain privileged information, or to influence the evaluation process will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 must be clearly marked as such in the offer when submitted.

5.5 COMPETITIVE RANGE

Following the initial evaluation of proposals, the Department will establish a competitive range composed of the highest-ranked Offerors whose proposals are determined to be reasonably susceptible of being selected for award based on stated evaluation criteria. Only those Offerors within the competitive range will be invited to participate in additional evaluation activities, to include a System demonstration.

The Department reserves the right to limit the number of Offerors in the competitive range based on the evaluation results, inclusive of Total Cost of Ownership, and the Department's determination of the most advantageous proposals.

5.6 SYSTEM DEMONSTRATIONS

System demonstrations will be conducted only with Offerors in the competitive range. Demonstrations will be based on use cases provided by the Department and will be limited to two (2) hours. Demonstrations must be conducted by the proposed project team members who will be responsible for day-to-day operations, not sales or marketing personnel. Demonstrations will be evaluated and scored as part of the Business and Technical Specifications criteria in section 5.2 and will influence final rankings. Details and demonstration guidelines will be provided once competitive range has been established. Offerors will be provided sufficient time to prepare for demonstration.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

- a. The Offeror must meet all the minimum qualifications of this RFP, as provided in *Attachment Y: Minimum Qualifications*, for its proposal to be evaluated
- b. It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications, requirements and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person.
- c. The Vendor will be responsible for investigating and recommending the most effective and efficient solution. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the recommended approach is not short lived. Several approaches may exist for hardware configurations, other products and any software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

- a. The Offeror is made aware, pursuant to 01 NCAC 05B .0501, that in soliciting offers, any or all offers received may be rejected. The basis for rejection may include, but not be limited to the following:
 - i. The offer is deemed unsatisfactory as to quantity, quality, delivery, price or service offered;
 - ii. The offer fails to comply with conditions of the solicitation document or with the intent of the proposed contract;
 - iii. The Department determines there is a lack of competition;
 - iv. error(s) in specifications or indication that revision(s) would be to the State's advantage;
 - v. Cancellation of or changes in the intended project or other determination that the proposed requirement is no longer needed;
 - vi. Limitation or lack of available funds;
 - vii. Circumstances which prevent determination of the most advantageous offer and selection in accordance with N.C.G.S. § 143-135.9; or
 - viii. Any determination that rejection would be to the best interest of the State.
- b. If all offers are rejected, the solicitation may be cancelled in its entirety, or the Department may negotiate with one or more sources of supply that may be capable of satisfying the requirements.
- c. The Offeror is cautioned that this is a Request for Proposal (RFP), not a request to contract, and the Department reserves the unqualified right to reject all offers deemed failing to meet minimum qualifications, not responsive, incomplete, or non-compliant with the requirements described herein; or when such rejection is deemed to be in the best interest of the Department or the State of North Carolina.
- d. The Department may also:
 - i. Modify provisions of this RFP in response to changes in law or as required by CMS;
 - ii. Waive any formality or informality;
 - iii. Waive a specification or requirement of the RFP if it is in the best interest of the Department;
 - iv. Waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
 - v. Negotiate directly with one or more Offerors, to achieve a contract that is in the best interest of the Department, if the responses to this solicitation demonstrate a lack of competition, or offers are found non-responsive; and/or
 - vi. Cancel this RFP at any time. Notice of Cancellation will be posted on the NC eVP website.
- e. In the event all proposals are rejected, and the Department enters into negotiation, pursuant to 01 NCAC 05B .0503, the Department reserves the right to award a contract to the Offeror or Offerors, which, in its opinion, has (have) made the best proposal through the negotiation process.

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

Any and all amendments or revisions to this document shall be made by written addendum from the Agency Procurement Office. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendors contact regarding this RFP with anyone other than the State's contact person may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.

6.1.5 E-PROCUREMENT

This is an E-Procurement solicitation. Sub-Paragraph #38 of *Attachment B: Department of Information Technology Terms and Conditions* applies to this solicitation.

6.1.6 ELECTRONIC VENDOR PORTAL

The State has implemented the NC eVP that allows the public to retrieve award notices and information on the Internet at <https://evp.nc.gov>. Results may be found by searching by Solicitation Number or agency name. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

When a Vendor protests a contract awarded by the agency, the agency and Vendor shall comply with the following:

- a. The Vendor shall deliver a written request for a protest meeting to the agency head or the agency head's designee within fifteen (15) calendar days from the date of contract award. The Vendor's request shall contain specific reasons and any supporting documentation regarding why there is a concern with the award. If the request does not contain this information or the agency head determines that a meeting would serve no purpose, then the agency head, within ten (10) calendar days from the date of receipt may respond in writing to the offeror and refuse the protest meeting request. **Note:** Contract Award notices are sent only to the Vendor awarded the Contract, and not to every person or firm responding to a solicitation. Proposal status and Award notices are posted at <https://evp.nc.gov/>. If the protest letter contains or points to anything deemed or marked confidential and/or proprietary, Protester must include a redacted copy of the protest letter in accordance with Section 7.10 Confidentiality of Offers of this RFP.
- b. If the protest meeting is granted, the agency head shall schedule the meeting within thirty (30) calendar days after receipt of the letter, unless a later date is accepted by the protesting party and the agency. The agency shall provide written notice of the date and time of the protest meeting to any awarded vendor. The awarded Vendor may attend the protest meeting and provide a response to the protest allegations but is not required to do so. If the awarded Vendor submits a response in writing, it shall be provided to the protester by the Department before the protest meeting. Each party will be given a set period of time in which to present their side. The protester and awarded Vendor (if attending) may be represented by legal counsel of their own choosing and at their own expense. Within ten (10) calendar days from the date of the protest meeting, the agency head shall respond to the protesting Vendor in writing with a final agency decision.
- c. If a protest is determined by the agency head to be valid then the following outcomes may occur:
 - i. The award and issued purchase order shall be canceled and the solicitation for offers to contract is not re-bid;
 - ii. The award and issued purchase order shall be canceled and the solicitation for offers to contract is re-bid;

- iii. The award and issued purchase order shall be canceled, and the contract shall be awarded to the next lowest priced, technically competent, qualified Vendor, if that Vendor agrees to still honor its submitted bid.
- d. If the Vendor desires further administrative review after receiving a decision under paragraphs a. or b., the protesting party may, within sixty (60) days from the date such decision is received, file a contested case petition with the Office of Administrative Hearings (OAH) in accordance with N.C.G.S. §150B-23.

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 SITE VISIT OR PRE-OFFER CONFERENCE - RESERVED

6.2.2 QUESTIONS CONCERNING THE RFP

Vendors contact regarding this RFP with anyone other than the contact person listed on Page One of this RFP may be grounds for rejection of said Vendor's offer.

Written questions concerning this RFP must be received by the stated deadline to Medicaid.Procurement@dhhs.nc.gov. Please enter "Questions Solicitation 30-2026-017-DHB" as the subject for the message. Questions must be submitted using the following format in an excel file.

Question #	RFP Section	RFP Page Number(s)	Vendor Question
1	(Example: 5.4.a)	64	Question regarding specific issue?
2			

6.2.3 ADDENDUM TO RFP

If a Pre-Proposal Conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State will be posted to the Ariba Sourcing Tool and shall become an Addendum to this RFP. Vendors' questions posed orally at any Pre-Proposal Conference must be reduced to writing by the Vendor and submitted via the Ariba Sourcing Tool's message board. Oral answers are not binding on the State.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State Ariba Sourcing Tool for any and all Addenda that may be issued prior to the offer opening date.

6.2.4 COSTS RELATED TO OFFER SUBMISSION

Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.

All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.

6.2.5 VENDOR EXCEPTIONS - RESERVED

6.2.6 RESERVED

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

6.2.9 NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- “This offer does not constitute a binding offer”;
- “This offer will be valid only if this offer is selected as a finalist or in the competitive range”;
- “The Vendor does not commit or bind itself to any terms and conditions by this submission”;
- “This document and all associated documents are non-binding and shall be used for discussion purposes only”;
- “This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties”; or
- A statement of similar intent.

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Learn how to register a business in the state of North Carolina at: <https://www.nc.gov/working/business-nc/start-my-business>

6.2.11 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC eVP allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the at the following website: <https://evp.nc.gov>.

This RFP is available electronically on the electronic NC eVP at the following website: <https://evp.nc.gov>.

6.2.12 RESERVED

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:

- a. Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.
- b. Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
- c. Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.
- d. Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.
- e. Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.
- f. Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.
- g. **Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not be considered as a response to this solicitation.

6.3.2 OFFER ORGANIZATION

Within each section of its offer, Vendor should address the items in the order in which they appear in this RFP. Forms, or attachments or exhibits, if any provided in the RFP, must be completed, and included in the appropriate section of the offer.

- a. **Contents of Proposal:** This section should contain all relevant and material information relating to the Vendor's organization, personnel, and experience that would substantiate its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If any relevant and material information is not provided, the offer may be rejected from consideration and evaluation. Offers will be considered and evaluated based upon the Vendor's full completion and response to the following, and any additional requirements herein, or stated in a separate Exhibit.

- **Offer Format:** The proposal must contain the entire completed and signed Execution page of this RFP must be placed at the front of the proposal. Each page must be numbered. The proposal should contain a table of contents, which cross-references the RFP requirement and the specific page of the response in the Vendor's offer.
- b. **Proposal Content:** This Section lists the required content for completion of this RFP. Vendor shall populate all attachments of this RFP that require the Vendor to provide information and include an authorized signature where requested. The RFP response should be arranged in the following order:
1. Letter of Transmittal to include:
 - i. the submitting organization's legal name and employer identification number (EIN);
 - ii. the name, title, telephone and fax number, and e-mail address of the person authorized to negotiate the Contract on behalf of the organization;
 - iii. the name, title, telephone and fax number, and e-mail address of the person to be contacted for clarification;
 - iv. **Completed Attachment D** along with detailed description of the Vendor's organization to include the following:
 - Date Established;
 - Ownership (public company, partnership, subsidiary, etc.);
 - If incorporated, state of incorporation must be included;
 - Background of the organization (not to exceed three (3) pages);
 - Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's organization has been in business, whichever is less.
 2. **Completed and Signed** version of the **Execution Page**, along with the body of the RFP and signed receipt pages of any addenda released in conjunction with this RFP;
 3. **Completed Attachment T:** Technical / Management Proposal to be provided in accordance with the instructions provided for completion;
 4. **Completed Attachment H:** Completed Past Performance Questionnaires from References in accordance with instructions provided for completion;
 5. **Completed Cost Proposal Workbook:** Cost form to be completed in accordance with **Section 4** and instructions found in Attachment E;
 6. **Completed and signed Attachment F:** Vendor Certification Form;
 7. **Completed Attachment G:** Location of Workers Utilized by Vendors;
 8. **Completed Attachment I:** Financial Review Form and copies of Financial Statements as further described in Section 7.2;
 9. **Confirm Acceptance of Attachment J:** Enterprise Architecture. Vendor must confirm acceptance to adhering to the Department's requirements regarding developing and maintaining enterprise architecture information and artifacts using the tools and processes established by the Department.

10. **Completed Attachment K:** Key Personnel in accordance with the Instructions provided for completion;
11. **Completed Attachment M:** Contract Administrators;
12. **Completed Attachment N:** Deliverables and Milestones Schedule in accordance with the instructions provided for completion in paragraph 2.0 Milestones;
13. **Completed Attachment O:** Business Continuity Plan in accordance with the Instructions provided for completion;
14. **Completed Attachment P:** Disaster Recovery Plan in accordance with the Instructions provided for completion;
15. **Completed** and **signed** version of **Attachment Q:** State Certifications;
16. **Completed** and **signed** version of **Attachment R:** Federal Certifications;
17. **Completed** and **signed** version of **Attachment S:** Business Associate Agreement;
18. **Completed** and **signed** version of **Attachment X:** Request for Proposed Modification To The Terms and Conditions
19. **Completed** and **signed** version of **Attachment Y:** Minimum Qualifications
20. **Completed** and **signed** version of **Attachment Z:** Subcontractor Identification Form for each known Subcontractor.
21. **Completed** and signed version of **Attachment AC:** GenAI Disclosure and Fact Sheet;
22. **Current independent 3rd party assessment report** in accordance with Section 3.3.2, paragraph b, subparagraphs i)-iii);
23. **Completed** Vendor Readiness Assessment Report Non-State Hosted Solutions (“VRAR”) in accordance with Section 3.3.2, paragraph a.

ADHERENCE TO INSTRUCTIONS: Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.

6.3.3 OFFER SUBMITTAL

The Vendor’s proposal is subject to the conditions made a part hereof and the receipt requirements described herein must be submitted as indicated below.

- a. **Vendor must submit its proposal in response to this solicitation to the Ariba Sourcing Tool. Paper and email copies will be deemed non-responsive, and the proposal will not be considered. Proposals submitted by physical mail delivery or in person delivery in response to this solicitation will be deemed non-responsive and will not be considered further. Files must not be password-protected and must be capable of being copied to other media.**

- b. **INSUFFICIENCY OF REFERENCES TO OTHER DATA:** Only information that is received in response to this RFP will be evaluated. Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation. The Department will not click on any links to access information.
- c. **It is the responsibility of the Vendor to submit their proposal in accordance with these instructions to the Ariba Sourcing Tool by the specified time and date of opening. All electronic proposal submissions are subject to the conditions made a part hereof. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues.**
- d. **Proposal and Cost Proposal Workbook must be submitted to the Ariba Sourcing Tool.**
- e. Vendor's Proposal and Cost Proposal Workbook must be separate files and clearly named (e.g. **RFP 30-2026-017-DHB, Vendor's Name, Proposal**) and (e.g. **RFP 30-2026-017-DHB, Vendor's Name, Cost Proposal**).
- f. If your proposal is being submitted as multiple files, then the file names must be clearly noted. For example: **RFP 30-2026-017-DHB, Vendor's Name, Proposal 1 of 2; RFP 30-2026-017-DHB, Vendor's Name, Proposal 2 of 2.**
- g. Vendor must submit **one (1) executed (signed) electronic copy of its proposal.**
- h. Proposals must be submitted with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to submit a signed proposal shall result in disqualification. All proposals must comply with *Section 6.3.1 General Instructions for Offer and Section 6.3.2 Offer Organization*.
- i. Vendor must submit one (1) electronic copy of Vendor's **redacted proposal** to the Ariba Sourcing Tool in accordance with Chapter 132 of the General Statutes, Public Records, identified as **RFP 30-2026-017-DHB, Vendor's Name, Proposal Redacted**. For the purposes of this RFP, redaction means to edit a document by obscuring or removing information that is considered confidential and/or proprietary by Vendor and that meets the definition of Confidential Information set forth in G.S. 132-1.2. If Vendor's proposal does not contain Confidential Information, Vendor must submit a signed statement to that effect as **RFP 30-2026-017-DHB, Vendor's Name, Statement of Confidential Information**. If no redacted proposal is submitted by the Vendor, then the Department may use the unredacted proposal for any public record requests. Redacted copies provided by the Vendor to the Department may be released in response to public record requests without notification to the Offeror.
- j. This RFP is available electronically on the NC eVP at the following website: <https://evp.nc.gov>
- k. Proposal documents as submitted must include the entire RFP, proposal, and all addenda. Linked or referenced documents from web or other locations cannot be included and will not be considered or evaluated. Hyperlinks and uniform resource locators (URLs) are not permitted in any of the proposal documents.

For Vendor training on how to use the Ariba Sourcing Tool to view solicitations, submit questions, develop responses, upload documents, and submit offers to the State, Vendors should go to the following site: <https://eprocurement.nc.gov/training/vendor-training>.

Questions or issues related to using the Ariba Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM EST to 5:00 PM EST.

6.3.4 FALSIFIED INFORMATION

The Department may initiate proceedings to debar an Offeror from participation in the offer process and from Contract Award as authorized by North Carolina law if it is determined that the Offeror has withheld relevant or provided false information.

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer.

Complete Attachment G: Location of Workers Utilized by Vendor and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (*Attachment I*), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

- a. For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.
- b. For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.
- c. The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

- a. Pursuant to N.C.G.S. §143B-1350(h)(1), Agencies must conduct a risk assessment, including whether the Vendor has sufficient financial resources to satisfy the agreed upon limitation of liability prior to the award of a contract with Vendor.
- b. Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
- c. Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

Vendor should present its license or support agreements for review and evaluation. Terms offered for licensing and support of Vendors' proprietary assets will be considered.

The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees or other similar costs.

7.5 RESELLERS - RESERVED

7.6 DISCLOSURE OF LITIGATION

The Vendor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Agreement.

- a. The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or Key Personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. The Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.
- b. The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud

by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.

- c. All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the DIT Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.

7.7 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or Services with any Department, institution or agency of the State.

7.8 SECURITY AND BACKGROUND CHECKS

All Vendor personnel who need access to project resources must have a security background check performed by their vendor prior to onboarding. Upon State's request, the Vendor must provide the background check reports of the personnel.

The State reserves the right to conduct a security background check or otherwise approve any employee or agent provided by the Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the State's security or other similar requirements.

7.9 ASSURANCES

In the event that criminal or civil investigation, litigation, arbitration, or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of the Agreement, causes the State to be reasonably concerned about:

- a. the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions; or
- b. whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

All offers and any other RFP responses shall be made public as required by the NC Public Records Act and GS 143B-1350. Vendors may mark portions of offers as confidential or proprietary, after determining that such information is excepted from the NC Public Records Act, provided that such marking is clear and unambiguous and preferably at the top and bottom of each page containing confidential information. Standard restrictive legends appearing on every page of an offer are not sufficient and shall not be binding upon the State.

Certain State information is not public under the NC Public Records Act and other laws. Any such information which the State designates as confidential and makes available to the Vendor in order to respond to the RFP or carry out the Agreement, or which becomes available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.

7.11 PROJECT MANAGEMENT

All project management and coordination on behalf of the Agency shall be through a Single Point of Contact (SPOC) designated as the MES Program Project Manager. The Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor's work. All work performed pursuant to the Agreement shall be coordinated between the MES Program Project Manager and the Vendor Project Manager.

The Vendor shall employ a robust project management methodology tailored to the scope of work and complexity of the engagement described in the RFP. The Vendor shall provide project management services that align with the Department processes and tools, including the development and maintenance of a detailed Project Work Plan (PWP) that supports transparent reporting, tracks milestones and dependencies, and integrates with the Department's Integrated Master Schedule (IMS).

The Vendor shall describe and provide the project management methodology (agile, agile-hybrid, or others) and sequencing that will be used to implement the project.

7.11.1 RISK AND ISSUE MANAGEMENT PROCESS

Vendor must align its Risk and Issue Management Process with the Department, which describes the processes to be employed by the Department and Vendor to ensure that risks and issues are identified, classified, monitored, and mitigated in a visible fashion. The Risk and Issue Management Process establishes procedures for documenting and updating risks and issues to ensure that all items are:

- i. Clearly identified and categorized based on severity, likelihood, and potential impact
- ii. Assigned to responsible owners for tracking and resolution
- iii. Logged in the Department's centralized repository for visibility and auditability
- iv. Regularly reviewed and updated to reflect current status and any changes in mitigation or resolution plans
- v. Escalated appropriately when thresholds are exceeded or resolution is delayed
- vi. Linked to mitigation strategies and contingency plans to minimize disruption

- vii. Closed formally with documented outcomes and lessons learned.
- a. The Risk and Issue Management Process includes procedures where the Parties interact to progressively reduce the program's exposure to events that threaten accomplishment of its objectives. The Vendor must comply with the following:
 - i. In coordination with the Contract Administrator, Vendor must promptly identify, categorize, and report risks and issues to mitigate potential impact. Categorization of risks and issues must follow the Department's severity, occurrence, and risk score metrics. Reporting of the risks and issues must occur within the Department defined tools.
 - ii. The Business Owner and Contract Manager will review this information within the Department defined tool to confirm if the risk or issue requires modifications.
 - iii. The risk and issue information must be presented through the Vendor's weekly status meeting. As applicable, the risks and issues must be presented through a weekly RAID meeting as well.
 - iv. The risks and issues must be reviewed at least weekly to ensure they reflect current status and any changes in mitigation or resolution plans. The Vendor must promptly notify the Department when a threshold is exceeded, or resolution is delayed.
 - v. The Vendor must formally close all risks and issues with documented outcomes and lessons learned.
- b. The Risk and Issue Management Process shall apply to all risks and issues identified by the Vendor, the Department, and any impacted parties.
- c. The Vendor's approach to risk and issue management will be subject to review as part of the Risk & Issue Management Plan deliverable. Additional contract requirements outline the Department's expectations for ongoing risk and issue management beyond this deliverable.

7.12 MEETINGS

The Vendor is required to lead and/or participate in a weekly status meeting during the DDI/Implementation/Closeout and applicable Operations & Maintenance (O&M) Phases of the project.

- a. These meetings will include an agenda containing updates, including but not limited to status, implementation, schedule, testing, training, risks, issues, actions, decisions, defects, and change management functions.
- b. The Vendor is required to lead and/or participate in stand-up meetings with the project team to address progress, risks, issues, and roadblocks to ensure the project deliverables and milestones are met as outlined in *Attachment N: Deliverables and Milestones Schedule*.
- c. Failure to participate in weekly status and/or stand-up meetings, two (2) consecutive or rescheduled meetings, may result in termination of the Contract.
- d. The Vendor is required to meet with State personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Contract. Meetings will occur as problems arise and will be coordinated by the State. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract.

7.13 RECYCLING AND SOURCE REDUCTION - RESERVED

7.14 SPECIAL TERMS AND CONDITIONS

7.14.1 PERFORMANCE BOND – RESERVED

7.14.2 CHANGE REQUEST MANAGEMENT PROCESS

Vendor must align its Project Change Request Management Process with the Department, which describes the processes to be employed by the Department and Vendor to ensure that changes are captured, planned, and implemented in a visible, controlled, and orderly fashion. The Change Request Management Process establishes procedures for documenting and controlling contract changes to ensure that all contract changes are:

- i. Necessary.
 - ii. Documented correctly in the Change Request Form (to be provided to the Vendor upon contract award) and include a detailed description of the impact to the project describing its severity and criticality.
 - iii. Evaluated to consider interfaces and IT environments.
 - iv. Evaluated against available resources.
 - v. Evaluated for cost reasonableness versus benefit, schedule, and performance trade-offs.
- a. The Change Request Management Process includes procedures where the Parties interact to propose, refine and if agreement is reached, sign off on the Project Change Request forms after approval by the Division's Governance Process. The Vendor shall comply with the following:
- i. In coordination with the Contract Administrator, Vendor must provide supporting information through the use of the change request management process as outlined herein. Completion of the Change Request Form includes a complexity assessment and the development of a level of effort (LOE).
 - ii. The Business Owner and Contract Manager will review this information to determine if the CR requires a new funding request or can be accommodated through funding set aside and approved for Necessary System Changes. Changes that have no impact to cost, schedule, scope or performance are administrative. Administrative changes, inclusive of those that may have a cost impact, but are determined to be within the scope of the contract, can be funded through the NSC. If a change is not administrative, it requires a contract amendment.
 - iii. The CR information will be presented through the Division's Governance Process. Vendors must allow a minimum fourteen (14) days for approval. The Division's assigned project manager will determine the appropriate governance committee and present the CR information.
 - iv. Change Requests of an administrative nature (not resulting in a Contract Amendment) do not require approval by the Centers for Medicare and Medicaid Services (CMS). All Contract Amendments require CMS approval prior to execution. Contract amendments require an additional sixty (60) calendar day review/approval cycle from CMS.

- v. Any new solution scope changes from approved change requests, resulting in either administrative changes or amendments, must be added to the solution project timeline.
- b. The State's Change Request Management Processes will not define or direct the manner in which each Party seeks internal approval of changes within that Party's decision-making hierarchy.
- c. Vendor shall not be entitled to compensation for any Services performed unless the Change Request Management Process is followed and approved by the governance committees in which all changes will be evaluated.
- d. The Change Request Process shall apply to all proposed Changes to the Services provided by the Vendor.
- e. Changes deemed reasonable, necessary, or proper that are made in the ordinary course of the Vendor's provision of Services that do not affect service levels, scope or time frames shall be made at no additional cost to the State.

7.14.3 MITA FRAMEWORK AND TECHNICAL ARCHITECTURE SEVEN STANDARDS AND CONDITIONS

The Medicaid Information Technology Architecture (MITA) is an initiative of the Center for Medicaid & Medicaid Services (CMS). It is intended to foster integrated business and IT transformation across the Medicaid enterprise and to improve the administration of the Medicaid program. The MITA framework has been adopted by the Agency to provide guidance in improving business operations and supporting Information Technology (IT). To advance the alignment of the MITA Maturity Model (MMM), the Agency has developed a Concept of Operations document which describes the operational needs, desires, visions, and expectations of the Medicaid Enterprise Systems. The vendor must support the State's conformance with the MITA Framework and the Seven Standards and achieve Level 3 or higher MITA capability levels.

7.14.4 PERFORMANCE MANAGEMENT

The Vendor is responsible for the performance and quality of all contracted work required by the Contract. NCDHHS will monitor the vendor's performance, review reports furnished by the Vendor, and review any available data to the State to determine how the Vendor is performing against the contractual performance objectives. If the Vendor does not meet a performance objective in this RFP or standard outlined in the Service Level Agreements (SLAs), or in the Key Performance Indicators (KPIs), NCDHHS requires that the Vendor develop a Corrective Action Plan (CAP). The CAP should describe the issue, what action the Vendor is taking to correct the issue, and the anticipated timeframe to return performance to contractually obligated levels.

The State will monitor and manage the Vendor performance through the following metrics and reports, including but not limited to:

- a. Service Level Agreements (SLAs)
- b. Monthly reports such as:
 - i. Backup Reports (detailing failed backups and subsequent remediation)
 - ii. Patching Reports (detailing failed patching efforts and subsequent remediation)

- iii. Security Reviews
- c. Approval of contract deliverables
- d. Review of contract deliverables
- e. Operations Reviews
- f. Comprehensive Business Reviews
- g. Compliance Audits

7.14.5 RETAINAGE

N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts.

- a. For this procurement, this will include withholding a retainage of 10% of each invoice, less any accrued service credits, and will be paid upon confirmation by the Contract Administrator that the Vendor has delivered services in accordance with the specifications and SLAs.
- b. The State will also withhold the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4).
- c. The services herein will be provided consistent with and under these services performance review and accountability guarantees.

7.14.6 CMS CERTIFICATION

The Centers for Medicare and Medicaid Services (CMS) requires that all federally funded Medicaid Enterprise Systems (MES) adhere to federal regulations to achieve CMS certification and thereby qualify for enhanced federal funding participation (FFP). Certification is the procedure by which CMS validates that the MES are designed to support the efficient and effective management of the program and satisfy specific requirements and regulations to achieve enhanced Federal Funding Participation (FFP).

The Department requires each Vendor to adhere to Title 42, Chapter 4, Subpart C of the Code of Federal Regulations and other statutes governing the implementation of Mechanized Claims Processing and Information Retrieval Systems. The Department and Vendor will leverage Streamlined Modular Certification for Medicaid Enterprise Systems Certification Guidance for MES IT projects and adopt updates released by CMS upon publication or as advised by the Department.

CMS requires that all federally funded systems regularly report their performance using the CMS-required outcomes and metrics. The Department may add state-specific outcomes for unique circumstances or characteristics not reflected within those metrics.

Failure to meet CMS Certification criteria may result in loss of Federal Funding Participation (FFP). Inadequate performance or non-performance of the required services by the Vendor shall be subject to contractual remedies.

A certifiable system must also meet all applicable standards and conditions, including modularity. Modularity requires acquisition of loosely coupled modules with open, documented interfaces, including COTS solutions. CMS defines a module as a packaged, functional business process or set of processes implemented through software, data, and interoperable interfaces that are enabled through design principles in which functions of a complex system are partitioned into discrete, scalable, and reusable components. The CMS Certification requirements are provided in Table 6: CMS Certifications Requirements

Table 7.14.6-1 Outcomes and Metrics provides the State Outcomes and Metrics the Vendor will produce using the CMS Operational Reporting Workbook template. The Operational Reporting Workbook will be updated by the State and Vendor prior to go-live.

Outcomes and Metrics

Reference #	Outcome	Default Metrics	Regulatory Sources
Outcome 1: PM1 Application	A provider can initiate, save, and apply to be a Medicaid provider.	- Number of requests to help desk for problems with initiating, saving, and applying. - Average time to enroll from point of submit. a. Total time to enroll all providers/ b. Total # of enrolled providers	42 CFR 455.410(a)
Outcome 2: PM2 Screening	A state user can view screening results from other authorized agencies (Medicare, CHIP, other related agencies) to approve provider if applicable.	- Average Time to screen providers upon initial application without Return to Provider time. (Total time to screen all providers – RTP time)/Total # providers screened - Average Time to screen providers upon initial application with Return to Provider time included. - Total time to screen all providers/Total # providers screened	42 CFR 455.410(c)
Outcome 3: PM3 Screening	A state user can verify that any provider purporting to be licensed in a state is licensed by such state and confirm that the	- Number of enrollment denials and reasons for denials. - Average Time to screen providers upon initial application without Return to Provider time (Total time to screen all providers – RTP	42 CFR 455.412

Reference #	Outcome	Default Metrics	Regulatory Sources
	provider's license has not expired and that there are no current limitations on the provider's license ensure valid licenses for a provider.	time)/Total # providers screened - Average Time to screen providers upon initial application with Return to Provider time included Total time to screen all providers/Total # providers screened - Average Time to credential providers Total time to credential providers/Total # of credentialed providers	
Outcome 4: PM4 Revalidation	The system tracks the provider enrollment period to ensure that the state initiates provider revalidation at least every five years.	- Number of providers scheduled for revalidation by year. (Total # of providers in Medicaid) - Percentage of providers enrolled in the state system that are in the CMS Adverse Actions List. - # of state providers enrolled that are on the CMS Adverse Actions List/ - # state providers enrolled	42 CFR 455.414
Outcome 5: PM5 Termination	A state user (or the system, based on automated business rules) must terminate or deny a provider's enrollment upon certain conditions (refer to the specific regulatory requirements conditions in 42CFR455.416).	- Number of providers denied enrollment or termination of participation with reason. Provide denial or termination reason.	42 CFR 455.416
Outcome 6: PM6 Reactivation	After deactivation, a provider seeking reactivation must be re-screened by the state and submit payment of associated application fees before their enrollment is reactivated.	- Number of providers seeking reactivation and turn-around time (TAT) for enrollment. - Number of providers seeking reactivation with submittal of payment and TAT for enrollment.	42 CFR 455.420

Reference #	Outcome	Default Metrics	Regulatory Sources
Outcome 7: PM7 Appeal	A provider can appeal a termination or denial decision, and a state user can monitor the appeal process and resolution including nursing homes and ICFs/IID.	- Number of provider (by provider type) appeals and status of appeal: include TAT to final determination.	42 CFR 455.422
Outcome 8: PM8 Site Visits	A state user can manage information for mandatory pre-enrollment and post-enrollment site visits conducted on a provider in a moderate or high-risk category.	- Number of providers scheduled for site visit categorized by moderate and high risk. - Number of Providers with past due site visits. Include number of days past due	42 CFR 455.432(a)
Outcome 9: PM9 Background Checks	A state user can view the status of criminal background checks, fingerprinting, and site visits for a provider as required based on their risk level and state law.	- List of providers in pending status due to checks listed in outcome. Provide screen shots of high-risk providers. - Number of provider enrollments in process listed by outcomes check and status of outcome check and duration for each check. For example: 10 providers undergoing background checks. Aging range from 1 -10 days.	42 CFR 455.434
Outcome 10: PM10 External System Checks	The system checks appropriate databases to confirm a provider's identity and exclusion status for enrollment and reenrollment and conducts routine checks using federal databases including Social Security Administration's Death Master File, the National Plan and Provider Enumeration	- Number of providers in pending status due to other database confirmations. Include the reason for pending. For example: # of providers pending for NPPES verification or mismatch and or # of providers found in the Death Master File - Number of providers by provider type found in the Death Master File and the enrollment status of each	42 CFR 455.436

Reference #	Outcome	Default Metrics	Regulatory Sources
	System (NPPEs), the List of Excluded Individuals/Entities (LEIE), and the Excluded Parties List System (EPLS). Authorized users can view the results of the data matches as needed.		
Outcome 11: PM11 Risk Level Assessment	A state user can assign and screen all applications by a risk categorization of limited, moderate, or high for a provider at the time of new application, re-enrollment, or re-validation of enrollment. A state user can adjust a provider's risk level due to payment suspension or moratorium.	- Number of providers in each category by category for each new application, re-enrollment/revalidation - Number of providers with changes from moderate to high due to payment suspension or moratorium	42 CFR 455.450
Outcome 12: PM12 Application Fees	The system can collect application fees. A state user ensures any applicable application fee is collected before executing a provider agreement.	- Total number of providers in the network, # of providers in pend status due to lack of application fee, # of providers denied due to lack of application fee payment - Aging report of number of providers with lack of application fee payment in enrollment pend status	42 CFR 455.460
Outcome 13: PM13 Moratoria	A state user can set CMS and state-imposed temporary moratoria on new providers or provider	- Number of providers in temporary moratoria status and duration range - Number of providers in temporary moratoria outside of 6 months	42 CFR 455.470

Reference #	Outcome	Default Metrics	Regulatory Sources
	types in six-month increments.		
Outcome 14: PM14 Network Adequacy	A state user can determine network adequacy based upon federal regulations and state plan.	- Network adequacy is already reported on	42 CFR 438.68
Outcome 15: PM15 Sanctions and Terminations	A state user, and/or the system, can send and receive provider sanction and termination information shared from other states and Medicare to determine continued enrollment for providers.	- Provider enrollment stats for providers in pend and denied status due to sanction and or pending sanction and Medicare information.	42 CFR 455.416(c)
Outcome 16: PM16 Notices and Communications	The system can generate relevant notices or communications to providers to include, but not limited to, application status, requests for additional information, re-enrollment termination, investigations of fraud, suspension of payment in cases of fraud.	- Provide a copy of relevant notices and communications submitted to providers for each outcome category.	42 CFR 455.23
Outcome 17: PM17 Fraud	A state user can report required information about fraud and abuse to the appropriate officials.	- Number of open FWA investigations by provider type and status (This may already be submitted by states)	42 CFR 455.17

Reference #	Outcome	Default Metrics	Regulatory Sources
Outcome 18: PM18 Payment Suspension	The system, or a state user, can suspend payment to providers in cases of fraud.	- Number of providers in suspend status due to fraud include reasons and aging by provider type	42 CFR 455.23
Outcome 19: PM19 Agreements and Closure	A state user can view provider agreements and disclosures as required by federal and state regulations.	- These are related to ownership regulations. - Number of providers identifying as one or more of the ownership relationships. List by ownership relationship type	42 CFR 455.104 42 CFR 455.105 42 CFR 455.106 42 CFR 455.107
Outcome 20: PM20 Change in Circumstances	A state user can view information from a managed care plan describing changes in a network provider's circumstances that may affect the provider's eligibility to participate in Medicaid, including termination of the provider agreement.	- List of providers by provider type who have been released from the managed care entity due to: - Change in state residence - Investigation of FWA - Death - Others as defined by state - Include provider state Medicaid status	42 CFR 438.608(a)
Outcome 21: PM21 Directory	A beneficiary can view and search a provider directory.	- Number of help desk tickets logged for inaccessibility to provider directory. - Number of website hits on provider directory page.	42 CFR 438.10(h)

Table 7.14.6-1 Outcomes and Metrics

7.14.7 FUNDING TO IMPLEMENT NECESSARY SYSTEM CHANGES (NSC)

The Parties agree that a quantity of hours provided at a specific not-to-exceed cost per year to allow flexibility for implementing necessary system changes. It is an administrative and budgeting estimate for executing work that is not included in the scope of this Contract but is determined by the State as necessary to expand PDM/CVO Solution functionality. During the Operations & Maintenance (O&M) Phase of the Contract, the Contractor shall make one pool of optional additional labor available to the State to implement changes or add functionality to the PDM/CVO Solution in ways not specified in this Contract. The State may use these hours to make such changes or additions to the PDM/CVO Solution functionality at the State's discretion.

During the O&M phase of the Contract, the Contractor shall perform modifications to PDM/CVO Solution, as requested by the State, such as new features, programs, and services, legislative changes to the extent applicable to the PDM/CVO Solution, associated with these modifications. There shall be a set number of hours at fixed labor rates (onsite and offsite) in the Cost Workbook of an O&M Phase to accommodate such changes. During the O&M Phase, the Vendor shall make available up to the total dollar value of additional labor hours indicated in the line item in the Cost Workbook for the O&M Phase. At the conclusion of each O&M year, the State may carry forward the unused balance of O&M Phase Modification dollars to the following O&M year to increase the total dollar value of the O&M Phase. Each change or new functionality to the PDM/CVO Solution using these hours shall be governed by the Change Request Management Process as set forth in Section 7.14.2 of this RFP. Accomplishing approval during a Change Order's Governance stage means that each change must meet the contractual and legal standards, including CMS approvals.

The State shall have no obligation to use any pool labor or to pay the Vendor for non-utilized pool labor. NCDHHS reserves the right to forego resorting to these labor hours, to obtain competitive bids, and to award the work to outside vendors, if NCDHHS is advised or directed to do so by other State or Federal authorities, or if resorting to the Contractor would be unacceptable due to anticipated problems with scheduling, resources, prior performance, and/or excessive estimated costs. For the avoidance of doubt, any changes to the PDM/CVO Solution must be performed by the Vendor. Key Personnel costs are not authorized for billing against these labor hours.

The Vendor shall provide a "firm fixed price" for the work; however, if the Parties mutually agree that work on an activity utilizing these labor hours shall be charged on a "time and materials" or "cost not to exceed" basis, the State's payment obligation shall accrue only for hours worked at rates bid by the Vendor. If the State requests in a particular instance that the fee for these labor hours shall be a "firm fixed price" for a result rather than a quantity of labor, that price shall be subject to negotiation.

Regardless of the basis on which the State is charged for activity under these set-aside labor hours, the contractual documentation that authorizes and specifies each change activity may set forth service levels, performance standards and/or deliverables relating to the activity, as well as a percentage of compensation that is to be withheld until such standards are met or such deliverables are provided in acceptable form.

The dollar value for these labor hours is established as a budgeting and administrative convenience to the Parties and shall not be construed as a limitation to the Contractor's obligation under *Attachment B – "Department of Information Technology Terms and Conditions, Section 1. Paragraph 40: Unanticipated Tasks"* of this Contract, not to unreasonably refuse amendments to the Contract that may involve additional costs. The amount set aside for these labor hours shall not exceed \$200,000 annually.

7.14.8 ESCROW AGREEMENT - RESERVED

7.14.9 STATE CONTRACT REVIEW

This RFP and subsequent contracts are exempt from the State contract review and approval requirements pursuant to N.C.G.S. § 143B-216.80(b)(4).

7.14.10 TECHNICAL SOFTWARE CHANGES / UPDATES

The Vendor will notify NCDHHS of any changes to the technical platform including but not limited to software updates, platform changes, hosting changes, or functional updates. The Department categorizes changes as Routine Operational Changes, Functional Changes, or High impact Changes and will categorize a change at the Department's discretion. Descriptions of the changes with examples and required action are as follows:

- a. Routine Operational Changes – Routine operational changes are generally accepted to be changes to the platform that do not impact the functionality of the software or system but may impact the availability of the system. Examples could be security patching, changes to adjacent systems that impact availability, or routine operational processes such as server reboots. For these events the Vendor must use the existing Tech Ops release processes to notify NCDHHS.
- b. Functional Changes – Functional changes include any updates to the software or technical platform that will impact the functionality of the system. Functional changes must be approved using the NCDHHS Medicaid governance processes prior to initiating the development and testing of the new or changing functionality. In addition, other Departmental processes such as end-to-end testing, readiness, and deployment may also apply at the Department's discretion. Once these changes have completed development and are ready for deployment, the Vendor must use the existing Medicaid deployment processes and Tech Ops release processes.
- c. High Impact Changes – High impact changes are any modifications to the system or technical platform that result in materially significant changes to the functionality of the system, or significant changes to the technical platform. Examples of high impact changes are major software version upgrades, hosting platform changes such as migrating the technical platform from an on prem data center to the cloud, or changes to the underlying software or platform sub systems. Changes in this category must be presented to the Department in writing and approved by the Department before any work commences. The Department will define the appropriate executive governance venues for the Vendor to present the project.

A document describing the changes should include at a minimum a description of the full scope of the work, costs, risks, schedule, where the work is being performed, impacted deliverables, system availability impacts, and contingency plans. At the Department's discretion additional information may be requested. In addition, these changes must be approved through the NCDHHS Medicaid governance processes prior to initiating the development and testing of the new or changed functionality. Other Departmental processes such as end-to-end testing, readiness, and deployment may also apply at the Department's discretion. Once these changes have completed development and are ready for deployment, the Vendor must use the existing Medicaid deployment processes and Tech Ops release processes.

7.15 TECHNICAL OPERATIONS

- a. Processes - The Vendor must comply with all NCDHHS Technical Operations (Tech Ops) team processes and procedures included herein. The Tech Ops processes may change over time, and any changes to these processes shall be mutually agreed upon between the Vendor and the Department. Any Tech Ops processes that impact the cost or scope will be managed through the Change Request Management Process as described in section 7.14.2. Upon contract execution and prior to implementation, the Tech Ops team will provide an onboarding process which will detail all specific processes and procedures the Vendor will follow.

The Department, at its discretion, will track issues reported by the Vendor and may require a more comprehensive corrective action plan if the Department identifies trends in the Vendor's performance.

- b. Retransmissions – If the Vendor receives an Unintelligible Transmission from the Department, the Vendor will immediately notify the Department via the Tech Ops team and the Department shall retransmit as soon as the errors are remediated. If the Vendor is notified by the Department or the Department's vendor of the receipt of an unintelligible transmission, the Vendor shall retransmit as soon as the errors are remediated.
- c. Test Data Transmissions - The Vendor will be required to test all data transmissions with the Department and the Department's agents and subcontractors to validate connectivity, format, and data. This may include data exchanges between the Department and the Vendor, or between the Vendor and other Department subcontractors. The Department will oversee any testing and review results. If the testing is not successful, the Department will define an appropriate remediation period if not defined in other sections of this RFP.

7.16 HELP CENTER

- a. Processes - The Vendor must comply with all NCDHHS Help Center processes and procedures included herein. The Help Center processes may change over time, and any changes to these processes shall be mutually agreed upon between the Vendor and the Department. Any Help Center processes that impact the cost or scope will be managed through the Change Request Management Process as described in section 7.14.2. Upon Contract execution and prior to implementation, the Help Center team will provide an onboarding process which will detail all specific process and procedures the Vendor will need to follow.
- b. Monitoring - The Help Center phone line, integrated email addresses, and case list will be monitored by the Help Center Monday through Friday from 8am until 5pm. Additionally, if the risk of increased case volume is forecasted in scenarios such as program launches, the Help Center will be monitored during off hours and weekends to ensure proper coverage. The Vendor's designated Help Center point of contact must be able to monitor the case work and respond to potential escalations during these times. The Vendor's Help Center point of contact must attend all weekly stand-up meetings to discuss case progress.
- c. Escalation - Business production issues that cannot be resolved through normal process and procedures must be escalated by the Vendor to the Help Center. The issue will be tracked and resolved via the Help Center. Urgent priority cases, which cause widespread impact to a critical business function with no workaround or that can result in possible user harm if not addressed immediately, may be escalated either via the Department or the Vendor. Urgent priority cases will follow the Urgent priority response guidelines below:
 - i. Upon receipt of an Urgent priority case, the Department will organize a rapid response team to include all appropriate internal and external vendors;
 - ii. The Department will initiate a meeting cadence to discuss the urgent issue and develop a plan of action;
 - iii. The Vendor assigned to manage the Urgent priority case must make daily updates, including on weekends and holidays if deemed necessary, in the work-notes of the case contained within the Help Center case management application, and be prepared to give further updates on rapid response and Help Center status calls;

- iv. The Help Center team will monitor and may make requests for updates inside the Help Center case management application while the case is open.
- d. Licensing and Training - The Vendor must inform the Department of any additional user licenses for the Help Center case management application, that are required or any users whose licenses need to be decommissioned. If any training is needed, the Vendor must contact the Help Center team for scheduling.

7.17 TESTING

The testing strategy requires close collaboration between the Department and the Vendor. The strategy is designed to provide the Department with oversight of all testing levels and Vendor performance to ensure contract requirements and business needs are met. This includes Vendor testing processes, Vendor testing, Vendor test data management, Vendor defect management, risk and issue management, requirement traceability, and Department acceptance prior to system go-live.

The Vendor will be responsible for the test phases and environments identified as the owner in the table below and for ensuring automation is incorporated where appropriate for new functionality and in the baseline regression suite. The Department will be the primary owner responsible for the UAT and E2E test phases with Vendor support as provided in the table below.

Throughout the module's implementation, the vendor will submit various testing artifacts such as test cases, scripts, reports, and plans to the Department for review and approval. The Vendor will utilize a test execution and reporting tool such as Jira or ALM for test management and reporting, and the selected tool must be configured for PHI, PII, and HIPAA data. Regular status updates are expected throughout the testing process.

- a. The following table provides the standard testing phases utilized by the State with associated environments, owner, and description of the testing phase.

Testing Phase	Environment	Owner	Description
Unit	Development	Vendor	Tests individual components of the software to validate expected behavior.
SIT	SIT	Vendor	Performed on the integrated system to confirm integration functionality and quality. SIT testing is conducted in the SIT environment.
Regression (includes automated testing)	SIT	Vendor	Executed to confirm that new configurations and developments do not adversely affect existing system design and functionality.
Performance (includes automated testing)	Performance	Vendor	Determines system performance and validates KPIs. Results are measured against baselined performance metrics such as responsiveness,

Testing Phase	Environment	Owner	Description
			speed, scalability, and stability under variety of load conditions to eliminate performance bottlenecks from the system.
Security	Security/Disaster Recovery	Vendor	Performed to uncover vulnerabilities, threats, and risks in the application to prevent system weaknesses and potential loss of sensitive and/or confidential information.
Disaster Recovery	Security/Disaster Recovery	Vendor	Verifies that the Department can restore data and applications according to the defined RTO and RPO.
UAT	UAT	NCDHHS (with Vendor support)	Formal validation of the module's acceptance criteria in the UAT environment. Provides the end users and business stakeholders the opportunity to gain experience with the system and execute test cases, using the results to determine whether the system is acceptable.
Parallel (as applicable)	Vendor will create one	Vendor	Executed on the "to be" system functionality and compared to production environment's "as is" functionality. Automation is used as applicable.
Conversion/Migration (as applicable)	N/A	Vendor	Validates the successful and accurate transfer of existing production data to the target system, ensuring data integrity and continuation of business operations.
E2E	E2E	NCDHHS (with Vendor support)	Conducted in the E2E environment to test the entire system (the module, applicable legacy systems, interfaces, and any third-party systems) and validate all integration points identified in the E2E test paths.
Third Party Assessment	Vendor will create one	Third-party vendor, Vendor will support	Performed by a third-party vendor chosen by the State for each module at the end of UAT prior to Operational Readiness Review (ORR) to uncover any potential vulnerabilities, threats and risks in the application which might result in a loss of sensitive and/or confidential information and user control that would need to be remediated prior to

Testing Phase	Environment	Owner	Description
			Go-Live. The module vendor will support this and remediate any identified defects.

Table 17-7: Testing

7.18 INCIDENT PRIORITIZATION

For any issues that are encountered whereby an incident is formally submitted during the performance of the operations and maintenance phase of this contract, the incident will be prioritized by the State based on its operational impact, urgency, and context of the issue as provided in Table 7.18-1 Incident Prioritization Matrix. The examples provided in the Incident Prioritization Matrix are for reference purposes only. The State reserves the right to assess and assign the priority level for any incident.

Priority Level	Definition	Impact	Examples
P1 – Critical	Complete system outage or security breach with no workaround and no ability to conduct business	Business-critical services are down; Affects all users or critical systems; Regulatory, legal, or safety risk	Data platform down, breach of PHI, Data Ingestion Failure; Critical Data Quality failure
P2 – High	Major functionality impaired; Frequent disruptions to production; workaround exists but is inefficient	Significant user impact; Affects a major component of operations; Involves data integrity or performance degradation	API failure; Data sync errors. Monitoring and Alerting services not working; Power BI reports failure; Substantial query performance degradation
P3 – Medium	Minor functionality issue; workaround available	Moderate user impact; does not block core operations; affects efficiency or usability for some users	Report formatting issues, non-critical alerts, RBAC configuration issues; slow query performance; data sync lag;
P4 – Low	Cosmetic or enhancement request	No operational impact; background or planned task; UI updates, documentation changes, minor enhancements.	Label changes, tooltip updates, UI/UX changes, report updates, user documentation updates.

Table 7.18-1 Incident Prioritization Matrix

ATTACHMENT A: DEFINITIONS

- 1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
- 2) **Agency:** The term “Agency” within this RFP is referring to the North Carolina Department of Health and Human Services (NCDHHS). Synonymous with Department.
- 3) **Advanced Medical Home (AMH):** State-designated primary care practices that have been attested to meeting standards necessary to provide local care management services.
- 4) **Advanced Medical Home Plus (AMH+):** Primary care practices certified by the Department as AMH Tier 3 practices, whose providers have experience delivering primary care services to the eligible population or can otherwise demonstrate strong competency to serve that population and have certified by the State or Health Plan(s) as such.
- 5) **Adverse determination:** A final decision by the Department to deny, terminate, suspend, reduce, or recoup a Medicaid payment or to deny, terminate, or suspend a provider’s or applicant’s participation in the Medical Assistance Program.
- 6) **API:** Application Programming Interface - An interface that provides programmatic access to service functionality and data within an application or a database.
- 7) **Appeal:** Has the same meaning as appeal as defined in NCGS 108C-12.
- 8) **Applicant:** Supplier, bidder, proposer, firm, company, corporation, partnership, individual or other entity submitting an application in response to this RFP.
- 9) **Atypical providers:** Do not provide healthcare services and will not be issued NPI numbers. Are individuals or businesses that bill Medicaid for services rendered but do not meet the definition of a healthcare provider according to the NPI Final Rule 45 CFR 160.103
- 10) **Bidder’s Library:** A centralized collection of documents, data, and reference materials that the issuing organization provides to prospective bidders during the Request for Proposal (RFP) process. Its primary purpose is to give bidders access to relevant background information necessary to develop informed, accurate, and compliant proposals. The contents of the Bidder’s Library are provided solely for informational purposes and will not be included as part of the final contract. The content of the Bidder’s library reflects the current state of information at the time the RFP is issued and is not guaranteed to be updated throughout the procurement process.
- 11) **BAA:** Business Associate Agreement, as that term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).
- 12) **BAFO:** Best and Final Offer. Submitted by a Vendor to alter its initial offer, made in response to a request by the issuing agency.
- 13) **BCCP:** Business Continuity and Contingency Plans. These plans describe how a vendor’s solution will carry out normal business functions after an unplanned event.

- 14) **Behavioral Health and Intellectual/Developmental Disabilities Tailored Plan (TP or Tailored Plan):** Has the same meaning as Tailored Plan as defined in N.C.G.S. 108D-1(4). Under the initial term of the Tailored Plans contracts, Tailored Plans are operated by regional Local Management Entity/Managed Care Organizations (LME/MCOs).
- 15) **Beneficiary:** An individual eligible to receive services from the North Carolina Department of Health and Human Services, Division of Health Benefits (NC Medicaid).
- 16) **Best Value:** Has the same meaning as defined in N.C.G.S. 143-135.9.
- 17) **BPM:** Business Process Modeling. The activity of representing processes of an enterprise so they can be analyzed, improved, and automated.
- 18) **Business Associate:** A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing (see 45 CFR 160.103).
- 19) **Business Days and Business Hours:** Business days are Monday through Friday, excluding North Carolina state holidays. Business Hours are from 8:00 AM – 5:00 PM ET on Business Days. A list of North Carolina State Holidays is located at <https://oshr.nc.gov/state-employee-resources/benefits/leave/holidays>.
- 20) **Business Rules:** Documentation that defines or constrains how the PDM/CVO business operates. They are used to guide decision making, standardize processes, and maintain consistency.
- 21) **Business Rules Repository:** a centralized location and the “single source of truth” for storing all business rules
- 22) **BCP:** Business Continuity Plan. Plan to ensure that business processes continue during a time of emergency or disaster.
- 23) **Calendar Day:** A calendar day includes the time from midnight to midnight each day. It includes all days in a month, including weekends and holidays. Unless otherwise specified in this RFP, days means Calendar Days.
- 24) **CAP:** Corrective Action Plan - A written document describing the deliberate set of actions and steps to be taken by an entity to fix identified problems, errors, or non-compliance issues.
- 25) **Change Management Plan:** Plan defined to manage the changes while executing a project.
- 26) **Change Request:** Formal proposal for an alteration to some product or system.
- 27) **Children and Families Specialty Plan (CFSP):** Has the same meaning as defined in N.C.G.S. 108D-1(5a).
- 28) **CIHA:** Cherokee Indian Hospital Authority.
- 29) **“Clean” Applications (Provider):** Provider Applications that meet all rule standards provided by the Department with no adverse findings, includes those submitted with all required documentation and signatures present. This includes the payment of the Application fee.
- 30) **Clinically Integrated Network (CIN) or Other Partner:** Entities with which provider practices choose to partner to share responsibility for specific functions and capabilities required to operate as an AMH+ practice or CMA.

- 31) **Cloud-Based System:** A solution for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- 32) **CMS:** The Centers for Medicare & Medicaid Services. This is the agency within the United States Department of Health and Human Services that administers the Medicare program and works in partnership with state governments to administer Medicaid, Children's Health Insurance Program (CHIP), and health insurance portability standards.
- 33) **CMS Revalidation Date:** Due to the revalidation requirement defined in 42 CFR 455.414, the Department sets a "CMS revalidation date" to indicate the five-year deadline from the date of the previous NC Medicaid revalidation and uses that date as a basis to establish a timeline sufficient to allow for the full completion of the revalidation process prior to that deadline.
- 34) **Contract Effective Date:** The date the Department accepts the Vendor's proposal by signing the RFP Execution Page.
- 35) **Contractor:** The Vendor awarded the Contract to perform the services and requirements defined therein. Synonymous with Vendor or Offeror.
- 36) **COTS:** Commercial Off the Shelf. A ready-made solution that is adapted to the specific needs of the State's business.
- 37) **Communications Management Plan:** Policy-driven approach to providing stakeholders with information. The plan formally defines who should be given specific information, when that information should be delivered and what communication channels will be used to deliver the information.
- 38) **Configurable:** Within software development, the ability for a system to be modified without changing the underlying code base, such as by updating table values or setting parameters.
- 39) **CM:** Configuration Management. A systems engineering process for establishing and maintaining consistency of a products performance, functional and physical attributes with its requirements, design, and operational information throughout its life.
- 40) **Credentialing:** The approach to collecting and verifying provider qualifications (e.g., the provider's training and education, licensure, liability record); and determining, for Medicaid Managed Care and State-funded Services, whether to allow the provider to be included in a BH I/DD Tailored Plan's network, subject to certain Department requirements.
- 41) **Credentialing Committee:** The North Carolina (NC) Credentialing Committee ("Credentialing Committee") is a review body that performs the following functions: Reviews the credentials of individual and organization providers in medium-risk and high-risk categories as part of enrollment, re-enrollment, recredentialing, and ongoing monitoring. Enrollment/credentialing decisions for the identified providers to ensure quality of care to members.
- 42) **Credentialing Committee Bylaws:** Establish a comprehensive credentialing framework and delegates certain authority and powers to the Credentialing Committee to comply with all federal and North Carolina statutes, Medicaid and other payer policies, and the standards established by the National Committee for Quality Assurance (NCQA). These bylaws uphold the centralized credentialing of providers for contracting with managed care plans.
- 43) **Credentialing Committee Provider Designated Risk Levels:** Designation assigned to a provider's file to determine if review at the Credentialing Committee is required and level of review. Definitions are outlined in more detail in the bylaws. Clean File – no negative

findings. Low-Risk – Designation assigned to a provider’s file includes findings that were previously reviewed and approved. Medium Risk – Designation assigned to a provider’s file includes findings that are significant but have either occurred in the distant past or have been fully resolved. High-Risk – Designation assigned to a provider’s file includes findings that reflect serious or unresolved adverse actions where the State has discretionary authority to make a decision.

- 44) Cybersecurity Incident (NCGS 143B-1320):** An occurrence that:
- a. Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.
- 45) Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include “Work Product” and means any expression of Licensor’s findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.
- 46) Department:** State of North Carolina Department of Health and Human Services, which is responsible for managing the delivery of health and human related services for all North Carolinians, especially its most vulnerable citizens, which includes children, elderly, people with disabilities, and low-income families. Includes the Division of Health Benefits. Synonymous with Agency.
- 47) Dev:** Development, Referring to the Development stage of the Software Development Lifecycle.
- 48) DDI:** Design, Development, and Implementation is a phase in the project cycle.
- 49) DHB:** Division of Health Benefits. The division within the NCDHHS responsible for implementing Medicaid transformation and administering the transformed Medicaid program.
- 50) DHHS or NCDHHS:** The North Carolina Department of Health and Human Services. This department is responsible for managing the delivery of health and human related services for all North Carolinians, especially its most vulnerable citizens, which includes children, elderly, people with disabilities and low-income families. The Department works closely with health care professionals, community leaders and advocacy groups; local, state, and federal entities; and many other stakeholders. Synonymous with Agency and Department.
- 51) DMH/DD/SUS:** Division of Mental Health, Developmental Disabilities and Substance Use Services. This is a division within NCDHHS that provides quality support to achieve self-determination for individuals with intellectual and/or developmental disabilities and quality services to promote treatment and recovery for individuals with mental illness and substance use disorders.
- 52) DMBok:** Data Management Body of Knowledge. A collection of best practices and provides a common vernacular for managing data across an enterprise.
- 53) DPH:** Division of Public Health. The division within the NCDHHS responsible for promoting disease prevention, health services and health promotion programs that protect communities from communicable diseases, epidemics, and contaminated food and water.
- 54) DRP:** Disaster Recovery Plan

- 55) Eastern Band of Cherokee Indians (ECBI) Tribal Option:** PCCMe in NC. Managed Care Classification is Indian Managed Care Entity (IMCE). Operating authority is Cherokee Indian Hospital Authority (CIHA). The eligible population is Indian Health Services (IHS). Primarily service five counties (Cherokee, Graham, Haywood, Jackson, and Swain) but it is available in a total of 11 Western NC counties.
- 56) Encounters:** Medical information submitted by health care providers (physicians, hospitals, Ancillaries, etc.) which document both the clinical conditions, services, and items delivered to the member to treat their conditions.
- 57) EPS:** Encounter Processing System. The Encounter Processing System replaces the existing encounter capability within NCTracks. The EPS solution processes encounter claims for the NC MIMS within North Carolina's MES. The EPS modular component will incorporate, manage, and maintain encounter claim files information transmitted from PHPs to the State Medicaid Agency.
- 58) Enterprise Architecture Documentation:** Conceptual blueprint that defines the structure and operation of an organization.
- 59) Essential Providers:** A health care provider that serves high-risk, special needs, and underserved individuals, for NC Medicaid they are Federally qualified health centers, rural health centers, free clinics, local health departments, State Veteran's Homes, and any other providers as designated by the Department in accordance with N.C.G.S. § 108D-22(b).
- 60) FFP:** Federal Financial Participation. The Federal Government's share of a State's expenditures under the Medicaid program.
- 61) FFS:** Fee for Service. A system of payment where a physician or other health care provider is paid a fee for each service rendered. NC Medicaid's Fee for Service program is called Medicaid Direct.
- 62) FI:** Financial Institution. Any office of a bank, savings bank, card issuer as defined in section 103 of the Consumers Credit Protection Act (15 U.S.C. 1602(n)), industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.
- 63) GenAI:** Generative AI - A class of artificial intelligence systems designed to generate new content, such as text, images, audio, code, or structured data, based on patterns learned from large datasets. These systems use advanced machine learning models—most commonly large language models (LLMs) and multimodal neural networks—to produce outputs that resemble human created content.
- 64) Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of "goods" in the context of N.C.G.S. § 25-2-105 (UCC definition of goods).
- 65) HEDIS:** Healthcare Effectiveness Data and Information Set. Developed and maintained by the NCQA. HEDIS reporting is a requirement of health plans by NCQA and the Centers for Medicare and Medicaid Services (CMS) for use in health plan accreditation, Star Ratings, and regulatory compliance.
- 66) HIPAA:** Health Insurance Portability and Accountability Act of 1996, as amended and its promulgating regulations.
- 67) HITECH Act:** Health Information Technology for Economic and Clinical Health Act
- 68) IMS:** Integrated Master Schedule
- 69) Indian Health Care Provider (IHCP):** Means an IHCP as defined by 42 C.F.R. § 438.14(a). In North Carolina, an IHCP is a provider of service which includes all services that Cherokee Indian Hospital Authority or the Eastern Band of Cherokee Indians offer under Medicaid.

- 70) Informal Appeal:** Also referred to as Informal Reconsideration Reviews, The NCDHHS Hearing Office conducts impartial informal appeals regarding adverse determinations (e.g., Medicaid provider denial or enrollment termination) made by DHB or one of its agents or contractors.
- 71) Integration Testing:** This is performed when two or more units have been tested and are integrated into a single structure. It includes testing on the interfaces between the components and the larger structure. This level of testing is used to identify defects prior to SIT.
- 72) Interface Testing:** Interface testing is performed by the selected Vendor to ensure providers, EDI service centers, business partners, and other Department Vendors can submit transactions over appropriate channels and can send and receive proper acknowledgements and negative responses, including the testing of timeframes between the receipt of a transaction and the notification/response to the submitter for all modes of transmission. This includes any interfaces relating to external systems.
- 73) ITD:** Information Technology Division of the NC Department of Health and Human Services
- 74) ITSM:** Information Technology Service Management. The processes used to manage IT services within an organization.
- 75) IVRS:** Interactive Voice Response System. An automated telephony technology that enables humans to interact with a computer-operated phone system.
- 76) Key Personnel:** Any person performing under the Contract whose absence would cause an immediate and substantial risk to Vendor's ability to perform its obligation in the Contract as specified in the Vendor's offer.
- 77) LME/MCO:** Local Management Entity/Managed Care Organization. Has the same meaning as LME/MCO as defined in NCGS § 122C-3(20c). For the Medicaid population, these entities are recognized under CMS Medicaid Managed Care rules and are known as a Prepaid Inpatient Health Plans (PIHP) or Managed Care Organizations, depending on the contract. LME-MCOs also manage federal block grant, State, local and county funds for other behavioral health services.
- 78) Maintain Eligibility:** A process to identify providers who have had no claims activity in the past 12 months then notify the provider to submit a Maintain Eligibility Application. Providers who meet these criteria yet do not comply are terminated from Medicaid. This process is reliant on provider activity through FFS and encounter data activity. The purpose is to help reduce fraud, waste and abuse while ensuring only active, engaged providers remain enrolled.
- 79) Managed Care Organization (MCO):** Has the same meaning as MCO as defined in 42 C.F.R. § 438.2. Standard Plans (SP), BH I/DD Tailored Plans (TP), and the Children and Families Specialty Plan (CFSP) are operated by MCOs.
- 80) Managed Care Health Plan (Health Plan):** Includes a Managed Care Organization (MCO), Prepaid Inpatient Health Plan (PIHP), or Primary Care Case Management Entity (PCCM entity) as those terms are used and defined in 42 C.F.R. 438.2, and any Subcontractor or instrumentality of such entities that is engaged in the operation of a Medicaid Managed Care contract.
- 81) Medicaid Managed Care:** The name of the North Carolina managed care program for North Carolina Medicaid benefits under which contracted Managed Care Health Plans arrange for medical and other services to be delivered to Medicaid enrollees. Medicaid Managed Care will include three types of entities: (1) Managed Care Organizations (2) Prepaid Inpatient Health Plans (3) Primary Care Case Management Entities. In NC the Health Plans are: (1) Standard Plans, (2) BH I/DD Tailored Plans, (3) Children and Families Specialty Plan, and (4) Eastern Band of Cherokee Indians (EBCI) Tribal Option.

- 82) Medicaid Program:** The joint federal-state health insurance program for low-income individuals and families who cannot afford health care costs. Medicaid serves low-income parents, children, seniors, and people with disabilities.
- 83) Medicaid Enterprise System (MES):** The current approach to Medicaid management systems that promotes the use of COTS and SaaS products along with modularity and a higher degree of interoperability among systems. The aggregation of technologies and applications required to operate a State Medicaid Agency (SMA).
- 84) MES PMO:** Technology Program Management Organization comprised of the engineers, architects, specialist, analysts, project managers, program managers, and the Program Director for the MES project.
- 85) Managed File Transfer (MFT):** A technology platform that allows organizations to reliably exchange electronic data between systems and people in a secure way to meet compliance needs.
- 86) Medicaid Integration Services (MIS):** A platform that will provide module vendors with a common infrastructure, which may consist of State developed and third-party solutions and tools, to communicate and integrate using a consistent standards-based approach.
- 87) Medicaid Information Technology Architecture (MITA):** The initiative sponsored by the Center for Medicare and Medicaid Services (CMS) is intended to foster integrated business and IT transformation across the Medicaid enterprise to improve the administration of the Medicaid program.
- 88) Medicaid Management Information System (MMIS):** An integrated group of procedures and computer processing operations (subsystems) developed to help automate the management of a Medicaid program.
- 89) National Provider Identifier (NPI):** Standard unique health identifier for health care providers adopted by the Secretary of US Department of Health and Human Services in accordance with HIPAA.
- 90) NCAC:** North Carolina Administrative Code
- 91) NCCARE360:** An electronic platform providing: (a) a robust statewide resource repository of community-based organizations and social service agencies and the services they provide, and (b) a referral platform for payers, care managers, clinicians, community health workers, social service agencies, and others to refer and connect members directly to community resources and track the connections and outcomes through “closed loop referral” capacity. The platform is being deployed as part of a public-private partnership with the Foundation for Health Leadership and Innovation.
- 92) NCDIT or DIT:** The NC Department of Information Technology, formerly Office of Information Technology Services.
- 93) North Carolina electronic Vendor Portal (NC eVP):** North Carolina electronic Vendor Portal - The State of North Carolina’s on-line system for advertising solicitations, posting addendums, and publishing award notifications. Vendors can view and search for procurement opportunities <https://evp.nc.gov>.
- 94) North Carolina Families Accessing Services through Technology (NC FAST):** North Carolina Integrated eligibility system for public assistance services for Temporary Assistance for Needy Families (TANF), Medicaid, Child Care, Food and Nutrition Services (FNS)
- 95) North Carolina Identity Service (NCID):** The standard identity management service that allows State, local, business and citizen users to achieve an elevated degree of security and real-time access control to the State’s customer-based applications and information.

- 96) NCQA:** National Committee for Quality Assurance
- 97) NCTracks:** The Department's multi-payer Medicaid Management Information System (MMIS). NCTracks adjudicates claims for multiple NCDHHS divisions, including DHB, DMH/DD/SUS, Division of Public Health, and Office of Rural Health. NCTracks also serves as a central repository for Medicaid and State-funded Services Provider, Member and Recipient data.
- 98) N.C.G.S.:** North Carolina General Statutes
- 99) NC Medicaid Direct:** North Carolina's current health care program for Medicaid beneficiaries who are not enrolled in NC Medicaid Managed Care. It includes care management by Community Care of North Carolina (CCNC), the primary care case management entity for physical health services. Refers to the Medicaid Fee-For-Service program serving Beneficiaries who are not enrolled in a Prepaid Health Plan (PHP) or the EBCI Tribal Option.
- 100) Network (Provider):** A group of providers, including, without limitation, doctors, hospitals, pharmacies, and others contracted by the Health Plans to provide health care services to its Medicaid Managed Care members or State-funded Services recipients.
- 101) NIST:** National Institute of Standards and Technology
- 102) NPI:** National Provider Identifier. Standard unique health identifier for health care providers adopted by the Secretary of Health and Human Services in accordance with HIPAA.
- 103) Non-Participating Provider:** Non-participating or "non-par" providers are physicians or other health care providers that have not entered into a contractual agreement with a Health Plan and are not part of the Health Plan's Network, unlike participating providers. They may also be called out-of-network providers.
- 104) NPES:** National Plan and Provider Enumeration System, which is managed by the Centers for Medicare & Medicaid Services (CMS)
- 105) OBC:** Outcomes-Based Certification is CMS's new methodology of Medicaid Enterprise System certification based on the combination of developing outcomes statements and evaluation criteria, identifying test cases for system demonstrations, and collecting and assessing operational data.
- 106) OPR – Ordering Prescribing Referring**
- 107) ORR:** Operational Readiness Review
- 108) ORT:** Operational Readiness Testing ensures the application and infrastructure have been installed and configured for successful operation in the production environment prior to Go-Live.
- 109) Participating Provider:** Participating Provider or "par" providers are physicians or other health care providers that have a contractual agreement with a Health Plan and are included in the Health Plan's Network. Participating Providers may also be called "in-network providers".
- 110) Paypoint:** The secure payment solution provided by the NC Office of the State Controller Solutions for automated payments managing provider application fee transactions

- 111) Primary Care Case Management Entity (PCCMe):** Has the same meaning as Primary Care Case Management Entity as defined by 42 C.F.R. § 438.2. ECBI Tribal Option and Community Care of North Carolina function as a PCCMe.
- 112) PDM:** The provider data management component of the solution.
- 113) PDM/CVO:** Provider Data Management/Credentialing Verification Organization
- 114) Protected Health Information (PHI):** Has the same meaning as PHI as defined by 45 C.F.R. § 160.103.
- 115) Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- 116) Prepaid Health Plan (PHP):** Has the same meaning as Prepaid Health Plan, as defined N.C.G.S. 108D-1(30).
- 117) Prepaid Inpatient Health Plan (PIHP):** Has the same meaning as Prepaid Inpatient Health Plan as defined in 42 C.F.R. § 438.2.
- 118) PHP Contract Data Utility (PCDU):** A secure file transfer platform to allow for posting of Department guidance to the MES Vendor's and submission of key contract deliverables and reports by the PHPs for review and approval by the Department.
- 119) Project Management Office (PMO):** Project Management Office responsible planning, organizing and delineating responsibility for the completion of an organization's specific information technology (IT) goals.
- 120) Primary Care Provider (PCP):** The participating physician, physician extender (e.g., physician assistant, nurse practitioner, certified nurse midwife), or group practice/center selected by or assigned to the member to provide and coordinate all the member's health care needs and to initiate and monitor referrals for specialized services, when required.
- 121) Program Management:** The process of managing several related projects.
- 122) Proposal:** The response to the RFP solicitation submitted to NCDHHS by the Vendor. This is also referred to as the Response or Offer.
- 123) Provider:** Provider means any individual or entity that is engaged in the delivery of services, or ordering or referring for those services, and is legally authorized to do so by the State in which it delivers the services. (42 C.F.R. § 438.2).
- 124) Provider (For the purposes of credentialing):** Individual practitioners and facilities, entities, organizations, atypical organizations/providers, and institutions, unless otherwise noted.
- 125) Provider Contracting:** The process by which the Health Plan negotiates and secures a contractual agreement with providers who are credentialed providers and are to be included in the Health Plan's Network.
- 126) Provider Data Vendor:** Agency or organization that collects and distributes primary source verified provider information.
- 127) Provider Enrollment:** The process by which a provider is enrolled in the North Carolina's Medicaid or State-funded Services programs with credentialing as a component of enrollment. A provider who has enrolled in North Carolina's Medicaid program shall be referred to as a "Medicaid Enrolled provider" or an "Enrolled Medicaid provider." A provider who has enrolled in North Carolina's State-funded Services program shall be referred to as a "State-funded Services Enrolled provider" or an "Enrolled State-funded Services provider."

- 128) Provider Grievance:** Any oral or written complaint or dispute by a Provider over any aspects of the operations, activities, or behavior of the Health Plan except for any dispute over for which the provider has appeal rights.
- 129) RCA:** Root Cause Analysis
- 130) Real-time:** Real-time refers to the synchronous exchange of data between IT systems resulting in immediate access to or update of data on which resides in another IT system.
- 131) Requirements Management:** The process of documenting, analyzing, tracing, prioritizing, and agreeing on requirements and then controlling change and communicating to relevant stakeholders. It is a continuous process throughout a project.
- 132) Readiness Review:** Has the same meaning as described in 42 C.F.R. § 438.66(d).
- 133) Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
- 134) Recipient also referred to as Beneficiary:** Person enrolled in a participating Medicaid program.
- 135) RPO:** Recovery Point Objective – The maximum acceptable amount of data loss the Department can tolerate after a disruptive event, measured in time.
- 136) RTO:** Recovery Time Objective - The maximum acceptable amount of time it takes to restore a system or application to a functional state after an outage or disruption.
- 137) Regression Testing:** The objective of regression testing is to retest important functionality of the solution/system after changes have been made. This test is often performed after each build. Regression testing allows a consistent, repeatable validation of each new release of a modified system component or an MES component or COTS solution. This testing ensures reported defects have been resolved for each new release and that no new quality issues have been introduced in the maintenance process.
- 138) RFP:** Request for Proposal is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over \$10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services.
- 139) RBAC:** Role-Based Access Control. Restricts network access based on a user's role within an organization.
- 140) SaaS:** Software as a Service. A software licensing model, which allows access to software a subscription basis using external servers.
- 141) SDLC:** System Development Life Cycle. A project management model that outlines the phases required to build an IT system.
- 142) Security Monitoring Plan:** Plan that documents the collection, analysis, and escalation of indications and warnings to detect and respond to security intrusions.
- 143) Seven Standards and Conditions:** Centers for Medicare & Medicaid Services issued standards and conditions that must be met by the States if they have to be eligible for Medicaid technology investments, if they are to be eligible for the enhanced match funding. These standards and conditions have been issued under sections 1903(a) (3) (A) (i) and 1903(a) (3) (B) of the Social Security Act. Sections include modularity, MITA, industry standards, leverage, business results, reporting, and interoperability.

- 144) Severity Definitions:** The State reserves the right to adjust the severity level set by the Vendor to align with the State definitions as follows.
- a. Priority 1 – Critical (P1): A critical business function is not functional, there is no viable workaround, and the problem must be resolved immediately. This includes scenarios in which system performance is degraded to the point critical business functions cannot be completed even though the system is available.
 - b. Priority 2 – High (P2): A non-critical business function is not functional, there is no viable workaround, and the problem must be resolved immediately. This includes scenarios in which system performance is degraded to the point where non-critical business functions cannot be completed even though the system is available.
 - c. Priority 3 – Medium (P3): Impacted business function can function with a workaround, and the problem must be resolved as soon as possible.
 - d. Priority 4 – Low (P4): Impacted business function can function with a workaround, and the problem can be resolved when possible.
- 145) (Significant) Security Incident (NCGS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:
- a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
 - i. That is not relabel to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
 - ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.
 - b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.
- 146) SIT:** System Integration Testing. A high-level software testing process to verify that all related systems maintain data integrity and can operate in coordination with other systems in the same environment.
- 147) SLA:** Service Level Agreement. Part of a contract that defines what services a service provider will provide and the required level or standard for those services.
- 148) SPOC:** Single Point of Contact. A person serving as a coordinator or the focal point of information.
- 149) SAE 18 SOC 2 TYPE 2:** A detailed report on the controls of a service organization's systems used to process customer data and the confidentiality and privacy of the information processed by these systems. This report provides assurance of the security, availability, and process integrity of these systems.
- 150) SMA:** State Medicaid agency. State agency responsible for the distribution of Medicaid benefits.

- 151) State Contract Administrator:** A person who performs administrative functions related to dealing with contracts, like 1) request to bid, 2) evaluating bid, 3) allotment of contract, 4) Implementing contract, 5) measuring completed work, and 6) computing payments.
- 152) SMC:** Streamlined Modular Certification. CMS's methodology of Medicaid Enterprise System certification based on the combination of developing outcomes statements and evaluation criteria, identifying test cases for system demonstrations, and collecting and assessing operational data.
- 153) Standard Plan (SP):** has the same meaning as Standard Benefit Plan as defined by NCGS 108D-1(36).
- 154) State:** The State of North Carolina, the Department as an agency or in its capacity as the Using Agency.
- 155) State-funded Services:** Refers to State and non-Medicaid federally funded services for mental health, I/DD, TBI and substance use disorders.
- 156) Subcontractor:** An entity having an arrangement with the Vendor, where the Vendor uses the products and/or services of that entity to fulfill some of its obligations under the Contract. Use of a Subcontractor does not create a contractual relationship between the Subcontractor and the Department, only the Contractor.
- 157) System:** Information technology components for collecting, creating, storing, processing, and distributing information, typically including hardware, software, and data itself. Multiple systems may comprise a Solution.
- 158) Technical Specifications:** Means, as used herein, a specification that documents Documentation of the requirements of a system or system component. Typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance standards, or similar terms.
- 159) Turnover:** The transfer of care, custody and control of the application or service. This includes all software, product licenses, documentation, data, or other intellectual capital associated with the environment. Synonymous with Transition.
- 160) TBD:** To be Determined
- 161) Unit Testing:** The lowest testing level, which is used by developers to verify that the implemented code functions as expected.
- 162) Unintelligible Transmission:** Any file or data packet that does not conform with the format of the data exchange or interface, is not readable by the target systems due to a malformed file (i.e., corrupt data, xml that cannot be parsed, etc.) or is incomplete.
- 163) UAT:** User Acceptance Testing in which the system is opened for end users to test in a pseudo production environment. The end users verify the system functions according to all established specifications and that the infrastructure works within the defined constraints.
- 164) Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation. Synonymous with Contractor or Offeror.
- 165) VRAR:** Vendor Readiness Assessment Report, which is completed by the responding vendor, identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the Vendor to concisely identify whether an application or Vendor is achieving the most important State Moderate or low baseline requirements.

- 166) Warm Transfer:** Defined as a member or provider call is transferred directly from the original call center to the appropriate party during business hours without requiring the caller to make an additional call and without the vendor abandoning the call until the other party answers.
- 167) Work Breakdown Structure (WBS)** A deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables. It organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of the project work.
- 168) Work Product:** Incidental artifact created during the performance of the Contract. All work products created during the performance of the Contract become the property of the State.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

Section 1: General Terms and Conditions Applicable to All Purchases

1) DEFINITIONS: AS USED HEREIN:

Agreement means the Master Service Agreement in conjunction with any task order.

Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State in Section 2, Paragraph 2 of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

Services shall mean the duties and obligations undertaken by the Vendor under, and to fulfill, the specifications, requirements, terms and conditions of the Agreement, including, without limitation, providing web browser access by authorized users to certain Vendor databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.

State shall mean the State of North Carolina, the Department of Information Technology (DIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

- 2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.
- 3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.
- 4) **SUBCONTRACTING:** Reserved.
- 5) **TRAVEL EXPENSES: All travel expenses should be included in the Vendor's proposed hourly costs. Separately stated travel expenses will not be reimbursed.** In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.
- 6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.
- 7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Reserved.
- 8) **AVAILABILITY OF FUNDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 3: Availability of Funds.
- 9) **ACCEPTANCE PROCESS:**
 - The State shall have the obligation to notify Vendor, in writing ten calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.

- Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations. The State shall have the obligation to notify Vendor, in writing and within thirty (30) days following installation of any software deliverable if it is not acceptable.

Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.

The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

10) **PAYMENT TERMS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 35: Payment and Invoice Terms.

11) **EQUAL EMPLOYMENT OPPORTUNITY:** Reserved.

12) **ADVERTISING/PRESS RELEASE:** Reserved

13) **LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.

14) **ACCESS TO PERSONS AND RECORDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 1: Access to Persons and Records.

15) **ASSIGNMENT:** Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty

(30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

16) **INSURANCE COVERAGE:** Reserved.

17) **DISPUTE RESOLUTION**: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) **CONFIDENTIALITY**: In accordance with N.C.G.S. §143B-1350I and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq.* Such information may include trade secrets defined by N.C.G.S.

§66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

- a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.
- b) Vendor warrants that all its employees and any approved third-party Vendor or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq.* The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS

Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.

- c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
- d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
- e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.
- c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

- d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9 of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) WAIVER OF DEFAULT: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate the Agreement by written agreement at any time.
- b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, as provided for in 9 NCAC 6B .1030 subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part, by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.
 - iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.

22) LIMITATION OF VENDOR'S LIABILITY:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (v) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the Agreement, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 34: Time is of the Essence.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or

time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

- 26) **INDEPENDENT CONTRACTORS:** Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Contractors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.
- 27) **TRANSPORTATION:** Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.
- 28) **NOTICES:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 20: Notices.
- 29) **TITLES AND HEADINGS:** Titles and Headings in the Agreement are used for convenience only and do not define, limit, or proscribe the language of terms identified by such Titles and Headings.
- 30) **AMENDMENT:** The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.
- 31) **TAXES:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 33: Taxes
- 32) **GOVERNING LAWS, JURISDICTION, AND VENUE:**
- a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina and stipulates that Wake County shall be the proper venue for all matters.
 - b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.
- 33) **FORCE MAJEURE:** Neither Party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.
- 34) **COMPLIANCE WITH LAWS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 7: Compliance with Laws.

- 35) SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.
- 36) CHANGES:** The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The Department shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.
- 37) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.
- 38) ELECTRONIC PROCUREMENT: (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document):** Purchasing shall be conducted through the Statewide E-Procurement Services. The Department's third-party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.
- a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E- Procurement Service.** This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement. Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.
 - b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier

Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.

- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership, or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the Security Breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any Security Breach.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

- e) Vendor has created, acquired, or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire, or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general-purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title, and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data, or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become non-infringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the

Vendor agrees to take back any goods/hardware or software and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.

- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS: In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

- a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.
- b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
- c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.
- d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.
- e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - i) Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - ii) Terminate the work authorization, or
 - iii) Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.

- iv) The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER: The Department may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

- a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.
- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

42) TRANSITION ASSISTANCE

- a) If the Contract is not renewed at the end of the Contract Term, or is terminated prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or Termination of the Contract, all reasonable transition assistance to include at a minimum: A list of vendor coordination activities that will occur during the turnover task and implementation of the activities to ensure continued system and services as deemed necessary by the Department. All re-useable artifacts, a list of incomplete tasks, such as system defects, modifications or enhancements, reference updates, and configuration requests. A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The description shall also include an estimate of the number and type of personnel required to support the technical platform and supporting services. The data and documentation shall be organized in a format required by the State (e.g., by provider unique ID and provider name). The conversion and migration of all pertinent information and work in progress, leases, etc. requested by the State, to allow

for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. The vendor must destroy all confidential state data it holds.

- b) Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Contract, (not withstanding this expiration or termination) except for those Vendor terms or conditions that do not reasonably apply to such transition assistance.
- c) The Department shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Contract for performance.
- d) If the Department terminated the Contract for cause, then the State will be entitled to offset the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the Department may have otherwise accrued as a result of said cancellation.

Section 2: Terms and Conditions Applicable to Information Technology Goods and Services

- 1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:** Deliverables comprising goods, equipment or products (hardware) may contain software for internal operation, or as embedded software or firmware that is generally not sold or licensed as a severable software product. Software may be provided on separate media, such as a CD-ROM or other media, or may be included within the hardware at or prior to delivery. Such software is proprietary, copyrighted, and may also contain valuable trade secrets and may be protected by patents. Vendor grants the State a license to use the Code (or any replacement provided) on, or in conjunction with, only the Deliverables purchased, or with any system identified in the solicitation documents. The State shall have a worldwide, nonexclusive, non-sublicensable license to use such software and/or documentation for its internal use. The State may make and install copies of the software to support the authorized level of use. Provided, however, that if the hardware is inoperable, the software may be copied for temporary use on other hardware. The State shall promptly affix to any such copy the same proprietary and copyright notices affixed to the original. The State may make one copy of the software for archival, back-up or disaster recovery purposes. The license set forth in this Paragraph shall terminate immediately upon the State's discontinuance of the use of all equipment on which the software is installed. The software may be transferred to another party only with the transfer of the hardware. If the hardware is transferred, the State shall i) destroy all software copies made by the State, ii) deliver the original or any replacement copies of the software to the transferee, and iii) notify the transferee that title and ownership of the software and the applicable patent, trademark, copyright, and other intellectual property rights shall remain with Vendor, or Vendor's licensors. The State shall not disassemble, decompile, reverse engineer, modify, or prepare derivative works of the embedded software, unless permitted under the solicitation documents.
- 2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:
 - a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Scope of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data

source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. This license shall be for the term of the contract , unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any Department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.

- b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.
- c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
- d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.

3) WARRANTY TERMS: Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.

- a. Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.
- b. Vendor warrants to the best of its knowledge that:
 - i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
 - iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.
- c. UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.

4) RESTRICTIONS: State's use of the Software is restricted as follows:

- a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.
- b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
- c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
- d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

5) SUPPORT OR MAINTENANCE SERVICES: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:

- a) **Error Correction:** If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.
- b) **Other Agreement:** This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
- c) **Temporary Extension of License:** If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
 - i) Return of the inoperative CPU to full operation, or
 - ii) Termination of the license.
- d) **Encryption Code:** Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
- e) **Updates:** Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no

additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.

- f) **Telephone Assistance:** Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 8:00 AM - 5:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) hours or eight (8) hours or next business day, etc. *(edit this time to what you want your response time to be)*, for calls made at any time.

- 6) **STATE PROPERTY AND INTANGIBLES RIGHTS:** The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data, and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 3: Terms and Conditions Applicable to Personnel and Personal Services

- 1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third-party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third-party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).
 - a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
 - b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the

Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.

- c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.

2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Scope of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement"). (Reserve if not needed).

3) **PERSONNEL:** Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be notified to the Agency's Contract Administrator in writing accompanied by the names, roles, resume and references of Vendor's recommended substitute personnel. *Within ten (10) calendar days of the request for a substitution, the State will notify the Vendor if the recommended substitute is acceptable. If the State does not accept the recommended substitute, the Vendor will have ten (10) calendar days to make another recommendation.* The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.

- a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.
- b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular workdays and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
- c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications, or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
- d) At no time may the Key Personnel Role be vacant. It is the Vendor's responsibility to keep the role filled until the Department approves a substitution.

4) **PERSONAL SERVICES:** Reserved

Section 4: Software as a Service (SaaS) Terms and Conditions (Only Applies to Proposed SaaS Solutions)

1) DEFINITIONS:

Data means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

Support includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) ACCESS AND USE OF SAAS SERVICES:

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made

generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

- d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
- h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
- i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.

3) WARRANTY OF NON-INFRINGEMENT; REMEDIES:

- a) Vendor warrants to the best of its knowledge that:
 - i) The services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
- b) Reserved
- c) Reserved
- d) Reserved

4) ACCESS AVAILABILITY; REMEDIES

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services. The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.

b) Reserved

5) EXCLUSIONS:

- c) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- d) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or services failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services

6) PERFORMANCE REVIEW AND ACCOUNTABILITY: N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) LIMITATION OF LIABILITY: LIMITATION OF VENDOR'S CONTRACT DAMAGES LIABILITY: See Attachment B: Agency Terms and Conditions, Section 1, Paragraph 22: Limitation of Vendor's Liability.

8) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY: See Attachment B: Agency Terms and Conditions, Section 1, Paragraph 23: Vendor's Liability for Injury to Persons or Damage to Property.

9) MODIFICATION OF SERVICES: If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.

10) TRANSITION PERIOD:

- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
 - f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 5: Travel Expenses.
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 23: Prohibition Against Contingent Fees and Gratuities.
- 14) **AVAILABILITY OF FUNDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 3: Availability of Funds.
- 15) **PAYMENT TERMS (APPLICABLE TO SAAS):**
- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
 - b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.

- c) For any third-party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State. product
 - d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
 - e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.
- 16) **ACCEPTANCE CRITERIA:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 9: Acceptance Process.
- 17) **CONFIDENTIALITY:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 18: Confidentiality.
- 18) **SECURITY OF STATE DATA:**
- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The service provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any Security Breaches within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security control appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the service provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75- 65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and

- (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75- 60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally

required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, another related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - i) The scale and quantity of the State Data loss;
 - ii) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - iii) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - iv) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

- o) Secure Data Disposal: When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

ATTACHMENT C: AGENCY TERMS AND CONDITIONS

Section 1: NCDHHS Department of Health Benefits (DHB)

1) ACCESS TO PERSONS AND RECORDS

- a. Pursuant to N.C.G.S. § 147-64.7 and N.C.G.S. § 143-49(9), the Department, the State Auditor, appropriate State or federal officials, and their respective authorized employees or agents shall have access to persons and premises, or such other locations where duties under the Contract are being performed, and are authorized to inspect, monitor, or otherwise evaluate all books, records, data, information, systems, and accounts of the Contractor, their Subcontractor(s), other persons directed by the Contractor, or Contractor's parent or affiliated companies as far as they relate to transactions under the Contract, performance of the Contract, or to costs charged to the Contract. The Contractor shall retain any such books, records, data, information, and accounts in accordance with Section 1, Paragraph 24, RECORD RETENTION of this Attachment C of the Contract. Changes or additional audit, retention or reporting requirements may be imposed by federal or state law and/or regulation, and the Contractor must adhere to such changes or additions.
- b. The State Auditor shall have access to persons and records as a result of all contracts or grants entered by State agencies or political subdivisions in accordance with N.C.G.S. § 147-64.7.
- c. The financial auditors of the Department shall also have full access to all financial records and other information determined by the Department to be necessary for the Department's substantiation of the monthly payment(s). These audit rights are in addition to any audit rights any federal agency may have regarding the use of federally allocated MFP funds.
- d. The following entities may audit the records of this Contract during and after the term of the Contract to verify accounts and data affecting fees or performance:
 - i. The State Auditor;
 - ii. The internal auditors of the affected department, agency or institution; and
 - iii. The Joint Legislative Commission on Governmental Operations and legislative employees whose primary responsibility is to provide professional or administrative services to the Commission.
- e. Nothing in this section is intended to limit or restrict the State Auditor's rights.
- f. This provision shall survive termination or expiration of this Contract.

2) ADVERTISING

Contractor agrees not to use the existence of this Contract or the name of the Department or State of North Carolina as part of any commercial advertising or marketing of its products or services, excepted as permitted under this Contract. A Contractor may inquire

whether the Department is willing to act as a reference by providing information directly to other prospective customers. The Department is under no obligation to serve as a reference.

3) AVAILABILITY OF FUNDS

All payments to Contractor are expressly contingent upon and subject to the appropriation, allocation, and availability of funds to the Department for the purposes set forth in the Contract. If the Contract or any purchase order issued hereunder is funded in whole or in part by federal funds, the Department's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Contract or purchase order. If the term of the Contract extends into fiscal years after that in which it is approved, such continuation of the Contract is expressly contingent upon the appropriation, allocation, and availability of funds by the N.C. General Assembly for the purposes set forth in this RFP and any resulting Contract. If funds to effect payment are not available, the Department will provide written notification to the Contractor and may terminate the Contract in accordance with TERMINATION of this Section 21 of Attachment. D. of the Contract. If the Contract is terminated, the Contractor agrees to take back any affected deliverables and software not yet delivered under the Contract, terminate any Services supplied to the Department under the Contract, and relieve the Department of any further obligation thereof. The Department shall remit payment for deliverables and services accepted prior to the date of the previously mentioned notice in conformance with the payment terms.

4) BACKGROUND CHECKS AND DISCLOSURE OF LITIGATION AND CRIMINAL CONVICTION AND ADVERSE FINANCIAL CONDITION

The Contractor's failure to fully and timely comply with the terms of this Sections 7.7, 7.8, and 7.9 herein including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Contract and result in Termination for Cause.

- a. Upon execution of this Contract, the Contractor shall notify the State if it, or any of its Subcontractors, or their officers, directors, or their Key Personnel, who may provide services under this Contract, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation, or deception. The Contractor shall promptly notify the Department of any criminal litigation, investigations or proceeding involving the Contractor or any Subcontractor, or any of the foregoing entities' then current officers or directors during the term of this Contract.
- b. The Contractor shall notify the State of any civil litigation, regulatory finding or penalty, arbitration, proceeding, or judgments against it or its Subcontractors during the three (3) years preceding the Effective Period Commencement Date of the Contract, or which may occur during the term of this Contract that involves (1) services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Contractor; and (2) a claim or written allegation of fraud by the Contractor or any Subcontractor hereunder, arising out of their business activities; and (3) a claim or written allegation that the Contractor or any Subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Contractor or its Subcontractors shall be disclosed to the Department to the extent they affect the financial solvency and integrity of the Contractor or Subcontractor.
- c. Contractor agrees not to use any personnel in the performance of this Contract who have been convicted of any of the crimes listed in subpart a. herein above. In addition, Contractor will not use or authorize any Subcontractor to use in the performance of this Contract

any persons who have been convicted of any federal or state crime involving antitrust laws, anti-kickback laws, self-referral laws, improper influencing of public officials, or improper management or destruction of public records or financial records.

- d. The Contractor shall notify the State of any legal action that could adversely affect the Contractor's ability to meet the requirements of the Contract.
- e. All notices under subsection a., b., c., and d. herein shall be provided in writing to the State within thirty (30) Calendar Days after the Contractor learns about any such criminal, regulatory, or civil matters or financial circumstances or material change to prior disclosures, unless such matters are governed by the other stated terms and conditions of the Contract. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Contractor may rely on good faith certifications of its Subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.
- f. The Department reserves the right to request a criminal background check on Contractor's employees or independent contractors or the employees of Contractor's approved Subcontractors.
- g. Where requested by the Department, Contractor must obtain, at its own expense, and provide the Department, or its designee, a North Carolina State Bureau of Investigation (SBI) and/or Federal Bureau of Investigation (FBI) background check on all employees prior to assignment.
- h. Contractor shall keep any records related to these verifications in accordance with Section 1, Paragraph 24, **RECORD RETENTION** of this Attachment C. of the Contract.

5) BENEFICIARIES

The Contract shall inure to the benefit and be binding upon the Parties and their respective successors. It is expressly understood and agreed that the enforcement of the Terms and Conditions of the Contract, and all rights of action relating to such enforcement, shall be strictly reserved to the Department and Contractor. Nothing contained in this Contract shall give or allow any claim or right of action whatsoever by any third person. It is the express intention of the Department and Contractor that any such other person or entity receiving services or benefits under the Contract shall be deemed an incidental beneficiary only and not a contractual third-party beneficiary.

6) CHANGE IN CORPORATE STRUCTURE

The Contract shall inure to the benefit and be binding upon the Parties and their respective successors. It is expressly understood and agreed that the enforcement of the Terms and Conditions of the Contract, and all rights of action relating to such enforcement, shall be strictly reserved to the Department and Contractor. Nothing contained in this Contract shall give or allow any claim or right of action whatsoever by any third person. It is the express intention of the Department and Contractor that any such other person or entity receiving services or benefits under the Contract shall be deemed an incidental beneficiary only and not a contractual third-party beneficiary.

7) COMPLIANCE WITH LAWS

- a. Contractor shall comply with all applicable federal and state laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and performance in accordance with this Contract.

- b. Contractor is responsible for ensuring its Subcontractors comply with all laws, rules, regulations, and licensing requirements applicable to Contractor's performance under this Contract, including but not limited to the applicable provisions of (a) Title XIX of the Social Security Act and Titles 42 and 45 of the Code of Federal Regulations,; and (b) those laws, rules, or regulations of federal and State agencies having jurisdiction over the subject matter of this Contract, whether in effect when this Contract is signed, or becoming effective during the term of this Contract.
- c. Clean Air Act
 - i. Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
 - ii. Contractor agrees to report each violation to the Department and understands and agrees that the Department will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
 - iii. Contractor agrees to include these requirements in each subcontract exceeding one hundred fifty thousand dollars (\$150,000) financed in whole or in part with Federal assistance.
- d. Federal Water Pollution Control Act
 - i. Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
 - ii. Contractor agrees to report each violation to the Department and understands and agrees that the Department will, in turn, report each violation as required to assure notification to the federal agency providing funds hereunder, and the appropriate Environmental Protection Agency Regional Office.
 - iii. Contractor agrees that these requirements will be included in each subcontract exceeding one hundred fifty thousand dollars (\$150,000) financed in whole or in part with Federal assistance.
- e. Pandemic, Endemic and Other North Carolina State Emergencies
 - i. Contractor agrees to comply with all applicable standards, Executive Orders and Department issued guidance for pandemics, endemics, and other North Carolina State emergencies.
 - ii. Notice shall be provided by the Department of the standards, orders and Department issued guidance prior to the Effective Date of the requirements, where practical.
 - iii. In the event requirements are announced and made effective immediately, such as Executive Orders, the Contractor shall adhere to such requirements.
 - iv. Contractor agrees to communicate to Subcontractors for compliance with all applicable standards, orders, and Department-issued guidance.
- f. Certifications and Representations
 - i. Contractor shall certify annually pursuant to C.F.R. § 200.209 Certifications and Representations that it is in compliance with federal certification and representation requirements regarding Nondiscrimination, Drug-Free Workplace Requirements,

Environmental Tobacco Smoke, Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier Covered Transactions and Lobbying.

- ii. Contractor shall certify annually that is in compliance with state certification requirements regarding Verification of Employee Work Authorization, Ineligibility, Prior Convictions and Prior Employment.

8) CONTRACT ADMINISTRATORS

Contract Administrators means the persons to whom notices provided for in this Contract shall be given, and to whom matters relating to the administration of this Contract shall be addressed. Contract Administrators for both Parties are included in Attachment M: Contract Administrators. Either Party may change its administrator or their address and telephone number by written notice to the other Party in accordance with **NOTICES** of this Attachment C of the Contract.

9) CONTRACT DISCLOSURES

Unless otherwise provided herein, Contractor shall complete any initial disclosures required under the Contract within thirty (30) Calendar Days of execution unless another timeframe is approved by the Department. Disclosures should be sent to the Department's Contract Administrator in accordance with **NOTICES** of this Attachment C of the Contract.

10) COOPERATION WITH OTHER STATE VENDORS

Contractor shall cooperate with Department Vendors that are providing goods or services to or on behalf of the Department in relation to Medicaid including those Vendors providing services with respect to system integration, encounter processing, enrollment and eligibility, data analytics, and those engaged by the Department to monitor, validate, or verify Contractor's performance.

11) COUNTERPARTS

This Contract may be executed in two (2) or more counterparts, each, and all of which shall be deemed an original and all of which together shall constitute but one and the same instrument. Any signature page transmitted by electronic mail in portable document format will have the same legal effect as an original executed signature page.

12) RESERVED

13) DISCLOSURE OF CONFLICTS OF INTEREST

The Contractor shall disclose any known conflicts of interest, or perceived conflicts of interest, at the time they arise, as follows:

- a. Disclose any relationship to any business or associate to whom the Contractor is doing business that creates or may give the appearance of a conflict of interest related to this Contract.
- b. By signing the RFP, Contractor certifies that it shall not knowingly take any action or acquire any interest, either directly or indirectly, that will conflict in any manner or degree with the performance of its services during the term of the Contract.
- c. Disclose prior to employment or engagement by the Contractor, any firm principal, staff member or Subcontractor, known by the Contractor to have a conflict of interest or potential conflict of interest related to this Contract.

- d. All notices required by this subsection must be provided to the Department within thirty (30) Calendar Days of Contractor becoming aware of the conflict.

14) ENTIRE AGREEMENT AND ORDER OF PRECEDENCE

This Contract consists of the following documents incorporated herein by reference:

- a. Any amendments, business requirements, or implementation plans, executed by the Parties, in reverse chronological order;
- b. Execution of Contract, if any;
- c. Best and Final Offers and negotiation documents, in reverse chronological order, if any;
- d. Written clarifications, in reverse chronological order, if any;
- e. Addenda to the RFP, in reverse chronological order, if any;
- f. This RFP in its entirety; and
- g. Offeror's proposal

In the event of a conflict between the Contract documents, the term in the Contract with the highest precedence shall prevail. The Contract documents constitute the entire agreement between the parties and supersede all prior oral or written statements or agreements

15) RESERVED

16) RESERVED

17) INDEMNIFICATION

- a. Contractor shall hold and save the State, its officers, agents, and employees, harmless from liability of any kind, including all claims and losses accruing or resulting to any other person, firm, or corporation furnishing or supplying work, services, materials, or supplies in connection with the performance of this Contract, and from any and all claims and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or intentionally tortious acts of Contractor.
- b. Contractor represents and warrants that it shall make no claim of any kind or nature against the State's agents who are involved in the delivery or processing of Contractor goods and/or services to the State. The representations and warranties in the preceding sentences shall survive the termination or expiration of this Contract. The State, Department, and/or Office of the Attorney General shall have the option to participate at their own expense in the defence of such claim(s) or action(s) filed, and the State shall be responsible for its own litigation expenses if it exercises this option.
- c. Contractor shall hold and save the Department, State, its officers, agents, and employees, harmless from liability of any kind, including costs and expenses, resulting from infringement of the rights of any third party in any copyrighted material, patented or unpatented

invention, articles, device, or appliance delivered relating to this Contract. This provision shall survive the termination or expiration of this Contract.

- d. Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity that otherwise would be available to the Department and State under applicable law.

18) **INSURANCE**

During the term of the Contract, the Contractor, at its sole cost and expense, shall provide commercial insurance coverage of such type and with such terms and limits as may be reasonably associated with the Contract. At a minimum, the Contractor shall provide and maintain the following coverage and limits:

- a. **Worker's Compensation**: The Contractor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of five hundred thousand dollars (\$500,000), covering all of Contractor's employees who are engaged in any work under the Contract. If any work is sublet, the Contractor shall require the Subcontractor to provide the same coverage for any of his employees engaged in any work under the Contract.
- b. **Commercial General Liability**: General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of two million dollars (\$2,000,000) Combined Single Limit.
- c. **Automobile**: Automobile Liability Insurance, to include liability coverage, covering all owned, hired, and non-owned vehicles, used relating to the Contract. The minimum combined single limit shall be five hundred thousand dollars (\$500,000) for bodily injury and property damage; five hundred thousand dollars (\$500,000) for uninsured/under insured motorist; and five thousand dollars (\$5,000) for medical payment.
- d. **Requirements**: Providing and maintaining adequate insurance coverage is a material obligation of the Contractor and is of the essence of this Contract. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Contractor shall always comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or this Contract. The limits of coverage under each insurance policy maintained by the Contractor shall not be interpreted as limiting the Contractor's liability and obligations under the Contract.

19) **MEDIA CONTACT APPROVAL AND DISCLOSURE**

Contractor shall not use the name or seal of the North Carolina Division of Health Benefits, the North Carolina Department of Health and Human Services or the State of North Carolina in any media release or public announcement or disclosure relating to the terms of this Contract without prior approval of the Department. Contractor shall not provide any information to the media regarding a recipient of services under this Contract without first receiving approval from the Department. In the event the Contractor is contacted by the media for information related to the terms of this Contract, the Contractor shall contact the Department as soon as practical. Contractor must

submit any proposed media release regarding the terms of this Contract to the Department for review and approval at least seven (7) State Business Days in advance of intended disclosure, to the extent practicable. The Department may, to the extent reasonable and lawful, timely object to its publication or require changes to the information intended for public release. The requirements of this Section shall not apply to any information the Contractor is required by law or by any court of competent jurisdiction to disclose.

20) NOTICES

Any notices permitted or required under the Contract must be delivered to the appropriate Contract Administrator for each Party. Unless otherwise specified in the Contract, any notices shall be in writing and **delivered by email**. In addition, notices may be delivered by first class U.S. Mail, commercial courier (e.g., FedEx, UPS, DHL), or personally delivered provided the notice is also emailed to the Contract Administrator at approximately the same time. All Notices required under this Contract including, but not limited to legal matters, contract termination, allegations of breach, and audits shall be delivered in accordance with this section of the Contract.

21) OUTSOURCING

Any Contractor or Subcontractor providing call or contact center services to the State of North Carolina or any of its agencies shall disclose to inbound callers the location from which the call or conduct center services are being provided. If, after award of a contract, the Contractor wishes to relocate or outsource any portion of performance to a location outside of the United States, or to contract with a Subcontractor for any such performance, which Subcontractor and nature of the work has not previously been disclosed to the State in writing, prior written approval must be obtained from the State agency responsible for the contract. Contractor shall give notice to the using agency of any relocation of the Contractor, employees of the Contractor, or other persons providing performance under a State contract to a location outside of the United States.

22) OWNERSHIP OF DELIVERABLES

All project materials, including deliverables, software, data, and documentation created during the performance or provision of services hereunder that are not licensed to the Department or other State entity, or are not proprietary to the Contractor are the property of the Department and must be kept confidential or returned to the Department, or destroyed. Proprietary Contractor materials shall be identified to the Department by the Contractor prior to use or provision of services hereunder and shall remain the property of the Contractor. Derivative works of any Contractor proprietary materials prepared or created during the performance of provision of services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the Department and the State. This term shall survive termination or expiration of the Contract.

23) PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES

Contractor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for obtaining any Contract or award issued by the State and its Departments and other agencies or entities. The Contractor further warrants that no commission or other payment has been or will be received from or paid to any third-party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the Department in writing prior to acceptance of the Contract or award in question. The Contractor and its authorized signatory further warrant that no officer or employee of the State has any direct

or indirect financial or personal beneficial interest, in the subject matter of the Contract; obligation or Contract for future award of compensation as an inducement or consideration for making the Contract. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for termination of all outstanding contracts. Violations of this provision may result in debarment of the Contractor as permitted by 09 NCAC 06B.1206, 01 NCAC 05B.1520, or other provision of law.

24) RECORD RETENTION

All records and data held by the Contractor as it relates to this Contract shall be retained and maintained as required by North Carolina law, federal law, State and Department Record Retention requirements and policies.

- a. All records created or modified by the Contractor and not duplicated in Department system via interfaces must be retained for ten (10) years, unless a longer or shorter period is required by federal or State law or policy. Federal record retention standards are located in 45 C.F.R. § 74.53. The State policy is mandated by the State Archives of North Carolina.
- b. Records shall not be destroyed, purged, or disposed of without the express written consent of the Department.
- c. If any litigation, claim, negotiation, audit, disallowance action or other action involving this Contract starts before the expiration of the legally required retention period, the records must be retained until completion of the action and resolution of all issues which arise from it.
- d. In the event there are changes in record retention requirements or policies due to North Carolina law, federal law, State or Department record Retention Policies, the Contractor shall make the necessary changes to be in compliance with all Records Retention requirements.
- e. Record Retention requirements included within the body of this Contract, subsequent contracts and amendments are intended to supplement this term. In the event of conflict, the provisions of this term are the controlling requirements.
- f. At the point the Contract terminates/expires, all data must be transitioned to the State in a format prescribed by the Department unless that data has exceeded its archive requirements. The Department may request verification from the Contractor that archive requirements are being met.
- g. This term survives termination or expiration of the Contract.

25) RESPONSE TO STATE INQUIRIES AND REQUESTS FOR INFORMATION

The Contractor shall prioritize requests from the Department to respond to inquiries from any Departments under the State of North Carolina, the North Carolina General Assembly or other government agencies or bodies. Contractor shall respond to urgent requests from the Department within twenty-four (24) hours and according to the guidance and timelines provided by the Department.

26) RIGHT TO PUBLISH - RESERVED

27) SEVERABILITY

If a court of competent authority holds that a provision or requirement of the Contract violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Contract shall remain in full force and effect.

28) SOVEREIGN & GOVERNMENTAL IMMUNITY

Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity that otherwise would be available to the Department and State under applicable law. Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of governmental immunity that otherwise would be available to the Contractor under applicable law against a third party.

29) RESERVED

30) SUBCONTRACTORS

- a. Unless otherwise notified by the Department, acceptance of Contractor's proposal includes any Subcontractor(s) specified therein.
- b. Work performed under this Contract by the Contractor or its employees shall not be subcontracted without prior written approval of the Department. Contractor must submit a written request for approval in accordance with **NOTICES** of this Attachment C of the Contract at least thirty (30) Calendar Days prior to the anticipated start of services by the Subcontractor. Any request for Subcontractor approval shall include a completed *Attachment N: Subcontractor Identification Form*.
- c. Upon request and within five (5) State Business Days of such request, Contractor shall provide the Department with complete copies of any contracts made by and between the Contractor and any Subcontractors. The Contractor remains solely responsible for the performance of its Subcontractors. Subcontractors, if any, shall adhere to the same standards required of the Contractor and this Contract. Any contracts made by the Contractor with a Subcontractor shall include an affirmative statement that the Department is an intended third-party Beneficiary of the Contract; that the Subcontractor has no contract with the Department; and that the Department shall be indemnified by the Contractor for any claim presented by the Subcontractor. Notwithstanding any other term herein, Contractor shall timely exercise its contractual remedies against any non-performing subcontractor and, when deemed appropriate by the Department, substitute another Subcontractor.
- d. The Contractor shall neither participate with nor enter into any agreement with any individual or entity that has been excluded from participation in federal health care programs or has been debarred from doing business with the State of North Carolina.
- e. Any contract(s) between the Contractor and Subcontractor(s) require:
 - i. The Subcontractor to agree that the State, CMS, the NCDHHS Inspector General, the US Comptroller General, or their designees have the right to audit, evaluate, and inspect its premises, any books, records, contracts, computer or other electronic systems of the Subcontractor relating to its Medicaid enrollees, or of the Subcontractor's contractor, that pertain to any aspect of services and activities performed, or determination of amounts payable under the Contractor's contract with the State;

- ii. The Subcontractor to agree that the right to audit by the State of North Carolina, the NCDHHS Inspector General, the US Comptroller General or their designees, will exist through ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later; and
- iii. That if the State, CMS or the NCDHHS Inspector General determine that there is a reasonable possibility of fraud or similar risk, the State, CMS or the NCDHHS Inspector General may inspect, evaluate, and audit the Subcontractor at any time.

31) SUBSTANCE USE DATA (42 C.F.R. PART 2)

Contractor is fully bound by the provisions of 42 C.F.R. Part 2 upon receipt of data from DHB that includes Patient Identifying Information (PII) regarding substance use disorder, as those terms are defined by 42 C.F.R. 2.11. Contractor shall implement appropriate safeguards to prevent the unauthorized uses and disclosures of data protected under 42 C.F.R. Part 2. Contractor shall report any unauthorized uses, disclosures, or breaches of data subject to this term and condition, to the Contract Administrators for DHB within three (3) Calendar Days of the unauthorized use, disclosure, or breach. This notice is in addition to any other notice requirement regarding unauthorized disclosure of PII or PHI required by the Contract. Information disclosed to Contractor is limited to that which is necessary for the Contractor to perform its duties under the Contract. Contractor shall not re-disclose information to a third party unless that third party is a contract agent of the Contractor or subcontractor, helping to provide services described in the contract and only if the subcontractor only further discloses the information back to the contractor or lawful holder from which the information originated.

32) SURVIVAL

The expiration, termination, or cancellation of this Contract will not extinguish the rights of either party that accrue prior to expiration, termination, or cancellation or any obligations that extend beyond termination, expiration or cancellation, either by their inherent nature or by their express terms.

33) TAXES

Any applicable taxes shall be invoiced as a separate item and in accordance with this paragraph and applicable laws.

- a. N.C.G.S. § 143-59.1 bars the Department from entering into contracts with Contractors if the Contractor or its affiliates meet one of the conditions of N.C.G.S. § 105-164.8(b) and refuses to collect use tax on sales of tangible personal property to purchasers in North Carolina. Conditions under N.C.G.S. § 105-164.8(b) include: (1) Maintenance of a retail establishment or office, (2) Presence of representatives in the State that solicit sales or transact business on behalf of the Contractor and (3) Systematic exploitation of the market by media-assisted, media-facilitated, or media-solicited means. By execution of the proposal document the Contractor certifies that it and all its affiliates, (if it has affiliates), collect(s) the appropriate taxes.
- b. All agencies participating in this Contract are exempt from federal taxes, such as excise and transportation. Exemption forms submitted by the Contractor will be executed and returned by the using agency.

34) TIME IS OF THE ESSENCE

Time is of the essence in the performance of this Contract and all provisions that specify a time for performance.

35) PAYMENT AND INVOICE TERMS

- a. Contractor shall submit a State of North Carolina Substitute W-9 Form, Request for Taxpayer Identification Number within two (2) State Business Days of contract award. The W-9 can be found at: <https://www.osc.nc.gov/state-north-carolina-sub-w-9>.
 - i. Completed W-9 should be sent to Medicaid.FinanceAP@dhhs.nc.gov.
 - ii. Contractor shall submit verification of submission of required forms via email to the Department's Contract Administrator for contractual matters. Failure to provide a completed form may delay payment to the Contractor.
- b. Contractor shall register for the North Carolina electronic Vendor Portal (eVP) within two (2) State Business Days of execution of the Contract at the following link: <https://evp.nc.gov/>.
- c. Contractor shall submit verification of registration with the North Carolina electronic Vendor Portal (eVP) to the Department's Contract Administrator for contractual matters. Failure to register may delay payment to Contractor
- d. Contractor must submit one (1) invoice per month, no later than the fifteenth (15th) Calendar Day of the month, unless the Department approves another date. Invoices shall state the period of performance (month, year) and include the total amount invoiced for the period.
- e. Invoices must be submitted as follows:
 - i. Electronically to: Medicaid.FinanceAP@dhhs.nc.gov and to the Invoices Electronic Submission Contact in *Attachment M: Contract Administrators*
 - ii. Department accounting staff may be reached at 919-855-4114 for questions regarding invoices.
 - iii. The Department will promptly notify the Contractor of any changes to the information above for submission of invoices.
- f. Payment will only be made for services and/or deliverables accepted by the Department in accordance with the Contract requirements *Attachment E: Cost Proposal* and actual implementation dates.
- g. Except as otherwise provided, the Contractor is responsible for all payments to Subcontractors under the Contract.
- h. Payment terms are not later than thirty (30) Calendar Days after receipt of a correct invoice as verified by the Department.
- i. In the event any invoice is incorrect, and the Department requires changes, the payment terms shall be net thirty (30) Calendar Days from the date the corrected invoice is resubmitted by the Contractor.
- j. The Department reserves the right to dispute an invoice after payment and require the Contractor to include a credit on the subsequent month's invoice to resolve disputes.
- k. Any reductions based on liquidated damages or other performance issues, may be withheld from the Contractor's invoices. Contractor shall provide a credit memo for such reductions within ten (10) Calendar Days, upon Department's request.

Section 2: NCDHHS Privacy and Security Office (PSO)

2. NCDHHS Privacy and Security Requirements

Under this agreement the Vendor shall implement data security measures compliant with industry best practices. Additionally, the Vendor agrees to adhere to the requirements established by the NCDHHS Privacy and Security Office (PSO) in the NCDHHS Privacy and Security policies as well as the NC Statewide Security Policies:

- [NC Statewide Security Policies](https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies) (<https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies>)
- [NCDHHS Privacy and Security Policies](https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/) (<https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/>)

3. Compliance with Applicable Laws and Regulations

The Vendor shall comply with all applicable laws, ordinances, codes, rules, regulations, licensing requirements, and electronic storage standards concerning privacy, data protection, confidentiality, security, and mandatory reporting including those of federal, state, and local agencies having jurisdiction where business services are provided for accessing, receiving, or processing all confidential information.

If the DHHS Division or Office determines that some or all the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended (HIPAA), or its implementing regulations, including the Privacy Rule (45 C.F.R. Parts 160 and 164, subparts A and E), Security Standards (45 C.F.R. Parts 160, 162 and 164, subparts A and C), and HITECH provision, the Vendor agrees to comply with all HIPAA requirements and will execute such agreements and practices as the Division or Office may require to ensure compliance.

4. Breach, Incident, and Notification Requirements

Duty to Report

Regardless of any other notification requirements the Vendor may have under this contract they shall report any suspected or confirmed privacy or security incidents or breaches to the PSO. This includes but is not limited to unauthorized access, use, disclosure, modification, or destruction of DHHS data.

Reports shall be made using the following website <https://security.ncdhhs.gov> no later than 24 hours of initial discovery. If the data is subject to Social Security Administration (SSA), Internal Revenue Service (IRS) or state tax, or Centers for Medicare and Medicaid Services (CMS) requirements, the report shall be made within one (1) hour, but no later than 24 hours of discovery.

At a minimum, incident reports shall contain to the extent known:

- The nature of the incident
- The date the incident occurred
- The date the vendor became aware of the incident
- The identity of affected or potentially affected individual(s)
- Any specific information known about the incident

Investigation

As part of any breach or incident investigation, the Vendor agrees to make good-faith, reasonable efforts to cooperate with DHHS Divisions and Offices to mitigate the damage or harm of such security incidents.

Breach Notification

If any applicable federal regulations, state regulations, local law, or rules require the DHHS division/office or the Vendor to give affected persons written notice of a privacy or security breach arising out of the Vendor's performance under this contract, the Vendor shall bear the cost of the notice.

Federal Office of Civil Rights (OCR)

If the Vendor is contacted by OCR regarding work being performed under this contract, they shall notify the PSO within 24 hours of initial notification.

5. Continuous Monitoring

In addition to the Continuous Monitoring requirements established in Section 3.2.2 -Solutions not Hosted on State Infrastructure of this contract, the Vendor agrees to comply with the following:

3rd Party Security Assessment

Vendors providing Infrastructure as a Service, Platform as a Service, and/or Software as a Service for NCDHHS are required to obtain approval from the PSO to ensure their compliance with statewide and departmental privacy and security policies.

To obtain such approval, the Vendor shall annually provide NCDHHS with both a written attestation to its compliance and an industry recognized, third party assessment report, such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, HITRUST CSF and ISO 27001. NCDHHS is required to review these security assessment reports, assess the risk of each vendor, ensure completion of all findings using a Corrective Action Plan (CAP), and provide an annual certification of the Vendor's compliance to the State CIO.

NCDHHS Assessment

The NCDHHS Privacy & Security office may perform periodic independent security assessments of Vendor hosted applications on the public/private/hybrid cloud or On-Prem data centers. The Vendor must provide access to their applications' hosting environment and their key resources to NCDHHS designated resources and NCDHHS engaged vendors to perform a privacy & security risk assessment that includes vulnerability analysis, penetration testing, and risk analysis based on the latest NIST 800-53, Federal, State and NCDHHS requirements.

Privacy Threshold Analysis

If requested, the Vendor shall work with the NCDHHS to provide a data inventory of all cloud hosted services and assist with the completion of a Privacy Threshold Analysis (PTA) documenting the data classification and the data fields hosted within the cloud, offsite, or Vendor-hosted environment. The Vendor shall review a Privacy Threshold Analysis (PTA) with the NCDHHS Privacy and Security Office annually and assist with updating the PTA when changes to the data being hosted occur.

If, during completion of the PTA, the NCDHHS Privacy and Security Office determines that the contract will involve data classified as Restricted, Highly Restricted, or other sensitive data, a Data Use Agreement (DUA) must be signed prior to restricted or sensitive data

being shared with the selected vendor. The current NCDHHS standard DUA template can be accessed here: [Template NCDHHS Data Use Agreement 072025.docx](https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/) (https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/)

6. Oversight / Record Retention

North Carolina General Statutes Chapters 121 and 132 govern the retention and disposition of all records located in, maintained by, or in the legal custody of NCDHHS.

Along with Federal record retention requirements, NCDHHS is subject to two retention schedules: the [NCDHHS Records Retention and Disposition Schedule for Grants](https://www.ncdhhs.gov/about/administrative-offices/office-controller/records-retention/) (https://www.ncdhhs.gov/about/administrative-offices/office-controller/records-retention/), and the [NC Department of Natural and Cultural Resources \(NCR\) Records Retention and Disposition Program Schedule](https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule) (https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule).

Examples of some general retention schedules include:

- Medicaid and Medical Assistance grants and programs are ten (10) years
- HIPAA record retention is six (6) years
- Internal Revenue Service (IRS) record retention is seven (7) years
- Social Security Administration (SSA), the record retention period is seven years
- Grant record retention period is a minimum of five (5) years

These examples represent the minimum data retention requirements. If data maintained under this contract is involved in any litigation, claim, negotiation, audit, disallowance action, or other action before the retention period expires, the retention schedule shall be extended until resolution of all issues. In cases where multiple retention schedules apply, the longer retention schedule shall prevail.

Records developed or maintained under this contract shall not be destroyed, purged, or disposed of without the express written consent of the appropriate NCDHHS Division or Office record or data owner and only in compliance with the published disposition schedule(s).

Any destruction of data must meet all requirements identified in the [Statewide Media Protection Policy](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment) (https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment). This includes ensuring electronic data is permanently deleted and non-recoverable. Data destruction shall be performed in accordance with the most current revision of NIST Special Publication 800-88. Additionally, a certificate of destruction shall be provided to the NCDHHS data owner upon completion of the data destruction.

2) Use of Artificial Intelligence

The transparent, secure, responsible, and ethical deployment of AI is essential to ensuring accountability and the protection of civil liberties in government operations and decision-making. The Vendor is fully and solely responsible and liable for and must disclose the use of Artificial Intelligence (AI) technologies within the proposed product, service, and performance. These AI technologies include, but are not limited to Machine Learning, Natural Language Processing (NLP), Generative AI (GenAI), Predictive Analytics (Predictive AI), Assistive AI, Conversational AI, and Computer Vision.

Any use of AI in the performance of the contract shall be implemented in compliance with the [North Carolina State Government Responsible Use of Artificial Intelligence Framework](https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment%3Fattachment=) (https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment%3Fattachment=).

If AI is being used, the Vendor's proposal shall include a section which specifically identifies how security and privacy are addressed within the AI portions of the application. Minimally this section shall include the following:

- The purpose and scope of AI's use
- How the AI will be implemented in a manner that is compliant with the seven principles and practices identified in [Framework for Responsible Use of Artificial Intelligence](https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment) (https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment)
- How the Vendor will ensure data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) under the [NC Statewide Data Classification and Handling Policy](https://it.nc.gov/documents/statewide-policies/statewide-data-classification-handling-policy/open) (https://it.nc.gov/documents/statewide-policies/statewide-data-classification-handling-policy/open) is not used to train AI models unless explicitly authorized by the NCDHHS Business Owner and the PSO
- Safeguards used to prevent unauthorized access, use, or disclosure of data used by the AI
- Inclusion of a [NIST AI Risk Assessment](https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf) (https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf) as a deliverable in the Vendor's proposal

NCDHHS reserves the right to authenticate and verify Vendor's adherence to the provisions of this section and Vendor shall make good-faith, reasonable efforts to cooperate with NCDHHS to do so.

3) Flow-Down

In addition to the subcontracting requirements in Paragraph 4) of the NCDIT Terms and Conditions, Attachment B, Section: (1) if a sub-vendor is used in the performance of this contract, written approval of the PSO is also required; and (2) Vendor must include, without modification, all the security and privacy terms and conditions in this Attachment C, NCDHHS Privacy and Security Terms and Conditions in each sub-contract.

Section 3: NCDHHS Development of Artificial Intelligence Systems

1) DEFINITIONS: AS USED HEREIN:

AI System shall have the meaning set forth in the Advancing American AI Act, section 7223(4) of Pub.L. 117-263.

Custom Development: means any design, modifications, customizations, configurations, or enhancements to AI Systems or associated implementations or workflows, and any related work product or deliverables, in each case developed specifically for the State under this contract, including (a) prompt templates specifically developed for the State under this contract and (b) any modifications, customizations, configurations or enhancements to AI Systems as a result of model training or fine-tuning. For clarity, Custom Development excludes any background intellectual property existing prior to entry into this contract or developed independently by such Vendor or Subcontractor without use of or reference to the State 's confidential information or design specifications during the term of this contract.

Data: shall have the meaning set forth in the Attachment B: North Carolina Department of Information Technology Terms and Conditions, Section 4, paragraph 1) Definitions and shall, without limiting the generality of the foregoing, specifically include Data Inputs and Data Outputs.

Data Inputs: means all data, information, PII or content submitted to the AI System, used to fine-tune, test, or validate the AI System, or otherwise provided to the Vendor or Subcontractor in the performance of this contract, including but not limited to user prompts, queries, instructions, source data, documents, and any other information or content submitted or provided by or on behalf of the State.

Data Outputs: means all data, information, PII or content generated by the AI System in the performance of this contract, including but not limited to responses, results, analyses, anonymized data, derivative data, metadata, logs, synthetic data, and any other output or action produced by the AI System.

State Data: collectively means Data Inputs and Data Outputs.

LLM: means a large language model, which is a generative AI model trained on vast, diverse datasets that enable the model to generate natural-language responses to user prompts and the definition includes any decoder or encoder design used in probabilistic language modeling.

Subcontractor: means the licensor of the AI System provided pursuant to this contract, if different from Vendor.

2) ORDER OF PRECEDENCE:

The terms and conditions of this section shall apply to this contract notwithstanding any language in this contract or any Subcontractor's commercial terms and conditions purporting to invalidate or override customer purchasing documentation or contract terms or establish a different order of precedence than set forth herein. In the event of a conflict between this section and any term or condition of this contract or a Subcontractor's commercial terms and conditions, the terms and conditions of this section shall control for AI Systems to the extent of the conflict.

3) INTELLECTUAL PROPERTY RIGHTS:

- a) Rights in State Data: The State retains full ownership of and will own all State Data, Data Inputs, Data Outputs, and Custom Developments. To the extent the Vendor or Subcontractor obtains any intellectual property rights in State Data, or any improvements, enhancements, feedback, or derivative works thereof, Vendor and Subcontractors hereby assign and transfer all such rights to the State effective immediately upon creation. The Vendor retains ownership of the underlying AI System and base models.
- b) Vendor License and Permitted Uses: Neither Vendor nor Subcontractor shall have any rights to use State Data, information provided to the Vendor nor Subcontractor, or Custom Developments; provided, however, that Vendor shall have a limited, revocable, non-exclusive, non-transferable, license to use State Data and Custom Developments solely for the following permitted purposes: (i) performing the specific requirements of this contract; (ii) providing technical support and maintenance as required under this contract; and (iii) such other uses as

may be expressly authorized in writing by the State. This license shall be exercised only during the contract period of performance and only through the Vendor or Subcontractors as authorized under this contract.

- c) Custom Developments and Model Rights: The Vendor shall: (i) dedicate the Custom Developments, including any custom models resulting from such Custom Developments, to the State's exclusive use; (ii) treat such Custom Developments, custom models and all associated Data as the State's confidential information; and (iii) not use, reproduce, or derive benefit from such Custom Developments or custom models for any other purpose, or for the benefit of any other party, without express written authorization from the State.
- d) Feedback and Improvements: The State retains ownership of any feedback provided by the State to the Vendor or Subcontractor with respect to the AI System and any improvements, enhancements, corrections, annotations, or other modifications made to State Data (collectively, "Data Improvements") or Custom Developments, regardless of whether such Data Improvements are generated by State personnel, the Vendor, Subcontractor, or through automated processes. To the extent the Vendor or Subcontractor obtains any intellectual property rights in such feedback or Data Improvements, except for the limited right to use provided herein, Vendor and Subcontractor hereby assign and transfer all such rights to the State effective immediately upon creation.
- e) State Data Usage
 - i) AI Use Disclosure: Vendor shall disclose the use of any AI System, including any use by a Vendor and Subcontractor in the performance of this contract. This includes both AI Systems that are expressly part of the contracted deliverables as well as any AI Systems utilized in the fulfillment of contract obligations. Unless instructed otherwise by the Contract Administrator, the initial disclosure shall be made in the Vendor's Response to the RFP and shall be amended or supplemented after award no less than thirty (30) days prior to a material change to the facts initially or previously disclosed. The Vendor must use only American AI Systems. The use of foreign AI Systems in the performance of this contract, including any AI components manufactured, developed, or controlled by non-U.S. entities, is prohibited;
 - ii) Data Handling: The State Data shall not be used to train, fine-tune, or otherwise improve any LLM or other machine learning or AI models, including those operated by third parties, or to develop or improve the AI System(s) for any other customers or any commercial or non-commercial purposes. State Data shall not be retained, accessed, or used beyond the scope and duration expressly permitted under this contract;
 - iii) License Grant to State: Notwithstanding anything to the contrary in the Vendor's licensing terms for the AI System, the Vendor grants to the State an irrevocable, royalty-free, non-exclusive license to use the AI System for the duration of this contract. This license includes the right to: (a) operate and access the AI System through agreed-upon methods; (b) input Data Inputs and receive Data Outputs; (c) allow authorized State personnel and contractors to use the AI System; and (d) integrate the AI System with State systems.

4) CONFIDENTIALITY OF STATE DATA:

The Vendor and Subcontractor shall:

- a) Protect all State Data by treating it as sensitive and confidential in perpetuity;
- b) Not disclose any State Data to any party without prior written permission of the Contract Administrator;
- c) Use State Data solely as required for the performance of the contract and for no other purpose and in no other manner whatsoever;

- d) Implement "eyes off" Data handling procedures that restrict human review of State Data except as strictly necessary to provide the AI System to the State (including ensuring that any human access to State Data must be logged, justified, and limited to the minimum necessary for system functionality);
- e) Implement and maintain appropriate technical and organizational measures to ensure that all State Data is logically and physically segregated from the Data of any other customer or client, and is not commingled with Data of other customers or clients; and
- f) Upon completion, termination or expiration of the contract, unless otherwise directed in writing by the State , securely delete all State Data from the AI System and all its other systems and all copies, backups and derivatives thereof, and certify deletion to the Contract Administrator in writing.

5) AUDIT AND COMPLIANCE:

Vendor Obligations for Compliance, Auditing, and Documentation. The Vendor shall:

- a) Provide, upon State request, and under appropriate confidentiality protections, comprehensive documentation including but not limited to: (a) compliance verification with terms and conditions of this contract; (b) AI System decision-making processes, logic, and operational parameters; (c) system documentation consistent with NIST AI Risk Management Framework guidelines, including system cards or equivalent documentation; (d) privacy controls effectiveness and PII processing prohibition compliance; (e) testing methodologies used to detect and mitigate noncompliance with unbiased AI principles; (f) known biases, limitations, safety concerns, and performance metrics; and (g) any other information necessary for the State to complete an AI Impact Assessment;
- b) Implement human oversight and intervention capabilities, including: (a) mechanisms for human review and override of AI decisions when required; (b) clear escalation procedures for human intervention; and (c) for high-impact AI Systems, automatic recording and retention of decision-making events and rationale. AI is considered high impact when its output serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on rights or safety;
- c) Establish feedback mechanisms allowing the State to: (a) provide performance feedback and improvement requests through formal channels; (b) request system modifications or enhancements; and (c) report operational concerns without requiring incident classification. State Data and State confidential information shall be expressly excluded from any feedback the Vendor may use for system improvement purposes or any other purposes (except solely the performance of the contract);
- d) Submit new model versions and features to State review and testing for compliance with performance standards prior to deployment. Performance standards shall include: (a) accuracy and reliability metrics; (b) security and privacy compliance; and (c) operational effectiveness criteria.

6) DATA PORTABILITY AND INTEROPERABILITY:

The Vendor shall ensure the use of open and standard Data formats and application programming interfaces (APIs) for all Data Outputs, Custom Developments and AI Systems. The Vendor, or any applicable Subcontractor, shall not use proprietary technologies or formats that otherwise require additional licensing or create vendor dependencies.

7) CHANGE MANAGEMENT:

- a) Advance Notice: Vendor shall provide a thirty (30) day written notice before implementing, updating or upgrading any AI enhancements, features, or components being incorporated into the AI services, including but not limited to modifications to system prompts, behavioral instructions, or other modifications that would impact performance.
- b) State Review: Following State receipt of change notice, the State has thirty (30) business days to test, review, and approve/reject proposed changes for performance and compliance with these terms and conditions.
- c) Version Control: Vendor shall: (a) maintain the previous AI version for ninety (90) calendar days post-deployment of a new version; (b) allow State to opt out of new features while retaining existing functionality by providing notice to the Vendor prior to deployment of the new version; (c) provide rollback capability to the previous version within thirty (30) calendar days if requested within the 90-day period under clause (a) of this section.

8) SYSTEM EVALUATION, TESTING, AND SAFETY MONITORING:

- a) Vendor shall make best efforts to ensure the AI system complies with the following Unbiased AI Principles:
 - i) Truth Seeking: The AI system shall be truthful in responding to user prompts seeking factual information or analysis. The AI system shall prioritize historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory;
 - ii) Ideological Neutrality: The AI system shall be a neutral, nonpartisan tool that does not manipulate responses in favor of ideological dogmas such as Diversity, Equity, Inclusion. Vendor shall not intentionally encode partisan or ideological judgments into the LLM's outputs.
- b) Vendor shall implement ongoing monitoring for bias, and safety issues, and shall:
 - i) Implement continuous improvement processes to enhance detection and mitigation of performance, bias, and safety issues and/or systems generating illegal or prohibited content, including regular evaluation of system outputs (excluding Data Outputs as defined in section 1.0 above) against verified factual sources;
 - ii) Notify the State within 24 hours of identifying any safety issue and provide written updates to the Contract Administrator every twenty-four (24) hours until all mitigation or remediation activities have been completed;
 - iii) Provide, upon request, detailed documentation of mitigation or remediation efforts, including testing results demonstrating resolution;
 - iv) Provide, upon request, quarterly reports summarizing AI System performance, user feedback, and any bias or safety incidents.
- c) The State reserves the right to conduct assessments of the AI model(s) used in connection with the AI System, including bias and safety evaluations, at any time during the contract period of performance.
- d) Vendor shall provide timely cooperation and access to enable effective performance of such assessments, including but not limited to disclosure of the LLM's system prompt, specifications, evaluations, or other relevant documentation.
- e) If the State assessment identifies performance issues with unbiased AI principles, safety concerns, or other harmful outputs:
 - i) State shall provide written notification to the Vendor specifying the nature of the identified issues
 - ii) Vendor shall, at no additional cost to the State, investigate and remediate substantiated issues within thirty (30) calendar days of notification
- f) If remediation efforts fail to adequately address performance, bias, and safety issues:

- i) State retains the right to suspend use of the AI System until remediation is satisfactorily completed;
- ii) The State may, at its discretion, initiate procedures for termination for cause in accordance with the terms of this contract;
- iii) The State may seek third-party remediation at Vendor's expense;
- iv) The Vendor shall be liable for any decommissioning costs and reasonable costs associated with transitioning to an alternative solution;
and
- v) Vendor shall indemnify and hold harmless the State against any claims, damages, or liabilities arising from demonstrable harm caused by issues that were not properly disclosed or were misrepresented by the Vendor.

ATTACHMENT D: DESCRIPTION OF OFFEROR

Provide the information about the offeror.

Offeror's full name	
Offeror's address	
Offeror's telephone number	
Ownership	☐ Public ☐ Partnership ☐ Subsidiary ☐ Other (specify)
Date established	
If incorporated, State of incorporation.	
North Carolina Secretary of State Registration Number, if currently registered	
Number of full-time employees on January 1 st for the last three years or for the duration that the Vendor has been in business, whichever is less.	
Offeror's Contact for Clarification of offer: Contact's name Title Email address and Telephone Number	
Offeror's Contact for Negotiation of offer: Contact's name	

Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Contractual Issues: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Technical Issues: Contact's name Title Email address and Telephone Number	

ATTACHMENT E: COST FORM

INSTRUCTIONS to VENDORS

Pricing Tables Submission Instructions:

The Cost Proposal Workbook is required to be completed as part of the RFP submission. Describe how the Vendor can provide its total all inclusive, turnkey costs associated with the solution and services outlined in this RFP, including all direct and indirect costs. The total proposed price is made

up of data from Sheet 3 Implementation Costs, and Sheet 4 O&M Costs. Vendors should also supply supporting information in sheets 5, Labor Rates, 6 Additional Information, and 7 Assumptions, sufficient for the State to have a clear understanding of the Vendor's pricing methodology.

To obtain an electronic version of the Cost Proposal Workbook in Excel format, please contact the Contract Specialist listed on the first page of this document.

Basis of Estimates (BOEs):

Vendors must include introductory information in their BOEs in order to describe any general method, assumptions, or other useful information needed to understand the estimates. The State is interested in understanding how each Vendor estimated the prices in its Proposal rather than forcing conformance to a specific format. As such, Vendors may format the BOEs in any reasonable manner that communicates the required information. BOEs are separated by pricing table to ensure consistency.

Vendor's must describe their bases of estimates (BOEs) in support of all pricing tabs in their Cost Proposal Workbook, and the awarded Vendor shall continue this practice throughout the life of the Contract. Each pricing table shall have a basis of estimate associated with it. The State is interested in the *quality* of the BOEs rather than the *volume* of information provided. Vendor's may use estimates driven by bottom-up analysis, analogy, statistical modeling, or any combination of these or other appropriate methods and apply expert judgment where applicable. Note that when using the analogy method, comparisons should be made to *actual* results (e.g., actual labor hours on a project), not proposed quantities (i.e., those included in a previous proposal).

Each major element of a BOE should identify:

General:

- Assumptions having a significant impact on the estimate
- Method(s) of estimation and Results of the estimate
- Pertinent actual data and the source(s) of data used (e.g., previous projects, parametric models, etc.)
- Adjustments made to account for risk (particularly the risk assumed on efforts with fixed prices)

Software-related BOEs must address at least:

- Software/configuration sizing in terms of new, modified, reused, and deleted software/configuration when applicable.
- Other pertinent measurements of the scope of work (e.g., effort associated with the creation of training materials)
- Productivity estimates and how they drive labor estimates
- Derivation of labor quantities and costs
- Derivation of material/non-labor costs (including licensing costs)

Operations-related BOEs must address at least:

- Derivation of labor quantities and productivities
- Derivation of material/non-labor costs

Bases of estimates may be submitted in any reasonable format that is easy to understand and which includes, at a minimum, the above elements. BOEs should **not** be included on the same excel workbook as the Vendor's Cost Proposal Workbook. Note that BOEs are not required to describe the derivation of labor rates (compensation, benefits, etc.). In addition, statements such as, "in our experience, it takes approximately XXX hours to complete this effort," do not, by themselves, constitute sufficient BOEs. BOEs should be responded to in the same sequence as the cost tables.

Department will not pay separately for implementation costs incurred in standing up Vendor's solution. Those cost should be included in their respective year along with all other associated costs during that timeframe.

No payments will be made for items not quoted in the Vendor's Cost Proposal Workbook. Each invoice submitted for payment must include a summary log of all invoiced amounts through the contract lifecycle.

The Cost Proposal Tables contained in the Excel Workbook must be completed and submitted by Vendor in accordance with these INSTRUCTIONS to VENDORS and the Cost Proposal Workbook format.

The Cost Proposal Workbook must be completed in Excel format.

ATTACHMENT F: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature: _____

Date:

Printed Name: _____

Title:

ATTACHMENT G: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with the Statewide Information Security Manual (SISM), the State restricts the location of information systems that receive, process, store, or transmit State and Federal data to the United States which includes the following areas: US States, US Territories, US Embassies, and US Military installations (stateside or overseas). This restriction applies to the Vendor and to any subcontractors engaged to provide Services under this Agreement or with access to State Data. The Vendor must ensure that its subcontractor agreements contain the same restrictions and will be responsible for monitoring and enforcing subcontractor compliance at all times.

Pursuant to N.C.G.S. §143B-1361(b), the Vendor must complete and return this Disclosure Statement Attachment F with its solicitation response. The Vendor may attach additional pages to its response if needed. The State of North Carolina will evaluate Disclosure Statement Attachments for additional risks, costs, and other factors associated with its service prior to making an award for any such Vendor's offer. The Vendor must provide the following information in its bid response:

[Click here to enter text.](#)

- a. The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the contract and whether any of this work will be performed outside the United States.
- b. The corporate structure and location of corporate employees and activities of the Vendor, its affiliates or any other subcontractors.

[Click here to enter text.](#)

- c. Vendor agrees to provide notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States in the event such relocation occurs during the contract term.

Click here to enter text.

- d. Vendor agrees that any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided.

Click here to enter text.

- e. Will any work under this contract be performed outside the United States?

☐ ☐

YES

NO

The use of resources or workers located outside the United States is a critical security exception that must be escalated to the State Chief Information Officer for review pursuant to N.C.G.S. §143B-1376(c) and §143B-1320(c). These critical security exceptions are approved only in rare and extenuating circumstances. Vendor should account for this when preparing its response.

ATTACHMENT H: VENDOR REFERENCES/PAST PERFORMANCE

The electronic version of the template for the Past Performance Questionnaire, found in this Attachment H, may be requested by contacting the Contract Specialist.

The Past Performance Questionnaires from Vendor references will be used in the evaluation of past performance. The Vendor is responsible for obtaining past performance information from their references and must provide the completed Past Performance Questionnaire from at least three (3) client references for which it has provided services of similar size and scope to that requested herein.

At least one (1) of the three (3) references must be from a State Medicaid program or healthcare organization where the services provided are substantially similar in scope to that proposed in the RFP.

The Department reserves the right to contact any or all of these client references to determine whether the services provided are substantially similar in scope to that proposed in the RFP, and validate the information provided in the Past Performance Questionnaire.

Client references from the NC Department of Health and Human Services, its divisions, programs, or employees are prohibited and will not be considered to satisfy this requirement.

The completed and signed Past Performance Questionnaires, provided from the references to the Vendor, **MUST** be included in the response to this RFP as directed in section 6.3.2 Offer Organization.



NC DEPARTMENT OF
**HEALTH AND
HUMAN SERVICES**

**Business Reference Response to Past
Performance Questionnaire For:
State of North Carolina Request for Proposal (RFP)
Number: 30-2026-017-DHB**

Provider Data Management Credentialing Verification Organization (PDM/CVO)

PART A: Name of Vendor Submitting Proposal

NAME OF VENDOR:

PART B: Company / Respondent Providing Reference

NAME OF COMPANY / AGENCY:

RESPONDENT ADDRESS: CITY, STATE & ZIP:

RESPONDENT TELEPHONE NUMBER:

RESPONDENT E-MAIL ADDRESS:

RESPONDENT NAME AND TITLE:

PART C: Contract Information

PROGRAM TITLE:

BRIEF PROGRAM DESCRIPTION AND WORK PERFORMED:

CONTRACT TYPE (TIME AND MATERIAL, FIXED PRICE, COST):

CURRENT PROGRAM PHASE (DESIGN, OPERATIONS):

PERIOD OF PERFORMANCE (INCLUDING ALL OPTIONS):

CONTRACT DOLLAR VALUE (INCLUDING ALL OPTIONS):

CONTRACTOR'S ROLE (PRIME OR SUB):

WAS THIS A COMPETITIVELY AWARDED CONTRACT (YES / NO):

PART D: Performance Information

Code	Rating Descriptions
E	EXCEPTIONAL – Performance meets contractual requirements and exceeds many requirements to the Agency's benefit. The contractual performance was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
V	VERY GOOD – Performance meets contractual requirements and exceeds some requirements to the Agency's benefit. The contractual performance was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
S	SATISFACTORY – Performance meets contractual requirements. The contractual performance contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
M	MARGINAL – Performance does not meet some contractual requirements. The contractual performance reflects a serious problem for which the contractor has not yet identified corrective actions or the contractor's proposed actions appear only marginally effective or were not fully implemented.

- U **UNSATISFACTORY** – Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance being assessed contains serious problem(s) for which the contractor’s corrective actions appear or were ineffective.
- N/A **NOT APPLICABLE** – Unable to provide a rating. Contract did not include performance for this aspect, performance was not observed, or information was not available. Do not know.

In the tables that follow, indicate your rating for the contractor’s performance by placing an “X” in the appropriate code to the right of each question. Refer to the Rating Descriptions above. Provide supporting information and comments for each response in the space provided. Attach additional pages if more space is needed.

TECHNICAL / BUSINESS EXPERTISE

TE1: Contractor understood the Provider Enrollment or PDM/CVO Solution and provided the technical expertise required to meet contract performance.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE2: Contractor provided staff with appropriate technical skills and training commensurate with those required for successful project completion.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE3: Contractor deployed a Provider Enrollment or PDM/CVO Solution to a State Medicaid program.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE4: Contractor provided an effective solution for the Provider Enrollment or PDM/CVO Solution.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE5: Contractor solution that was deployed did not substantially deviate from solution that was proposed.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

QUALITY OF SERVICES

QS1. Contractor provided and followed effective quality control plan to meet program objectives.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

QS2. Contractor corrected deficiencies in a timely manner and pursuant to their quality control procedures.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SCHEDULE AND COST

SC1. Contractor delivered services within the required time period specified by contract requirements.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SC2. Contractor performed the effort within the estimated cost/price and actual costs/rates realized closely reflected the negotiated costs/rates.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

--	--	--	--	--	--	--

SC3. Contractor submitted accurate invoices on a timely basis.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SC4. Contractor demonstrated cost efficiencies in performing the required effort.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

PART E: General Comments and Signature
PLEASE PROVIDE ANY ADDITIONAL COMMENTS CONCERNING THIS CONTRACTOR'S PERFORMANCE, AS DESIRED.
Based on what you know today about the Contractor's ability to execute what they promised in their proposal, would you award another contract to the Contractor, if given the choice? Yes or No. Please explain in the area below.
Have there been any indications that the Contractor has had any financial problems? Yes or No. Please explain in the area below.

RESPONDENT SIGNATURE: Please provide your signature confirming the information you have provided is an objective assessment of the Contractor's past performance.	DATE:
---	-------

Thank you for your prompt response and assistance!

ATTACHMENT I: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses, and submit the completed Form as with its offer. Vendor shall not add or delete rows or columns in the Form or change the order of the rows or column in the file.

1. Vendor Name:
2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):
3. Have you been in business for more than three years? ☐ Yes ☐ No
4. Have you filed for bankruptcy in the past three years? ☐ Yes ☐ No
5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters. ☐ Yes ☐ No
6. Are the financial figures below based on audited financial statements? ☐ Yes ☐ No
7. Start Date of financial statements:
End Date of financial statements:
8. Provide annual reports with Financial Statements and management discussion, in electronic format, for the past three complete fiscal years:
9. Provide the following information for the past three complete fiscal years:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments			
b. Accounts Receivable (beginning of year)			
c. Accounts Receivable (end of year)			
d. Average Account Receivable for the Year (calculated)			
e. Inventory (beginning of year)			
f. Inventory (end of year)			
g. Average Inventory for the Year (calculated)			
h. Current Assets			
i. Current Liabilities			
j. Total Liabilities			
k. Total Stockholders' Equity (beginning of year)			

l. Total Stockholders' Equity (end of year)			
m. Average Stockholders' Equity during the year (calculated)			
INCOME STATEMENT DATA			
a. Net Sales			
b. Cost of Goods Sold (COGS)			
c. Gross Profit (Net Sales minus COGS) (calculated)			
d. Interest Expense for the Year			
e. Net Income after Tax			
f. Earnings for the Year before Interest & Income Tax Expense			
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities			
b. Capital Expenditures (property, plant, equipment)			

ATTACHMENT J: ENTERPRISE ARCHITECTURE

The Department maintains a comprehensive set of Enterprise Architecture information and artifacts that must be created and maintained by each vendor. The Department's Enterprise Architecture standards are based on the Federal Enterprise Architecture framework (FEA) and is aligned with the business capabilities and processes described within the Medicaid Information Technology Architecture (MITA) framework. It is, however, understood that the MITA framework is a high-level depiction of a Medicaid program and that additional capabilities and processes will be required to fully describe and document the North Carolina Medicaid Enterprise Systems.

The MES Enterprise Architecture standards require the use of industry standard conventions such as UML2, BPMN and ArchiMate to consistently describe all applications and all other architecture components within the MES environment. Vendors are required to provide standard documentation, of the following architecture areas, during the DDI phase of the project and to maintain this documentation during the O&M phase of the project:

BUSINESS ARCHITECTURE: Describes the business needs, dependencies and outcomes.

APPLICATION ARCHITECTURE: Describes the applications, products or software services used.

DATA ARCHITECTURE: Describes the data, how it is used, stored and transmitted.

INFRASTRUCTURE ARCHITECTURE: Describes the hardware, platforms or infrastructure services used.

PERFORMANCE ARCHITECTURE: Describes the performance measures and metrics that must be met.

SECURITY ARCHITECTURE: Describes the security measures across each of the five above areas.

While this attachment will provide a high-level understanding of the Departments EA standards, the Department maintains the right to add or change required Enterprise Architecture information and artifacts as needed.

The Department leverages Orbus Infinity ([Orbus Software](#)) as a central repository for all MES EA information and artifacts. All MES vendors will be given access to the Orbus Infinity environment and will be required to enter architectural details into this system. The Orbus Infinity application is accessed through remote desktop services that are provided by the Department and maintains vendor information in separate, secured instances of the application. Vendors cannot view information provided by other vendors.

Information is entered into Orbus Infinity using online forms and templates while additional information is provided through attached documents or diagrams. The Department has standardized on Microsoft Office products, which will be used as the accepted format for most of the attached artifacts. Other formats are being considered to support the documentation of data models and will be presented to the vendor upon finalization of the standard.

The following table outlines the key concepts that the vendor will be required to document through the EA information and artifacts collected by the Department.

Attachment J: Enterprise Architecture Table 1. Key Concepts	
Business Architecture	Business Capabilities, Business Processes, Functional and Non-Functional Requirements with traceability across the architecture
Application Architecture	Functional Design, Conceptual Design, Detailed Design, Application Data Exchanges, Application Maintenance Procedures, Disaster Recovery Plan, Software and Service Inventory, Application Definitions
Data Architecture	Data Management (Data Development, Operations, Governance, Security, Quality, Dictionary), Data Exchanges, Data Integrations, Data Interfaces, Data Architecture Designs, <u>Conceptual Data Models</u> , Logical Data Models, Physical Data Models
Infrastructure Architecture	User Infrastructure Design, Interface and Data Exchange Infrastructure Design, Cloud/Data Center Infrastructure Design
Performance Architecture	Performance Measures and Metrics, Compliancy Monitoring, Business Performance Monitoring, Application Performance Monitoring, Application Reliability Monitoring, Standards Management
Security Architecture	Business Security, Disaster Recovery and Business Continuity, Application Security, Data Security, Infrastructure Security, Security Monitoring.

All MES Enterprise Architecture information and diagrams must be maintained throughout the life of the solution and must be controlled through Project and Operational Change Management procedures.

Any change to requirements, measures or metrics must be updated within Orbus Infinity so that a full impact assessment can be performed by the Department.

ATTACHMENT K: VENDOR KEY PERSONNEL

- a) Key Personnel will be the accountable individuals to the State and will interface directly with existing State staff to form a management team. Key Personnel cost should be included in the fixed support cost and not be viewed as resources billable at an hourly rate. NCDHHS shall have full access to key personnel and 100% of their time be dedicated to this Contract. Any resources proposed as shared must be identified along with the percentage of time expected on this project. Any resources proposed at less than 100% (excluding the Account Manager) must be approved by the State Contract Manager. All other staff should be included in the fixed cost and not be listed as Key.
- b) Vendor must identify key personnel to be assigned for the duration of the Contract. Key Personnel must be identified and mapped to the staffing roles provided in *Attachment K: Table 1: Key Personnel*. Vendor must indicate the name of the proposed individual to perform each role. If a substitution is needed and the appropriate personnel is not immediately available, the Contractor should notify the Department of the interim personnel as they work to obtain the Department approval of the formal substitution request.
- c) If the Vendor must provide additional Key Personnel for consideration, the following information must be provided:
 - i. Name
 - ii. Role
 - iii. Experience relevant to the services to be provided under this Contract.
 - iv. Certifications or credentials for the role suggested
 - v. Requested effective date

The Contractor shall provide an updated org chart within five (5) business days of the Department's approval of substitution.
- d) The Vendor must provide a detailed staffing contingency plan for handling sudden and unexpected increases in volume of transactions or the number of users with a description on how the plan will be implemented and coordinated with the Department.

Key Personnel Role	Phase	Duties and Responsibilities of the Role	Minimum Certifications or Credentials Preferred by NCDHHS
Business Operations Manager	DDI, Certification, Operation, Maintenance & Configuration Phases of the Program.	This position is considered to be a key specific management position. During DDI this person designs and builds operational components to be overseen during O&M period. This person is responsible for overall project quality. Lead the Vendor's Business Operations for Provider Screening, Enrollment and Monitoring, including: -Provider Data Management (PDM) and Centralized Verification Organization (CVO) - Ensures compliance with the appropriate accrediting and regulatory agencies. - Oversees the operations of the PDM/CVO to develop, manage and monitor processes and procedures that support the credentialing, re-credentialing, expirable data management, and delegated credentialing contract processes. - Oversees all the credentialing functions including application management and primary source verification. -- -Oversees end-to-end process of Document Management and Workflow Performance --Oversees Provider Support Services (training and site visits) --Oversees the Provider Enrollment Call Center - Oversees credentialing staff in the day-to - day management of the overall CVO credentialing process and database management) -Coordination with the State Auditor's Office (SAO)	Business Operation Manager must meet the qualification of B.A./B.S. preferred; or equivalent combination of education and additional years of directly relevant experience five (5) years of experience directly related to the duties and responsibilities specified. A minimum of 3 years with Provider operations support, preferred, but not required

Certification Lead	DDI and Certification Phases of the Program	The Certification lead is responsible for coordination of all certification activities.	Has advanced knowledge of Streamlined Modular Certification (SMC) to support certification activities throughout the certification process a. Minimum of three (3) years' experience certifying systems against industry standards for projects similar in size and scope to this project. b. In-depth understanding of the most current CMS certification lifecycle required to successfully validate the system.
Change Manager	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	The Vendor must designate a Change Manager (CM) that ensures initiatives supporting the basis for changes are prioritized, justified, submitted, approved and released following Vendor and state processes agreed upon during negotiations. From the Vendor's perspective, there will be an organizational change management (OCM) function that will also need to be addressed which is considered an ancillary function of the CM role. The release management (RM) function is also critical to the State as it drives service tickets, coordination of the changes to operational systems, decommissioning efforts, and a logical sequencing of the functionality being deployed. The Change Manager is responsible for the RTM and all Deliverables.	Change Manager (CM) must meet the qualification minimum of ten (10) years of current experience relative to the role of a change/release manager.

Configuration Manager	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	The Contractor must designate a Configuration Manager with the ability and authority to ensure delivery of the Configuration Management services described within the Configuration Management Plan and in alignment with ITIL standards. Managing the configuration management processes, including establishing priorities and work assignments. Tracking compliance to policies and procedures and resolving / escalating any compliance issues. Facilitating Configuration Management audits. Facilitating communication with business and IT management to support configuration management efforts. The Configuration Manager provides information about the IT services and IT infrastructure (IT assets) utilized by IT Service Management. For this purpose, he/she maintains a logical model containing the components of the IT services.	Configuration Manager must meet the qualification of 7 years of Configuration Management experience with at least 5 years of experience as a Configuration Manager. 5 years of experience working with ITIL based Service Management (ITSM) tools and methodologies. Prepared ITIL Asset and Configuration Management in the Cloud environment.
-----------------------	---	--	--

Contract Manager	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	Acts as the single point of contact for matters concerning the Contractor's performance under the Contract. This person shall have the authority to make decisions that are binding to the Contract, shall be responsible for timely completion of the project, and shall be responsible for meeting all contractual obligations. The Contractor must designate a Contract Manager to be the single point of contact for matters concerning the Contractor's performance under the Contract. This person shall have the authority to make decisions that are binding to the Contract, shall be responsible for timely completion of the project, and shall be responsible for meeting all contractual obligations.	- Minimum of five (5) years' contract management experience managing related services with similar budgets, preferably in Medicaid or the healthcare industry and for a project similar in size and scope to this project.
Deputy Account Director	DDI, Certification, Operation, Maintenance & Configuration Phases of the Program.	Responsible for coordination of work activities throughout the life cycle of a specific project or wider ranging program to ensure defined performance, schedule, and cost objectives are met.	Deputy Account Director must meet the qualification of master's degree or equivalent combination of education and experience. Fourteen (14) or more years of experience required.
Implementation Director	DDI Phase of the Program.	Oversees program resources to achieve cost, performance, and quality objectives of the company and customer(s) for a large, complex, multi-account program. Manages project planning, tracking, and oversight to ensure project(s) are completed on-schedule and within budget.	Implementation Director must meet the qualification of bachelor's degree or equivalent combination of education and experience. Nine (9) or more years of project management experience. Agile and PMP, Scrum - Implementation methodologies.

Integration Lead	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program	Manage the design, configuration/build, integration, defect management, and implementation of the Contractor's scope of work.	- Minimum of ten (10) years leading system design and integration projects, including the technical design and implementation of projects similar in size and scope to this project. Work with SMEs to clarify requirements. - Experience must involve directing multi-discipline technical teams producing integration solutions (e.g., Interfaces, ETL, Data Ingestion, Service Oriented Architecture, MITA3.0, SOAP, REST API). - A bachelor's degree in information systems engineering, Computer Science, or a related field is preferred. - Experience with external System Integrator. - Experience with Cloud. - Preferred Medicaid or MMIS Provider Enrollment experience.
Medical Director	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	Directly responsible for the operation of the Credentialing Committee and serves as its chair and voting member, as well as appointing a proxy in their absence. The Medical Director is subject to Department approval. The Medical Director will follow and enforce the Bylaws of the Credentialing Committee as approved by the Department. The Medical Director shall participate in the review of Bylaws, credentialing committee operating policy and procedures, recruitment of credentialing committee members, and coordination of peer reviews.	The Medical Director must meet the qualifications specified by NCQA. The Medical Director must have a valid, current Medical Doctor degree; be North Carolina licensed, and board certified within their specialty; have a minimum of 5 years' experience in medical practice; and have a minimum of 3 years' experience in supporting policy and claims resolution services in commercial or government health insurance programs.
Project Manager	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	Represent and oversee the day-to-day activities of the project. Serve as the Department's primary point of contact for matters relating to the project and serve as a liaison for certification, collaborating with other contractors, and stakeholders.	- A minimum of seven (7) years' project management experience managing projects of similar size and scope, preferably in Medicaid or the healthcare industry. This experience must include relevant experience within the last three (3) years from the release date of the RFP. - Project Management experience should include each phase of the system development life cycle. - Project management certification through the Project Management Institute (PMI) is preferred. - Experience with Agile and Scrum certification.

Security Architecture and Compliance Specialist	Required during DDI and optional during O&M.	Act as the primary point of contact for the DHHS Privacy and Security Office (PSO). Ensure the solution complies with federal, state, and agency privacy and security policies and procedures. Implement and enforce industry-standard security best practices to maintain an optimal security posture for the solution. Design, develop, and review security documentation and deliverables to ensure alignment with the requirements. Coordinate with DHHS PSO–approved third-party independent assessors to successfully complete the independent privacy and security assessments for Operational Readiness Review (ORR) and Biennial for CEF requirements.	10+ Years Security Architecture, 5+ Years in Cloud Security Architecture and Industry standard framework such as NIST 800-53, HITRUST, SOC2 TYPE2. Practical experience in implementing Cloud Security Well Architected Principles. Designing and Implementing the Data Security in compliance with the HIPAA regulatory requirement. Cloud Security Specialist and Vendor Agnostic certifications such as CISSP and CISM is required.
---	--	---	--

Senior Business Analyst	DDI, Certification, Operation, Maintenance & Configuration Phases of the Program.	The Contractor must designate a Sr. Business Analyst. The Business Analyst position is a key role in helping North Carolina Medicaid establish its new, modernized, Medicaid Enterprise System. This individual must be a proactive, take-initiative, individual comfortable with the following business analysis core competencies: • Information Gathering • Identification of Key stakeholders • Identification and documentation of business objectives • Feasibility Study and Alternatives Analysis • Scope Definition • Definition of Delivery Plan • Definition of project and product requirements • Implementation and evaluation activities - o Documenting use cases - o Development of test cases for UAT Fit-Gap Analysis. Additional roles will require the individual to be: • Familiar with Waterfall/Agile Methodology as it relates to completing sprints and working on tasks • Strong Understanding of State/Commercial Medicaid Operations and Waiver Programs • Must have strong analytical skills, the ability to think logically, and must be a self-starter able to research and find solutions independently • Strong user support and interpersonal skills are required • Must have experience in performing detailed analysis and creating documentation • Experience and ability to research and document business rules/requirements information by interviewing business personnel and by mining laws, regulations, and policy documents	Sr. Business Analyst must meet the qualification of 7 years of MMIS or Medicaid experience.
-------------------------	---	---	---

		• Develop business rules and requirements via interviews with stakeholders, translation of governing documents and other means • Gather business requirements and translate them into functional/non-functional requirement/specifications developing user stories, acceptance criteria • Gather information on changes to applications, assess those changes for items which affect business users, and communicate changes to the users. • Assist business users with gaps in knowledge about IT systems, and IT staff with gaps in knowledge about business requirements. • Develop user stories, standard operating procedures, processes, and test plans • Participate in Joint Application Design (JAD) sessions with the Product Owners and business stakeholders • Serve as team expert with the modernization with the Medicaid Enterprise Systems and programs • Experience with business integration with a modular approach e.g. Operations Management, Managed Care Organizations (MCO), Member Enrollment, Member Information Management, Financial Management, Provider Enrollment, Claims and Encounters, Reference, Waiver Programs, Business Rules, Decision Support System, Federal and State regulations, MITA 3.0, and related topics	
--	--	---	--

Technical Manager	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	Lead all architecture, design, development, testing, configuration management, system integration, data conversion, and implementation work that is done to support system integrations across the MES. Interfaces heavily with business stakeholders, state IT Architects, and Engineers on all technology matters. This is the lead technical architect responsible for resolving complex technology issues and providing strategic direction.	- Minimum of ten (10) years of experience leading large-scale technology initiatives with significant system integration experience. Medicaid or MMIS experience.
Testing Lead	DDI, Certification, and Operation, Maintenance & Configuration Phases of the Program.	Coordinate all testing activities.	- Minimum of five (5) years' experience leading testing activities for a project similar in size and scope to this project. Work with SMEs to clarify requirements. - In-depth understanding of the testing lifecycle and all artifacts required to successfully validate the system. - Agile testing experience. - Test Automation experience.

Table K-1: Key Personnel

ATTACHMENT L: SERVICE LEVEL AGREEMENTS

1.0 Service Level Agreements (Implementation, O&M & Transition)

The State has identified the Service Level Agreements (SLA)s provided in *Table L-1 Service Level Agreements* that will be monitored throughout the life of the contract. The Vendor must work with the State to drive the automation of all SLA validation, verification, and reporting.

The State and Vendor agree that failure to meet certain performance standards will result in liquidated damages as set forth in Table L-1 Service Level Agreements. The State reserves the right to adjust the liquidated damages in alignment with the 10% Retainage, described in Section 7.14.5 Retainage, of any of the SLAs with thirty (30) days’ notice to the Vendor of changes in the liquidated damages. The change will go into effect upon execution of an Amendment.

The total amount of SLA liquidated damages assessed to the Vendor will at no time exceed 10% of the monthly invoices due.

Table L-1 Service Level Agreements information includes:

- SLA ID: Unique identifier of the SLA
- Description: A description of the SLA.
- Liquidated Damages: The State and Vendor agree that failure to meet certain performance standards will result in liquidated damages.
- Phase / Stage: The phase of the project when the SLA will be enforced and measured.
- Frequency / Updates: Indicates how often the SLA will be measured.
- Category: Categorization and grouping of SLA.

Note: The SLA ID assigned to each SLA in *Table L-1 Service Level Agreements* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

Service Level Agreements					
SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
PDM-SLA-BO-001	The Vendor must ensure that final status determination for all initial enrollment, re-enrollment, change request, and re-validation applications adheres to the following timeframes:	Monthly	Business Operations	Failure to meet the standard will equal \$1,000 per State business day beyond the required timeframe. For any re-validation application that does not reach final status by	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	• All clean and low risk applications are approved within five (5) State business days of receipt of all data necessary to adjudicate the application. • All medium and high-risk application decisions are applied to the application within two (2) business days. • Final status determination is made within ninety (90) Calendar Days of receipt of the application. ---If the application requires a fee, the SLA clock starts upon confirmation of a successful application fee payment. ---The SLA excludes business days in which the application is pending State review. ---The SLA includes calendar days in which the application is returned to the provider awaiting additional information. • Final status determination is made for all clean and low risk applications within thirty (30) Calendar Days of receipt of the application. ---If the application requires a fee, the SLA clock starts upon confirmation of a successful application fee payment. ---The SLA excludes business days in which the application is pending State review. ---The SLA is applicable to applications that do not have to be returned to the provider for additional information. • All re-validation applications must reach final status (approved or denied/terminated) by the CMS re-validation due date, with no exception.			CMS re-validation due date \$2,000 per occurrence.	
PDM-SLA-BO-002	Vendor must ensure 100% accuracy in credentialing providers in accordance with state and federal requirements	Monthly	Business Operations	\$1000 per provider record with an inaccuracy	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
PDM-SLA-BO-003	Vendor, and/or its approved sub vendor, must meet and maintain all the core requirements and certification or accreditation options specified by the National Committee for Quality Assurance (NCQA) for Credentialing Verification Organization and demonstrate compliance with federal and State credentialing regulations.	Monthly	Business Operations	Failure to meet the standard will equal \$10,000 per week or any part thereof in which Vendor did not meet NCQA core requirements for certification.	DDI (start of contract) & O&M
PDM-SLA-BO-004	The Vendor must ensure the Credentialing Committee: • Meetings are scheduled on a weekly basis (except as approved by the State). • Meeting Agendas and provider profile packages are sent three (3) business days prior to each meeting • Confirm planned attendance by voting members at least one (1) business day in advance of the meeting. Distribute meeting minutes within two (2) business days after the meeting. The meeting minutes must include attendance and all decisions made during the meeting.	Monthly	Business Operations	\$1000 per incident of non-compliance	O&M
PDM-SLA-BO-005	Vendor must perform 100% oversight and monitoring of delegated credentialing entities to include for each Delegated Entity: - A pre-delegation audit that includes a performance and staffing assessment, a policy and procedure review, and a review of the entities understanding and adherence to NCQA, State, Federal enrollment and credentialing requirements and delegation tasks. - Completion of an annual compliance audit to re-review all the components of the pre-delegation audit, audit 5% of the entity's credentialing and recredentialing files against NCQA, State, and Federal enrollment and credentialing requirements,	Monthly	Business Operations	\$10,000 per incident that is not conducted.	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	and create corrective action plans on deficiencies in collaboration with the Department to include revocation recommendations of delegated entity participation.				
PDM-SLA-BO-006	The Vendor must complete the enrollment process for providers submitting a Disaster Relief Provider Enrollment Application within one (1) State business day from the time that the application was received	Ad hoc, following a disaster	Business Operations	\$500 per application that does not meet the timeline	O&M
PDM-SLA-BO-007	The Vendor will adhere to all re-validation timelines (initial invite, reminders, suspensions, terminations) outlined by the Department.	Monthly	Business Operations	For missing initial invitation, reminders, suspensions, or terminations \$1,000 per missed item.	O&M
PDM-SLA-BO-008	Informal Appeals/Reconsideration Review: The Vendor will be notified of appeals that are filed by providers via an established email listserv account through which the NCDHHS Hearing office distributes all appeal correspondence. The Vendor must acknowledge receipt of all correspondence sent from the NCDHHS Hearing Office or any member of its staff via the listserv email account by replying to the email (reply all) within (1) state business day(s). Types of correspondence include: Notice of Appeal Scheduling Letter (Notice of Reconsideration Review) Notice of Dismissal Final Agency Decision All other related documents/correspondence	Monthly	Business Operations	\$1,000 per Business Day after Day 1.	O&M
PDM-SLA-BO-009	Vendor Internal Review Process: The Vendor must establish an Internal Review Process whereby a documented examination of the provider's record is conducted after receiving notice of an appeal, and within three (3) state business days, to determine if the adverse action was proper.	Monthly	Business Operations	\$2,500 per Business Day after Day 3.	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
PDM-SLA-BO-010	Outreach/Education: The Vendor will complete the outreach/education requirement via email directed to the contact person listed on the provider's record within seven (7) state business days of receipt of an appeal notice (Reference examples of proper email outreach provided by DHB). The purpose of this activity is to help providers understand what led to the adverse action (denial/termination), answer questions, and discuss various options and outcomes.	Monthly	Business Operations	\$2,500 per Business Day after Day 7.	O&M
PDM-SLA-BO-011	The Vendor must submit a Summary of Facts to the NCDHHS Hearing Office at least three (3) state business days in advance of the scheduled hearing. The Summary of Facts is a single page, memo style Word document purposed to defend the adverse action under appeal. The Summary must, at a minimum: explain the adverse action taken • reference the regulation/authority upon which the action was taken • include DHB's position and conclusion • be accompanied by supporting documents	Monthly	Business Operations	\$5,000 per Occurrence.	O&M
PDM-SLA-BO-012	The Vendor must a) add or remove a taxonomy on the provider's record or b) change the providers risk level on the provider's record or c) add additional licensure, accreditation, or certification on the provider's record, as directed by the State, within 2 business days.	Monthly	Business Operations	\$500 per business day late	O&M
PDM-SLA-BO-013	The Vendor must make exceptions to established business rules that require manual intervention, as directed by the State, within 5 business days or by the agreed due date.	Monthly	Business Operations	\$500 per business day late	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
PDM-SLA-BO-014	The Vendor must make updates to provider agreements, attestations, template letters, or notifications, static text and/or exclusion sanction questions, as directed by the State, within 4 weeks or by the agreed due date.	Monthly	Business Operations	\$500 per business day late	O&M
PDM-SLA-BO-015	The Vendor must add a new taxonomy including all associated business rules and exceptions, and end-date or modify criteria for an existing taxonomy, as directed by the State, within four (4) weeks or by the agreed due date.	Monthly	Business Operations	\$500 per business day late	O&M
PDM-SLA-BRR-001	The Vendor must update business rules and business rules matrix documentation within two (2) business days of deployment.	Monthly	Business Rules	\$500 per business day late	O&M
MES-SLA-CC-001	Vendor must staff the Call Center toll-free phone lines from 8:00 a.m. to 5:00 p.m., Eastern Time, on all State business days, Monday through Friday (excluding State holidays).	Monthly	Call Center	\$90.00 per quarter hour (15 minutes) that the Call Center is not operational during 8:00 a.m. to 5:00 p.m., Eastern Time, on all State business days Monday through Friday (excluding State holidays)	O&M
MES-SLA-CC-002	Vendor must respond to telephone and written inquiries with a researched response within two (2) business days.	Monthly	Call Center	\$50.00 per business day per inquiry that is not responded to within two (2) business days.	O&M
MES-SLA-CC-004	Vendor must ensure the total number of busy signals, disconnected calls (either by the system or person), and abandoned calls measured against the total inbound calls must not exceed five percent (5%) per day.	Monthly	Call Center	\$250.00 per day where busy signals, disconnected calls (by the system or a person), and abandoned calls exceed five percent (5%) of total inbound calls	O&M
MES-SLA-CC-005	Vendor must ensure the Average Speed to Answer (ASA) must be less than or equal to thirty (30) seconds as measured monthly 85% of the time, after the caller makes a selection in the IVR.	Monthly	Call Center	\$1,250 per month that the average speed to answer is between thirty-one (31) seconds and sixty (60) seconds.	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
				\$2,500 per month that the average speed to answer is between sixty-one (61) seconds and one hundred and twenty (120) seconds. \$5,000 per month that the average speed to answer is greater than one hundred and twenty-one (121) seconds.	
MES-SLA-CC-006	Vendor must survey at least every 10th caller to assess service quality, timeliness, and overall satisfaction. A minimum average caller satisfaction rate of 80% must be maintained. Monthly reports of survey results and satisfaction scores must be submitted to the Agency.	Monthly	Call Center	\$500.00 per month below eighty percent (80%) satisfaction	O&M
MES-SLA-CC-007	Within any given month, the average duration of unscheduled downtime preventing incoming calls on any service line must not exceed five (5) consecutive minutes.	Monthly	Call Center	\$5000 per month per service line	O&M
MES-SLA-CC-008	The Vendor's IVR must respond within three (3) seconds at least 98% of the time, measured 24 hours a day, 7 days a week, 365 days a year, excluding State-approved scheduled maintenance periods.	Monthly	Call Center	\$2,500 per day below 98%	O&M
MES-SLA-CC-009	The Vendor's call center must have a live answer rate of greater than 90% during business hours.	Monthly	Call Center	\$10,000 per month where live answer rate falls below 90% during business hours	O&M
PDM-SLA-CONV-001	The Vendor must ensure that 99% of all Data converted is correctly mapped and usable by the scheduled completion date in the Work Plan.	Ad hoc, based on reports for conversion/deliverable schedule	Conversion	\$1500.00 per business day, in which less than 99% of all Data converted is correctly mapped and usable beyond the scheduled completion date in the Work Plan	DDI/Conversion
PDM-SLA-INT-001	The Vendor must ensure timely and reliable delivery of provider data to designated technical partners supporting real-time and batch	Monthly	Integration	Liquidated damages are for each interface.	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	delivery. Delivery mechanisms and scheduling intervals for each interface are to be documented in the respective interface control document approved by the Department. - Real-time data must be delivered within three (3) seconds from the time of generation or availability. - All batch data must be delivered by the scheduled time as defined in the agreed processing schedule.			1 late delivery in month = \$500 2-3 late deliveries in a month = \$2,500 4 or more late deliveries in a month = \$5,000	
MES-SLA-PM-001	The Vendor must meet the due date for submission and subsequent resubmissions for each deliverable as defined in the Department approved project schedule.	Monthly	Project Management	\$500.00 per Business Day from the Deliverable due date.	DDI & O&M
MES-SLA-PM-002	Vendor must ensure there are no more than two submissions of any Deliverable to gain Acceptance by the Department using the process defined in Attachment N: Deliverables and Milestones Schedule.	Monthly	Project Management	\$1500.00 per submission per Deliverable requiring more than two submissions.	DDI & O&M
MES-SLA-PM-003	Vendor must have an acceptable documented risk mitigation plan submitted to the Department within five (5) business days of risk identification for 100% of high or critical project risks. The Department, after consulting with Vendor, will determine the level of criticality of each project risk.	Monthly	Project Management	\$1,000.00 per Business Day beyond the Performance Standard for high or critical project risks without the submission of a risk mitigation plan meeting the acceptance criteria.	DDI & O&M
MES-SLA-PM-004	Vendor must provide accurate responses to all Department Change Requests for Enhancements including proposed Solution and hours/cost within fifteen (15) business days for low complexity projects, twenty-five (25) business days for medium complexity projects or thirty-five (35) business days for high complexity projects, from submission of a Department Change Request for an Enhancement.	Monthly	Project Management	\$1000 per business day for each day an acceptable Change Request for an Enhancement is not received by the Department from Vendor within the Performance Standard. "Acceptable" means that the Change Request for an	DDI & O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	The Vendor will determine the level of complexity in consultation with Department.			Enhancement from Vendor includes Vendor's proposed Solution and associated pool hours/costs to comply with request made by the Department.	
MES-SLA-PM-005	Vendor must ensure all reports will be available online for review by the Department pursuant to the following schedule: A. Daily or Weekly Reports – by the end of the calendar day following the end of the reporting period. B. Monthly Reports – by the third calendar day following the end of the reporting period C. Quarterly or Annual reports – by the fifth calendar Day following the end of the reporting period.	Monthly	Project Management	\$500.00 per calendar day per report beyond the Performance Standard.	O&M
MES-SLA-PM-006	The Vendor must provide a Corrective Action Plans (CAP) or Plan of Action Milestones (PO&AM) to address any major deficiency identified by the state within ten (10) State Business Days from the time the state notifies the Vendor of the deficiency. The CAP or PO&AM must include deadlines and is subject to negotiation with and acceptance by the state. Once accepted, the Vendor must meet all milestones or actions specified by the approved deadlines.	As needed, daily when active	Project Management	\$1,000 per day a required CAP or PO&AM is late. \$1,000 per business day any milestone or action deadline is late	O&M
MES-SLA-OM-001	Vendor's Production Solution must have Availability 99.5% of the time, twenty-four (24) hours a day, seven (7) days a week, excluding Department approved planned Downtime. Availability is calculated as follows: Availability percentage =	Monthly	Operations & Maintenance	Department will assess as specified below, per hour for each hour, or portion thereof, if any of Vendor's Solutions fails to meet the 99.5%	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	unplanned Downtime (Total Downtime-approved Downtime) divided by Total time (24X7). The module is considered unavailable when any of the capabilities do not function as described in this RFP and subsequent documentation.			Availability Performance Standard. \$1,000/hour 0 to 24 hours beyond the Performance Standard \$2,000/hour 24 to 48 hours beyond the Performance Standard \$3,000/hour > 48 hours beyond the Performance Standard	

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
MES-SLA-OM-002	The Vendor will meet the following NC Medicaid reporting timelines for production issues. • Critical priority Issues: Must be reported within one (1) hour of identification. • High, medium, and low priority Issues: Must be reported within four (4) business hours of identification, or by 7 AM the next business day if discovered outside of business hours.	Monthly	Operations & Maintenance	Critical Priority Issues: • \$500/hour – 0 to 24 hours beyond the Performance Standard • \$1000/hour – 24 to 48 hours beyond the Performance Standard • \$2000/hour - >48 hours beyond the Performance Standard High, Medium, and Low Priority Issues: • \$100/hour – 0 to 24 hours beyond the Performance Standard • \$200/hour – 24 to 48 hours beyond the Performance Standard • \$300/hour - >48 hours beyond the Performance Standard	O&M
MES-SLA-OM-003	The Vendor will meet the following NC Medicaid resolution timelines for production issues. • Critical priority Issues: Must be resolved within twelve (12) hours of reporting. Status updates are required every two (2) hours, or at an alternative interval if mutually agreed upon. Note: Environment down/availability will require 24/7 response and resolution effort until the issue is resolved.	Monthly	Operations & Maintenance	Department will assess as specified below, per hour for each hour or business day per business day where noted, or portion thereof, if issues are not resolved within the resolution performance standard.	O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	• High priority Issues: Must be resolved within forty-eight (48) hours from the time the incident is reported. • Medium priority Issues: Must be resolved within four (4) business days from the time the incident is reported. • Low priority Issues: Must be resolved within ten (10) business days from the time the incident is reported.			Critical Priority Issues: \$1000/hour – for any delay beyond the Performance Standard High Priority Issues: \$250/hour – for any delay beyond the Performance Standard Medium Priority Issues: \$1000/business day – for any delay beyond the Performance Standard Low Priority Issues: \$100/business day - for any delay beyond the Performance Standard	
MES-SLA-SEC-001	Vendor must set up the alternate processing site with a Recovery Time Objective (RTO) of five (5) minutes and a Recovery Point Objective (RPO) of one (1) hour from the time a disaster is declared. The Vendor will restore essential services and information, irrespective of the time the incident occurred, in less than or equal to five (5) minutes 100% of the time.	Monthly	Security	5% of monthly retainage for each occurrence.	O&M
MES-SLA-SEC-002	Vendor must conduct and pass comprehensive annual technical and operational testing of the Disaster Recovery and Business Continuity Plan with any test failures documented and resolved within thirty (30) calendar days of testing completion.	Annually	Security	\$500.00 per day beyond the Performance Standard until the detailed Disaster Recovery Plan test results are delivered to the Department.	O&M
MES-SLA-SEC-003	If the Vendor is out of compliance with the Federal, State, and NCDHHS privacy & security policies, a mitigation plan to regain compliance is due to the Department within ten (10) State Business Days,	Monthly	Security	5% of monthly retainage for each failure to submit the plan within the specified timeline.	DDI, O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	with mitigation and testing to be completed in the timeframe defined in the mitigation plan.				
MES-SLA-SEC-004	The Vendor must provide the Corrective Action Plans (CAP) or Plan of Action Milestones (PO&AM) for mitigating the identified gaps in the internal risk assessments, third-party privacy & security assessments, or security audits to the NCDHHS Privacy & Security Office (PSO) within ten (10) State Business Days from the time the reports are submitted to the Vendor.	Monthly	Security	10% of monthly retainage for each failure to pass any Security Audit as identified in the SLA, 100% of the time, or Failure to provide a Corrective Action Plan to the NCDHHS Privacy & Security Office within 10 Business Days	DDI, O&M
MES-SLA-SEC-005	The Vendor must report all, including suspected, privacy/security incidents involving unauthorized access, use, disclosure, modification, or data destruction to the NCDHHS Privacy and Security Office within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare & Medicaid Services (CMS) data, the Vendor must report the incident within one (1) hour after the incident is first discovered.	Monthly	Security	0.5% of monthly retainage for each failure within the notification periods identified in the SLA	DDI, O&M
MES-SLA-SEC-006	Vendor must report any confirmed security breaches to the Department Contract Administrator and NCDHHS Privacy and Security Office within one (1) hour. Vendor must work collaboratively with the Department to gather, analyze and report findings to the Office for Civil Rights (OCR) for any HIPAA or HITECH incident involving Vendor. Sufficient technical evaluation will be completed by the Vendor to verify the number of member potentially affected. The Vendor must share, coordinate, and assist in workarounds (as required) with any impacted modules.	Monthly	Security	All costs of mitigation (all Vendor and Department costs) for any HIPAA incident that results from actions attributed to Vendor's performance of the Contract. In addition, Vendor will receive sanctions, if any, determined by the OCR and be responsible for mitigation costs and other associated costs such as call center costs, credit reporting, publications, and media centers.	DDI, O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
MES-SLA-SEC-007	Vendor must perform patching and corrections to mitigate critical security vulnerabilities within seven business days, high vulnerabilities within thirty business days, medium vulnerabilities within sixty business days, and low vulnerabilities within ninety business days. The Vendor must determine the level of criticality in consultation with the Department and in accordance to Section 3.3.3 Vulnerability Risk Ratings and Remediation.	Monthly	Security	\$5,000.00 per occurrence per day for Critical and \$5,000 per occurrence per week if the patch or correction is not Implemented within the Performance Standard time frame.	DDI, O&M
PDM-SLA-SEC-008	The Vendor must revoke user access within one business day or as agreed by state.	As needed	Security	\$500 per business day late	O&M
MES-SLA-TST-001	The Vendor must resolve defects identified during all applicable test phases in accordance with the approved Master Test Plan. Consistent failure to meet the defined timelines will trigger SLA enforcement if any of the following thresholds are exceeded during a sprint or test cycle: • More than fifteen (15) open defects remain unresolved. • The average age of critical and high-priority defects exceeds eight (8) business days.	Per Testing Cycle	Testing	If any of the SLA thresholds are reached within a testing cycle: \$500 per business day until the threshold level is resolved.	DDI
MES-SLA-TST-002	The vendor's E2E test execution must complete 85% of the test cycle's execution target, measured against ALM reports, weekly.	Per Testing Cycle	Testing	\$2,000 every week the vendor is out of compliance with the SLA, measured weekly.	DDI
PDM-SLA-TST-003	The Vendor's E2E test execution must complete 85% of the test cycle's execution target, measured against ALM reports, weekly.	Monthly	Testing	\$5,000.00 per Implementation in which Vendor is not able to demonstrate that 100% of the Specifications have been met.	DDI, O&M
PDM-SLA-TST-003	Vendor must thoroughly test the Solution and demonstrate proof of successful Vendor Testing for 100% of the Specifications defined for each Implementation. Vendor can demonstrate proof of	Monthly	Testing	\$5,000.00 per Implementation in which Vendor is not able to demonstrate that 100% of the	DDI, O&M

SLA ID #	SLA Description	Frequency	Category	Liquidated Damages	Phase/Stage
	successful Vendor Testing by providing Documentation such as system, integration or parallel test results or demonstration of the Specifications including Interfaces/APIs. All Specifications must be tested through the use of testing procedures, verification procedures and other testing methodologies identified in Contract Section 7, Section 3.10.2.6 of the RFP, and the associated testing requirements. This applies to all testing efforts, including SIT, UAT, and End-to-End Testing			Specifications have been met.	

Table L-1 – Service Level Agreements

ATTACHMENT M: CONTRACT ADMINISTRATORS

Contract Administrators are the persons to whom notices provided for in this Contract shall be given, and to whom matters relating to the administration of this Contract shall be addressed. The Department and the Vendor may change its respective administrator, address, and telephone number by providing written notice.

For the Department

Contract Administrator for all contractual matters:

Name and Title	Brandon Newpher Associate Director Technology and MES Contracting
Address	1915 Health Services Way Raleigh, North Carolina 27607
Mail Service Center Address	2501 Mail Service Center Raleigh, North Carolina 27699-2501
Telephone Number	
Email Address	Brandon.newpher@dhhs.nc.gov Medicaid.Contractadministrator@dhhs.nc.gov

Contract Administrator for all day-to-day matters:

Name and Title	Christina Bunch, Deputy Director Provider Operations
Address	1915 Health Services Way Raleigh, North Carolina 27607
Mail Service Center Address	1950 Mail Service Center Raleigh, NC 27699-1950
Telephone Number	(919) 215-6993
Email Address	Christina.Bunch@dhhs.nc.gov Medicaid.Contractadministrator@dhhs.nc.gov

State Privacy and Security Point of Contact:

Name and Title	Ramana Posam
Address	1915 Health Services Way, Raleigh, NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	919-855-3090
Email Address	Posam.ramana@dhhs.nc.gov

State Technical Point of Contact:

Name and Title	Naga Name
Address	1915 Health Services Way, Raleigh, NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	919-820-0712
Email Address	Naga.name@dhhs.nc.gov

Invoices Electronic Submission Contact:

Name and Title	Christina Bunch, Deputy Director Provider Operations
Address	1915 Health Services Way Raleigh, North Carolina 27607
Mail Service Center Address	1950 Mail Service Center Raleigh, NC 27699-1950
Telephone Number	(919) 215-6993
Email Address	Christina.Bunch@dhhs.nc.gov Medicaid.Contractadministrator@dhhs.nc.gov

For the Vendor

Contract Administrator for all contractual communication:

Name & Title	
Address 1 Physical Address	
Address 2 Mail Service Center Address	
Telephone Number	
Email Address	

Vendor's Technology contact for technical matters:

Name & Title	
Address 1 Physical Address	
Address 2 Mail Service Center Address	
Telephone Number	
Email Address	

ATTACHMENT N: DELIVERABLES AND MILESTONES SCHEDULE

1.0 DELIVERABLES

Table N-1 Deliverables lists the deliverables to be provided by the Vendor for this project. The information for each deliverable includes:

- Deliverable ID: Unique identifier of the deliverable
- Title: Name of the deliverable
- Description: A summary of the elements to be included in the deliverable.
- Phase / Stage: The phase of the project when the deliverable is expected to be delivered. The timing of the deliverable with the phase is in alignment with the milestone schedule provided in *Table N-2 Milestones*
- Frequency / Updates: Indicates how often the deliverable is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the deliverable. The meaning of the values is as follows:
 - None – No preferred template exists. The Vendor is free to provide the deliverable in its own format and content.
 - State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Deliverable ID.
 - DED Required: A Design Expectation Document (DED) must be submitted by the Vendor and approved by the State prior to the actual deliverable being submitted.

Deliverables submitted by the Vendor should follow industry standards, best practices, and the description provided. Upon submission of the Deliverable(s), the State will review that Deliverable, and acceptance will be in accordance with the *Attachment B: Department of Information Technology Terms and Conditions Acceptance Process*. The Vendor must ensure that, for each deliverable, no more than two review iterations are used to gain acceptance by the State of the deliverable.

The Vendor must provide deliverables that meet the following minimum quality standards:

- a. Provide accurate and comprehensive content.
- b. Ensure appropriate technical level for the audience
- c. Utilize correct grammar, spelling, and versioning
- d. Ensure diagrams are clear, concise, and add value
- e. Follow industry standards and best practices
- f. Appropriately define and reference information

Informal reviews and walkthroughs of draft and final deliverables are encouraged. When submitting deliverables for review, the Vendor must not submit an excessive number of deliverables to the Department for simultaneous review.

Note: The Deliverable ID assigned to each deliverable in *Table N-1 Deliverables* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-ARCH-001	Data Architecture	Document that describes the Vendor's solution's data, how it is used, stored, and transmitted. The document should also include, at minimum, the following information: • Data Governance: Define the authority and control over the management of data assets as well as how the Vendor will act as a Data Governance partner with Business and Technology Owners to decide how data can be used and how this usage must be controlled. Data Governance will influence all levels of Data Management and other architectural areas. • Data Management: Define processes that will be used to support Data Development, Data Operations, Data Security and Data Quality while supporting the functional and non-functional requirements and adhering to the Data Governance processes. • Data Development Management: Describe the process for designing, implementing and maintaining the solutions to meet the data needs of an organization. • Data Operations Management: Describe the process for planning, monitoring, controlling and supporting of structured and unstructured data assets across the data assets lifecycle. • Data Security Management: Describe the process for planning, development, and execution of data security policies and procedures to provide proper authentication, authorization, access and auditing of data and information. Must include processes for data privacy and security analysis along with requirements for encryption during processing, transmission and storage. • Data Quality Management: Describe the process for planning, implementation, and control activities that apply data quality management techniques to measure, assess, improve, and ensure the fitness of data for use.	DDI, O&M	Quarterly	None
MES-DEL-ARCH-002	Data Architecture Document –	Conceptual Data Model (CDM) identifies the data elements required for an end-to-end business process execution including the identification of data standards that will reduce	DDI, O&M	Quarterly	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
	Conceptual Data Model (CDM)	future rework to achieve successful data sharing across the enterprise and for intrastate/interstate exchanges. The CDM is required to be used as a reference to provide high-level overview of the data and relationships used by the enterprise and to provide a tool for ensuring the completeness of the business model.			
MES-DEL-ARCH-003	Data Dictionary (Electronic)	Electronic data dictionary using industry best practices to be approved by the Department. At a minimum, the data dictionary shall contain for each field: field name in human readable format, field description, database field name, database table, field type and length, valid values and their corresponding descriptions, source, and authorization for access for each data element in the files and databases. It must also include a business glossary and an inventory of Critical Data Elements (CDEs) that contains business definition, data lineage, ownership, and applicable data quality rules.	DDI, O&M	Quarterly	None
MES-DEL-ARCH-004	Logical Data Model (LDM) Document	Logical Data Model that describes and diagrams the module's data elements and relationships. This should include a description of all table structures, including column names, column data types, column constraints, primary keys, foreign keys, and relationships (a Physical Data Model).	DDI, O&M	Quarterly	None
MES-DEL-ARCH-005	MES Architecture Document	Document that contains data and information regarding the total solution to include each subsystem. It will address Enterprise Architecture as well as Application/Solution Architecture, Infrastructure Architecture, Performance Architecture and Integration Architecture as defined within the Federal Enterprise Architecture Framework. The Application Architecture will describe the application functions, process flows, communication flows, services used, user communities, use cases, software used, etc. The Application Architecture will demonstrate how the functional and non-functional requirements are being met or expanded upon. The Solution Architecture Document includes a technical explanation of all aspects of the solution including detailed architectural diagrams, data flows, component specifications, SaaS, COTS products and hosting environment details. The document will include architectural tradeoffs using the Architecture Tradeoff Analysis Method (ATAM) method or	DDI, O&M	Quarterly	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		other suitable method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of Agency's business goals. The Infrastructure Architectures describe the hardware, platforms or infrastructure services used by the Contractor's solution. It will also describe in sufficient detail the physical characteristics of the hardware, system software, and network components to build and integrate the architectural solution. The Performance Architecture describes how the application will scale and what metrics are measured to ensure the components are meeting the performance levels set by the State. Describe the tools used to measure the metrics and how they are used in capacity planning. The Interface Architecture should describe the interface(s) between the system being developed and other systems (e.g., batch transfers, real time APIs, queries, etc.), indicating the location of the interfacing system. Include the interface architecture(s) being implemented and the interfacing mechanisms (e.g., MQ, Gentran, etc.) and how they incorporate the State's Medicaid Integration Services capabilities. If remote connectivity is required, identify the method of access. Provide a diagram depicting the communications path(s) between this system and each of the other systems. The graphical representation should depict the connectivity between systems, showing the direction of data flow.			
MES-DEL-ARCH-006	Configuration /Customization Plan	Document that describes the Vendor's responsibility to identify, control, and track versions of hardware, software, documentation, processes, procedures, and all other components of the environment under the control of change management. Processes are provided to ensure that only authorized components, referred to as configuration items (CIs), are used in the environment and that all changes to configuration items are recorded and tracked through the component life cycle. This plan will outline the Vendor's: • Approach to conducting design sessions or walkthroughs. • Configuration management.	DDI, O&M	Quarterly	DED Required

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		• Approach to system enhancements • Programming and coding standards • Approach to moving and promoting code between lower and production environments • Approach to applying the latest patches to software, hardware, and environments. The Vendor will perform and manage the configuration/customization process and keep the State apprised of its progress. The initial configuration/customization plan is part of the implementation cost and not eligible for Change Order or Change Request spending. The Configuration Management Approach specifies: • How the solution will store configurations, including naming conventions and data management (repository design, creation, loading, updating, backup, and recovery). • Baseline • Baseline documents list • Configuration items list • Configuration items compatibility list (version)			
MES-DEL-ARCH-007	Business Rules Configuration Document	The Vendor must provide a Business Rules Configuration Document that describes the capabilities and operation of its Business Rules component. This document should explain the method for setting triggers, criteria evaluation, how to create/modify business rules to meet NC Medicaid requirements, and how actions can be driven off the business rules. It should detail the process by which business rules are maintained, tested, and integrated into operations. The document should also describe how the business rules can be configured without any development/coding effort to maintain separation of duties as per CMS guidance (e.g. business rules are not hard coded).	DDI, O&M	As needed	DED Required
MES-DEL-ARCH-008	User Interface Style Guide	The Vendor must provide a User Interface Style Guide that documents the design standards for the Solution's user interfaces and includes:	DDI, O&M	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		• User ability to customize or make adjustments (e.g. language support, font size) to portal presentation. • Users utilizing scripting languages and/or assistive technology have the ability to access the information, field elements, and functionality required for electronic form or page completion and submission including directions and cues. • User Interface organization so documents are readable without requiring an associated style sheet. • User Interfaces identifying row and column headers for data tables. • User Interfaces informing users when a timed response is required and given sufficient time to indicate more time is required. • User Interfaces providing a method that permits users to skip repetitive navigation links. • User Interfaces provide text titles for frames to facilitate frame identification and navigation. • User Interfaces use markup to associate data cells and row/header cells for data tables that have two or more logical levels of row or column headers.			
MES-DEL-ARCH-009	Business System Design	The Business System Design (BSD) document describes the business process design, application requirements and design to produce a picture of what the new business system functionality, how the new business processes will flow, and what the top-level application structure will be. The BSD document contains the following information: • Subsystem overview • Design Baseline • Business process scope • Organizational scope • Design assumptions and constraints • Business volumes and service levels • Business Process Model Summary • Business process hierarchy • Business process flows/workflow description • Event / Result definitions • Elementary business process descriptions/business rules	DDI, O&M	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		• Business volumes • Input forms layout • Application Design and Approach • Top-level subsystem model • Subsystem design (diagram) • Subsystem module definition • Subsystem data • Subsystem Screens, Reports, and Interface layouts – Data rules and edits • Organization model • Role definition and mapping • Location definition and mapping • A list of all local and off-site facilities • A network schematic showing all network components and technical security controls • Interface control documents • A description of each component, including basic functions and the business areas supported • Enterprise system diagrams, including all components, identifying all logic flow, data flow, systems functions, and their associated data storage • A bi-directional traceability to requirements and test plan The Vendor will work with the State to ensure that Business Process Models are maintained to accurately reflect the processes supported by the Vendor's solution. Upon State request, the Vendor will update and maintain the Business Process Models along with the business process information stored within the iServer tool.			
MES-DEL-ARCH-010	System Design Document	Documentation that describes how the functional and nonfunctional requirements recorded in the Requirements Response Matrix transform into more technical system design details from which the system is configured and built. The SDD documents the high-level system design and the low-level design details. The SDD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system,	O&M	As needed	DED Required

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level design details for each system component, including infrastructure, integration patterns, data flows, internal communications, software, system integrity controls, external interfaces, monitoring & observability, and migration technical design (e.g. encryption, data model mapping, entity relationships, security control). The SDD documents and tracks the necessary information required to effectively define architecture and system design in order to give the development team guidance on the architecture of the system to be developed. Design documents are incrementally and iteratively updated during the system development life cycle and include proprietary contractor material. Its intended audience is the project manager, project team, and development team. The Contractor shall provide and maintain system design documentation that includes at a minimum: • A description of each component, their purpose, including basic functions and the business areas supported • User stories/use cases • User interface design • A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage • Configurations • Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures. • Listing of the edits and audits applied to each input item and the corresponding error messages. • Narrative descriptions of each of the reports and an explanation of their use must be presented. • Definition of all fields in reports, including a detailed explanation of all report item calculations.			
MES-DEL-ARCH-011	User Interface/App	The Vendor must provide the User Interface (UI) solution and activities includes accessibility, browser support, error	DDI, O&M	As needed	DED Required

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
	lication Design	handling, digital media support, and other technical and operational expectations, including access capabilities to various data elements, some of which reside in other systems, but not limited to: • Support for preferred stakeholder communication methods • Utilization of human-readable URLs as navigational aids within browser-based components • Compliance with applicable State and federal accessibility requirements • Development and maintenance of a user-friendly, role-based configurable User Interface • Management of cookies to ensure any generated, used, or required by the solution do not contain user identifiable data • Access and error messages that are understandable to end-users • Validation, editing, and verification of form field data			
MES-DEL-ARCH-012	Section 508 Compliance Test Report	The Vendor must provide a completed Vendor Product Accessibility Template (VPAT) in accordance with Section 508 of the Rehabilitation Act, using the most current VPAT available at the time of submission, whenever there are changes to the User Interface. Third-party attested VPATs do not require separate accessibility testing documentation. Self-reported VPATs must include documented test results demonstrating conformance with WCAG Level AA, as adopted under Section 508 and in effect at time of completion.	DDI, O&M	As Needed	None
MES-DEL-AI-001	GenAI Disclosure and Fact Sheet	The Vendor must submit and maintain the GenAI Disclosure and Factsheet using the Department provided template.	DDI, O&M	Annually	None
MES-DEL-CC-001	Call Center Scripts	Scripts used by Vendor Call Center agents and staff when speaking with Providers and authorized representatives. Each individual service line must have a script. They are clear and easily understandable and reflect the specific requirements, policies, and procedures of the North Carolina market.	DDI, O&M	Annually	None
MES-DEL-CC-002	IVR Scripts	Scripts used by the Vendor call center's IVR system that are maintained, secure, and user friendly. These scripts are used by the system to respond to inquiring using a telephone menu and response system.	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
PDM-DEL-CC-003	Provider Complaint System Policies and Procedures	The Vendor must submit its Provider Complaint System policies and procedures to NCDHHS for review according to the process defined by the Department. The Vendor must make available electronically its Provider Complaint System policies and procedures. This information must include, but not be limited to, specific instructions about how to contact Vendor's Provider Services to file a complaint and which individual(s) have the authority to review and resolve a Provider complaint.	DDI	As needed	None
MES-DEL-CERT-001	Certification Plan	Document which defines the Vendor's approach to CMS certification. It must include supporting the State with the following: The processes and procedures that will be used to manage certification requirements throughout the project lifecycle • Intake form • Complete certification phase deliverables • Solution functionality validation against Conditions for Enhanced Funding • CMS-required and State-specific outcomes • Deliverables traceability to Appendix B - Required Artifacts List found in the CMS Streamlined Modular Certification (SMC) Guidance document at https://cmsgov.github.io/CMCS-DSG-DSS-Certification/SMC%20Guidance.pdf • Operational Reporting Workbook • The process the vendor will use to support CMS Certification Life Cycle The Certification Plan must comply with the most current SMC process to ensure the system will meet all certification requirements.	DDI	As needed	None
MES-DEL-CERT-002	CMS Operational Report Workbook	The Vendor must submit monthly operational reports and data to the Department that support the module in CMS certification and utilize the most updated CMS templates. The Operational Report Workbook deliverable requires a flexible solution that can be updated as directed by CMS that allows the state to pull the reports as needed. These reports must demonstrate the continuous achievement of the module's required and desired outcomes through the delivery of the new module and include data and metrics. The Department may also use these reports to support funding requests as needed and to provide CMS with early	O&M	Monthly	State-Provided

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		and ongoing insight into program evaluation and opportunities for improvement.			
MES-DEL-CERT-004	Operational Readiness Review Checklist	Checklists that will examine the actual solution characteristics and the procedures of the product's operation to ensure that all testing, hardware, software, resources, procedures, and user documentation accurately reflect the deployed state of the system.	DDI	As needed	DED Required
PDM-DEL-CERT-005	Credentialing Policy Deliverable – Annual Deliverable	The Vendor must provide a Credentialing Policy which adheres to state, federal, and NCQA standards. The Policy must include: a. Internal Quality Improvement Plan • Defined goals and process for assessing performance • Analysis of quality activities • Follow-up activities b. Confidentiality Policies and Procedures c. Credentialing Information Integrity Policies and procedures • Auditing, documenting, and reporting of information integrity issues • Annual training for credentialing staff • Annual audits d. Delegated Entity Pre-delegation Evaluation and Monitoring Processes e. Credentialing Verification Process • The process for making credentialing and recredentialing decisions. • The process for managing credentialing files that meet and do not meet the organization's established criteria. • The criteria for practitioner sanctions, complaints and other adverse events found during ongoing monitoring that need to be reviewed by the Credentialing Committee or other designated peer-review body. • Credentialing Committee Meeting Procedures	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
PDM-DEL-CERT-006	Provider Credentialing Committee Bylaws	The Vendor must create and maintain Bylaws for the Credentialing Committee subject to the approval of the Department. The Bylaws must cover: • The Charter and Purpose of the Credentialing Committee • The criteria used in the process to automatically approve or deny applicants and providers • The criteria for risk level determination for an applicant or provider • The data sources to be consulted in the consideration of applicants and providers • References to the statutory authority, regulatory authority, NCQA standards and best practices that inform the Bylaws, policies and procedures of the Credentialing Committee • The rights of applicants and providers to appeal and file grievances • The voting and non-voting membership of the committee • The term, roles and responsibilities of committee members • Confidentiality, Conflict-of-Interest, and non-discrimination requirements • The schedule of Credentialing Committee meetings, which should be at least weekly and must keep up with the level of applications and revalidations to assure timely consideration of applicants and providers • Preparation of Credentialing committee materials, including profile packages for medium- and high-risk providers. • Training of Credentialing Committee members • Record-keeping and Committee communications • Method for maintaining and amending the Bylaws	DDI, O&M	Annually	State-Provided Template
PDM-DEL-CERT-007	Operational Performance Reports	The Vendor must provide summary and detailed level Operational Performance Reports delivered to the Department, at agreed upon intervals, pertaining to provider enrollment, disenrollment, termination, re-enrollment, revalidation, recertification, provider-initiated change request and credentialing status as well as SLAs and other provider maintenance and credentialing activities as specified.	O&M	Per Contract Agreement	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-COMM-001	DDI Communicati on Plan	Document to provide a description of the communications that will occur on the project and how it will be managed. This includes details about various types and means of communication, communication channels, communication flow within the organizational structure, escalation, guidelines for meetings, dissemination of knowledge, and communication effectiveness. It must include, but is not limited to: • A defined approach and actions to engage stakeholders throughout the life of the project • Information communications • Information communication requirements/needs • How, where, and when communications will occur • Who will provide/receive the communication • The purpose of communications • The title of communications • Meeting protocol procedures—noting when minutes are taken etc. • Stakeholder communications approach—to include interactions among the State and other Stakeholders Updates/modifications to the DDI Communication Plan, as mutually agreed, will occur as needed.	DDI	One time on strategy with quarterly updates on any additional needs.	None
MES-DEL-COMM-002	Operations Communicati ons Plan	This document will define the methodology for engaging users and stakeholders during the Operations Phase to promote adoption of the new system. It will describe the processes to ensure timely and effective communication, training, and support to facilitate user interaction with the system. The plan must include: • User communication strategies • Identification of user needs and requirements for system interaction • How, where, and when user engagement and training will occur (including hands on training sessions) • Roles and responsibilities for providing and receiving user-related communications	O&M	One time on strategy with quarterly updates on any additional needs.	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Meeting protocols to address user feedback and system updates—including documentation of key decisions - Interactions among the State, the Vendor, and other stakeholders to support user adoption - The Vendor's approach to raising awareness of system features and benefits following Contract award; and the facilitation of ongoing user engagement and system adoption efforts - Reporting and escalation of user-related issues—to include reporting of system usability concerns and adoption challenges			
MES-DEL-DATA-001	Data Management, Conversion, and Migration Plan	Document that describes how the Vendor will convert and migrate all required data from existing systems into the Solution and includes the following: - A data management strategy that will support integration, optimization, quality, stewardship, standards, and align with the Department's Data Governance processes. - Description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed. - Approach to conversion, cleansing and migration. - Approach to risk management and security for data conversion effort. - Approach for testing migration or converted data. - Approach to reporting the number of records successfully converted vs. errors or exceptions. - Approach for cleansing and validating data to prepare it for loading to the proposed solution that is refined as necessary. - Approach to resolving data conversion errors and issues. - Approach for supporting the Department validation of converted data. - Tasks, timelines, and responsible parties for all conversion and migration tasks. - Entrance and exit criteria for each phase of the effort.	DDI	As needed	DED Required

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-DATA-002	Data Conversion Test Results	Document containing test results for each test run during migration of historical data from the current solution to new Solution. The test results include: • Executed test cases • Mapping of executed test cases to the associated requirement • Mapping of executed test cases to their artifacts and results • Executing tester for test case • Date of execution • Pass/fail status • Balancing reports that account for all input data being transformed to output data and identify anomalies for resolution • Exception reports that identify data which fails the conversion process Data Conversion will not be considered complete until the Department validates successful data conversion through these reports.	DDI	As needed	None
MES-DEL-INT-001	System Interface Design Strategy	Document that describes: • how interface requirements are gathered • how top-level designs are defined and responsibilities assigned • how detailed designs are determined and created • how interface tests are identified, created and executed • how defects or data exchange failures are escalated for quick resolution • how interface creation is managed and executed • how interfaces are maintained and monitored • any other key features of the Vendor's Interface Design Strategy The document must also include the template the Vendor will use and populate during the interface design sessions. That template must minimally gather: • data exchanges and contact points between the MIS and the Vendor	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		• interface frequency • method of data exchanges • interface requirements Additionally, the Vendor must work with the Medicaid Integration Services (MIS) on how the Vendor will coordinate with the MIS to achieve all product requirements.			
MES-DEL-INT-002	Interface Control Documents	Document which details all interfaces and will include data layout documentation, data mapping crosswalk, inbound/outbound capability, business rules, and frequency of all interfaces. This document will be used to request State approval of the integration or interface prior to the start of this development work. Source to target mappings should be provided in Excel format as Addendums to the Interface Control Document.	DDI	As needed	State-Provided
MES-DEL-OM-001	Operations, Maintenance and Configuration Plan	Document that describes post-implementation processes for areas such as: • Architecture/hosting operations. • Monitoring daily operations performance. • Performing routine maintenance. • Maintaining user documentation. • Online help approach and documentation, as appropriate. • Approach to enhancements and other new requirements. • Maintaining system documentation. • Archiving requirements. • Process improvement • Performance metrics (which ones will be measured, how the measurements will be collected and reported on, and what happens if something exceeds an acceptable threshold, document performance optimization techniques used) • Risk and issue management plan • Resource management • Software testing and system engineering, O&M defect management The above areas will be included in the plan, either by incorporating the topic in the document or referring to other	DDI, O&M	Quarterly	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		stand-alone documents. Roles and responsibilities of the State and Vendor will be clearly delineated.			
MES-DEL-OM-002	Capacity Plan	Document that describes, at a minimum, the number of concurrent users supported, number of transactions, storage capacity, throughput volume, scaling, availability and how it will be continuously monitored during operations and maintenance.	DDI	As needed	None
MES-DEL-OM-003	Decommission Recommendations Report	The Vendor must review and identify monthly, any unneeded hardware, software, and licenses, present recommendations to the State for review and ensure that any unneeded hardware, software, and licenses have been decommissioned upon approval from the State.	O&M	Monthly	None
MES-DEL-OM-004	Operations Procedure Manual	Document that provides guidelines for the operation and use of the module and/or module component(s). At minimum the Operations Procedure Manual shall contain policies, processes and workflows for the module and/or module component(s). The manual shall contain Contractor staff procedures for: - Processing of applications - Ongoing Monitoring - Appeals and Hearings - Returned mail - Federally mandated screening (site visit) - New Medicaid Provider training The manual must also include a mapping of all Provider Credentialing requirements to the applicable procedures	DDI, O&M	Quarterly	DED Required
MES-DEL-OM-005	Release Management Plan	Document that describes the approach to work with the Department or impacted Department Contractors, and the MES PMO with the objective of a 60-day lead time for releases. The document should also contain details on the Vendor's approach to managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases.	DDI	As needed	DED Required
MES-DEL-OM-006	Turnover Plan	Document submitted at least nine (9) months before the end of the final Contract year (including option years that have been exercised), or within a timeframe specified by the Department in the event of early contract termination, that includes:	O&M/Turnover Period	As needed	DED Required

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Proposed approach to turnover, including established roles and responsibilities between Vendor and State team. - Tasks and subtasks for turnover. - Schedule for turnover and contingency plans - Updated operational tasks and procedures during turnover. - Description of vendor coordination activities that will occur during the turnover task and implementation of the activities to ensure continued system and services as deemed necessary by the Department. - List of incomplete tasks, such as system defects, modifications or enhancements, reference updates, and configuration requests. - A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The description shall also include an estimate of the number and type of personnel required to support the technical platform and supporting services. - The data and documentation shall be organized in a format required by the State - The conversion and migration of all pertinent information and work in progress, leases, etc. .			
MES-DEL-PM-001	Project Management Plan	Document to provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how information will be communicated with the project. It will serve as a reference for decisions and clarifications as well as define how all project activities will be executed, monitored, and controlled. This document describes the processes for ensuring adherence to State, NCDHHS, and federal policies, standards, guidelines, and procedures. The document will also include: - Project charter - Project budget and adherence thereto - List of all known assumptions, risks and risk mitigation strategies, and target resolution dates	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-PM-002	Quality Management Plan	Document that identifies what defines quality, the quality standards for the project, how those quality standards are measured, and how the quality of all submissions to the Department will be ensured and maintained. It includes the process steps and quality tools that will be used (i.e. templates, standards, and checklists).	DDI	As needed	None
MES-DEL-PM-003	Risk and Issue Management Plan	Document that describes how risks and issues will be monitored, maintained and acted upon throughout the project in accordance with Section 7.11.13 of the RFP. The document must contain the following: • Proactive identification and analysis of risks before they become issues. • Roles and responsibilities • Development of risk avoidance, transfer, mitigation or management strategies. • Approach to monitoring, communicating, reporting of risk and issue status including procedures for documenting, resolving, and reporting issues and risks identified by the Vendor, the Department or other project contractors. • Approach to impact analysis. • Approach to root cause analysis. • The appropriate methods, tools, and techniques for active and ongoing identification and assessment of project risks. • Describe how risks will be quantified and qualified. • Describe the plan for timely notification to the Department of any changes in risk or trigger-of-risk events.	DDI	As needed	None
MES-DEL-PM-004	Change Management Plan and CR Approval Process	Document that describes how changes will be initiated, submitted, assessed for impacts, reviewed, approved, or rejected throughout the life of the project. Applicable changes include alterations to project's budget, requirements, scope, and schedule. The plan must align with the Department's formal process and include the following: • Approach to coordinating with any other Department Contractor that may be impacted by or have a dependency on the change • A process flow that clearly outlines the life cycle of a CR • Roles and responsibilities	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Approach to monitoring change requests through their lifespan to ensure timely resolution - Approach to communicating changes to internal and external stakeholders - Approach to status tracking and escalation for at-risk CRs			
MES-DEL-PM-005	Requirements Traceability Matrix (RTM)	The Vendor must develop, maintain, and submit a Requirements Traceability Matrix (RTM) to show bi-directional traceability with applicable testable and non-testable contractual requirements and their realization throughout all project phases (e.g., requirements, design, testing and Streamlined Modular Certification (SMC) items). This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State and linked back to the approved change request. The Vendor's RTM must follow the guidelines provided by the Department. For any Commercial off the Shelf (COTS) or Software as a Solution (SaaS) systems, the initial RTM will also include a Gap Analysis that details any discrepancies between the initially configured solution and the RFP's business requirements.	Contract Award	Aligned with Project Milestones	DED Required, State-Provided
MES-DEL-PM-006	Project Work Plan	Document which details a comprehensive work plan, with Gantt Chart, aligned with the project scope and Department requirements. The document must include: - Identify planned completion dates for all deliverables and milestones. - Include key elements for the Department's Integrated Master Schedule (IMS), such as major phase dates, milestones, vendor integration points, and cross-module dependencies. - Be regularly updated and refined throughout the project, with baseline schedules maintained for comparative reporting. - Reflect any approved changes through the Change Request Management Process and be re-baselined as needed.	DDI	Weekly	State-Provided
MES-DEL-PM-007	Agile Approach	Document that describes the Vendor's overall agile methodology and approach to program increment (PI) planning and sprint planning that includes, at minimum: Defined roles and responsibilities	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Number of agile ceremonies (sprints, feature refinement, design sessions) - Program increment planning – provide a PI Schedule and describe what the Vendor does within a PI - Description of tools used during program increments and sprints - Backlog management prioritization process – how product backlogs are refined, prioritized, and maintained - Definition of “Done”- how to ensure consistent quality and completion criteria across features, stories and releases - Integration and testing approach – how continuous integration, test automation and quality gates are embedded in sprints			
MES-DEL-PM-008	SLA Assessment Report	The Vendor must minimally include the following in SLA assessment reports: - Vendor not meeting SLA - SLA number not being met - Evidence used for determination - Date SLA became out of compliance - Resolution Process (if known) - Planned Resolution Date (if known) - Criticality Level - Escalation Required (Y/N) - Corrective Action - Log and Aging Report for all Resolution Efforts	DDI, O&M	Monthly	None
MES-DEL-PM-010	Project Performance Measures	Document that provides performance measures related to ongoing project progress. It describes how the performance measures and success criteria will be monitored and reported on throughout the project lifecycle. At a minimum, these measures shall relate to scope, schedule and budget performance areas. Additionally, the document contains project performance measures that will be used to determine if the stated project objectives have been met by the close of the project. These measures should be specific, measurable, and attainable within the project scope, time, and budget.	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-PM-011	Implementation Cutover Plan	Document which provides a more detailed view of the high-level tasks, pre-launch cutover tasks captured in the project schedule and must be kept in sync with that document. The Plan will contain the following information: • The rollout approach • Overall integration approach • Approach to continuous integration of other modules or data from other data providing entities. • The proposed Implementation Schedule. • The rollback strategy. • Communication and Contractor support procedures. • Contractor and State roles and responsibilities. • Operational Readiness Checklist(s) that defines, in advance, the go/no-go decision, and all aspects of Contractor, solution, and State readiness. • All critical tasks that are required for cutover. • Post cutover monitoring. • The onsite (upon approval by state team) and offsite user support provided by the Contractor and State during the initial solution implementation. • Solution acceptance procedures. • Tools and processes to ensure overall quality. • Describe post implementation production deployment process and activities. • Post-implementation evaluation (includes metrics for measurement of successful implementation)	DDI	As needed	DED Required
MES-DEL-SEC-001	System Security Plan	Document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The Plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems. The document will use industry-standard templates such as FedRAMP or NIST, to ensure alignment with compliance requirements.	DDI, O&M	As needed	None
MES-DEL-SEC-002	Privacy & Security Incident	Document that contains a plan to manage privacy and security incidents with established processes that minimally:	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
	Management Plan	- Detect and identify events. - Triage and analyze events to determine whether an incident is underway. - Respond and recover from an incident. Improve the organization's capabilities for responding to a future incident.			
MES-DEL-SEC-003	Business Continuity Plan	Document providing details for a business continuity plan that must include the following: - Procedures for activating any special teams for business continuity. - A plan for recovery of business functions, units, processes, human resources, and technology infrastructure. - Communication protocols and process for restoring operations in a timely manner. The document must also include identification of the core business processes involved in the production solution. For each core business process include: - Identification of potential failures for the process. - Risk analysis - Impact analysis and Definition of minimum acceptable levels of service/output. - Definition of triggers for activating contingency plans.	DDI, O&M	Annually	None
MES-DEL-SEC-004	Disaster Recovery Plan	Document providing details for a disaster recovery plan that must include the following: - Retention and storage of backup files and software. - Hardware backup for critical solution components. - Facility backup. - Backup for any telecommunications links and networks. - Backup procedures and support to accommodate the loss of any online communications. - A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility. - The off-site storage facility must provide security of the data stored there, including protections against unauthorized access or disclosure of the	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		information, fire, sabotage, and environmental considerations. • An enumeration of the prioritized order of restoration for Contractor's proposed solution. • Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss			
MES-DEL-SEC-005	Privacy Impact Analysis	Document that details the privacy impact of each module or module component that includes the following information: • Use of personally identifiable information (PII) or personal health information (PHI) and a description of the types of data that will be collected • Sources of PII/PHI, populations, and transfer and disclosure mechanisms • Legal environment (legal authorities and state privacy laws) • Details about the entities with which the collected information will be shared • Privacy and security standards for its business partners and other third parties and the agreements that bind these entities • Incident handling procedures • Privacy and/or security awareness programs and materials for its workforce	DDI, O&M	As needed	None
MES-DEL-SEC-006	Third Party Privacy Security Assessment	The Vendor must provide access to the infrastructure and systems for the State-hired third-party vendor to perform the privacy & security assessments in compliance with the latest NIST 800-53 requirements overlaid with the HIPAA privacy & security requirements and the penetration testing . If the Vendor has obtained a HITRUST CSF for their solution (not the cloud service provider HITRUST CSF), the State may accept the HITRUST CSF as an equivalent for 3rd Party Privacy Security Assessment. The Vendor needs to provide detailed HITRUSTCSF assessment reports, not just a certification letter	DDI, O&M	Every other year	None
MES-DEL-SEC-007	Disaster Recovery/Business Continuity Test Report	Report which contains the test results of an annual test of the Disaster Recovery Plan and Business Continuity Plan. The report includes the After-Action report, test results, outcomes, corrective action plan, and revisions, if any, to the Department.	DDI, O&M	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
MES-DEL-SEC-008	Penetration Test Report	Report from an independent third party which has performed penetration testing within 90 Days prior to implementation. Penetration testing must also be performed by an independent third party on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Penetration Test Report results must be supplied to the Department and critical and high vulnerabilities mitigated.	DDI, O&M	Annually	None
MES-DEL-SEC-009	IT System Risk Assessment	Document which contains results and outputs from an internal risk assessment conducted by the Vendor. The assessment will be in compliance with the latest NIST 800-53 and HIPAA privacy & security controls. The assessment will be performed on an annual basis and when additions or changes to system functionality impact the security framework, architecture or when a new vulnerability exists. The results and outputs of the assessment will be documented and submitted to the State.	DDI, O&M	Annually	None
MES-DEL-SEC-010	Service Organization Control (SOC) 2 Type II Report	The Vendor must provide a completed Security Audit Report with results to the Department by the 30th of September each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE - 18 at a minimum level service organization control (SOC) 2 Type II or current NIST 800-53 assessment at a "moderate" system risk control level.	O&M	Annually	None
MES-DEL-SEC-011	CMS Information Security Program Plan of Action and Milestones (POA&M)	The Vendor must respond to all risks identified through the periodic security risk assessments with a CMS Information Security Program Plan of Action and Milestones (POA&M) containing clarifying information, a proposed mitigation strategy if necessary, a timeline for implementation, and shall work with the Department to successfully execute the POA&M. The Vendor should use the FedRamp template.	Dependent on the data this is provided and when the system has access to the state PHI and PII data.	Monthly	None
MES-DEL-STAF-001	Staffing Plan	Document containing a staffing plan that must include: - Identify the roles and responsibilities by resource type throughout all phases of the contract, including identifying key and non-key personnel as well as FTE allocation for all personnel. Clearly differentiate between Vendor staff and - subcontractor staff. - Provide estimated staffing levels by resource type for each project phase	DDI, O&M	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Detail how the staffing levels shall achieve consistent, dependable service regardless of changes that may influence work volume. - Identify total hours to be expended, per phase or effort, and for the entire project, by Vendor staff and by State project staff. - Tools and processes used to screen available staff and fill positions. - Expectations regarding onsite time for Vendor resources - Process for temporary and permanently replacing vacancies in key personnel and other manager/lead positions - Detail how the staffing levels shall achieve consistent, dependable service for handling sudden and unexpected increases in volume of transactions or the number of users.			
MES-DEL-STAF-003	Key Personnel Resume	The Vendor must provide a detailed resume for a proposed key personnel replacement that demonstrates the minimum qualifications for the role are met. Replacements are subject to Department approval prior to any assignment.	DDI, O&M	As needed	None
MES-DEL-TST-001	Master Test Plan	The Vendor must develop, submit, and maintain a Master Test Plan that describes the Vendor's plan for all testing activities, processes, types, and levels. Testing must be as automated and self-documenting as possible (e.g., continuous unit testing). This plan must be aligned with CMS's Testing Guidance Framework. At a minimum, the Master Test Plan must address the following: - Overall testing strategy for the testing types defined in Section 7.17 of the RFP - Approach to planning and preparing the necessary environments as described in Section 7.17 of the RFP. - Approach for testing nonfunctional requirements. - Approach to test documentation - Approach to quality control/quality assurance. - Tools, techniques, and methods. - Reporting mechanisms, traceability, and metrics. - Defect management including Approach and tools utilized to collect, assign, identify, prioritize, track,	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		manage, resolve, and test system defects reported by the Department, other Department Vendors or other personnel authorized by the Department. -Approach to defect severity categorization. -Approach to reporting and documenting defects. Defect reports should include at a minimum the current defect list (with frequency and severity), associated implementation timelines, and information on operational impact. • Describe aging information to track how long defects are taking to resolve. • Describe the defect management processes related to all test types and levels in Section 7.17 of the RFP (e.g., the relationship between defect resolution and the coordinated test case execution). • Describe the defect management processes after implementation. • Entrance and exit criteria for each test level • Configuration management for each test level • Testing roles and responsibilities for vendor and Department • Acceptance Criteria • Test Coverage • Walkthroughs, Inspections, and Demos • Test Data Considerations • Inputs to and outputs of System Testing • Pass/Fail Criteria • Suspension Criteria and Resumption requirements • Meetings and Communication • Applications or systems that are part of the testing • Integrations that are part of the testing • Test environment build and maintenance • Test scenario, case, and result traceability to contract requirements • Test schedule • Approach to working collaboratively with other State healthcare programs enterprise Vendors. • Constraints and assumptions and all associated dependencies			

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		- Approach to testing compliance with Section 508 accessibility requirements - Testing scope, including what is out of scope			
MES-DEL-TST-002	Performance Test Results	Document providing test results demonstrating that the solution meets all Service Level Agreements for system performance.	DDI	As needed	None
MES-DEL-TST-003	Test Results	Document providing testing results for each applicable test phase listed in Section 7.17 Testing that include: - Executed test cases - Mapping of executed test cases to the associated contract requirement - Mapping of executed test cases to their artifacts and results - Executing tester for each test case - Date of execution - Pass/fail status - Registry of open, closed, and deferred defects - Screenprints, test results, and artifacts No test phase will be considered complete until the Department reviews and approves of the testing results. Depending on the testing methodology, these results may be submitted in phases.	DDI	As needed	None
MES-DEL-TRN-001	Training Plan and Schedule	Document that describes the Vendor's cohesive and responsive training to ensure that all users can be efficient and effective while using the system, including State staff and external users. The plan reflects the relative lead-time for the development of training materials prior to conducting training classes (including the training of testing participants and all training before implementation); how users' skills will remain current throughout the operations phase; and how the Vendor will build and maintain the training environment. Additionally, it specifies the planned duration of implementation training rollout, including development of Desk Procedures (User Manual) for use in the Operations Phase. The plan specifies delivery media to be used for each training activity and the accessibility of training materials and/or training news before, during, and after training. It describes the process used to identify and track training	DDI	Annually	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		needs and to evaluate trainee feedback to improve course materials and methods. The Training Plan will be updated annually to define the approach and actions to engage stakeholders during training to address specific training activities for the upcoming year and shall be completed at least ninety days prior to the beginning of the Contract year. The Plan must also include the following: • User Data: The Contractor must develop a User Training Plan that explains the data available to each user type and how to sign on and access that data. • Department Call Center: The Contractor shall provide training to State staff in the use of the Customer Call Center System, initially and on an ongoing basis, as defined by the Department. • Summary of training approach that focuses on the train-the-trainer methodology, objectives, and desired outcomes. • Training needs analysis, including an assessment of the target audience and their knowledge and skills. • Recommendations on type and delivery approach based on training needs analysis. • Summary of proposed training materials and documentation in addition to hands-on training. • Approach to maintaining training documentation and accompanying materials. • Approach to providing training necessary to support new functionality and/or major software releases that materially change the user interaction. • Approach to processing for incorporating feedback to improve train the trainer effectiveness over the course of the Contract. • Approach to conducting dry runs for training sessions.			
MES-DEL-TRN-002	Training Guides and Materials	The Vendor must submit Training Guides and Materials that include a comprehensive set of training documentation and learning content, covering all materials needed to train Vendor staff, State staff, providers, and external users on the new technology. These guides and materials ensure all	DDI	As Needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		stakeholders can effectively adopt and use the system by go-live. The deliverable is intentionally open-ended in format – it may include user manuals, step-by-step “how-to” guides, presentation slide decks, e-learning modules, quick reference cards, or other media – to accommodate different training methods (instructor-led sessions, self-paced online tutorials, etc.) that are secure, browser-based, and web-enabled as directed by the State. The Contractor shall produce State-approved initial and ongoing updates to training materials and assess the training needs of end users prior to implementation by meeting with subject matter experts for the different functions to be performed and will design training methods that will meet or exceed the established goals as identified in the training requirements.			
MES-DEL-TRN-003	Functional Design Documentation	The Vendor must provide User Documentation during the DDI phase of the project for use during UAT and maintained throughout the project for final review and submission prior to Go Live. The State requires User Documentation for use by a novice business user to understand the automated system or application from a business function perspective. The Vendor must provide comprehensive, well-organized user documentation. The Vendor's User Documentation must include at a minimum: • User documentation must be written and organized so that novice users can learn from reading the documentation how to access the on-line windows/screens, read reports, and perform all other user functions. Should be written in a procedural step-by-step format. (Instructions for sequential functions must follow the flow of actual activity). • Manuals that help users understand the purpose and operation of the module/module component(s) for each business process/major program/functional area. Should cover system navigation, online help, and policies and procedures. • Acronyms and abbreviations used in user instructions must be identified and must be consistent with windows, screens, reports, and the data element dictionary. • The documentation must be available on-line and provide an on-line search capability with context-sensitive help.	DDI	As Needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		• Provide the ability to produce a PDF version upon request • Use version control to retain historical versions of documentation and revisions must be clearly identified. • User manuals must contain a table of contents and an index. • Definitions of codes used in various Sections of a user manual must be consistent. • Descriptions of error messages for all fields incurring edits must be presented and the necessary steps to correct such errors must be provided. • Each user manual must contain a Section describing all reports generated within the subsystem, which includes the following: ○ A narrative description of each report. ○ The purpose of the report. ○ Definition of all fields in the report, including detailed explanations of calculations used to create all data and explanations of all subtotals and totals. • Definitions of all user-defined, report-specific code descriptions; and a copy of representative; and pages of each report. • Instructions for requesting reports or other outputs must be presented with examples of input documents and/or screens. • Instructions for making on-line updates must clearly depict which data and files are being changed.			
MES-DEL-TRN-004	Training Evaluation Report	The Vendor must develop a Training Evaluation Report that details the results, findings, interpretations, conclusions, and recommendations derived from the training evaluation. This report will include an analysis of the training and its intended outcome to ensure that the training was delivered effectively and efficiently to all users, including the Vendor staff, State staff, Providers and external users. The Vendor will collect feedback from the users to assess whether the training achieved its intended outcome, and if the training materials and resources used aligned with or met the training objectives and needs of the users. Also, the Vendor will	DDI	As needed	None

Deliverable ID	Title	Description	Phase/Stage	Frequency/Updates	Template
		document any training gaps, lessons learned, and opportunities for improvement in the evaluation report			
PDM-DEL-WKF-001	Workflow Configuration Document	The Vendor must provide a Workflow Configuration Document that describes the use of workflow templates in the Vendor's solution. This document should describe how workflows are identified, the tools used to markup and configure workflow rules, the capability to identify manual and automated workflow actors, how workflow task lists and histories are maintained, and other key data relevant to the operation of defined workflows.	DDI	As needed	None

Table N-1 Deliverables

2.0 MILESTONES AND ACCEPTANCE CRITERIA

The milestone information shown in *Table N-2 Milestones* includes defined milestones (“events”) representing meaningful progress points during the execution of the DDI phase of the PDM/CVO Solution project. The Vendor must provide the duration associated with each milestone in Table N- 2 Milestones to support the reasonableness of the proposed schedule. The Vendor must also provide the proposed payment for each milestone in sheet 2. Milestone Costs Payments included in the Cost Proposal Workbook.

Each milestone includes:

- ID: Identifier of the milestone
- Milestone: Name of the milestone
- Scope: Scope of the of the activities to be completed during the milestone.
- Acceptance criteria: Criteria required to be met before milestone considered complete.
- Deliverables: Deliverables that must be submitted and approved in PCDU.
- Prior Milestones: The milestone(s) that are required to be completed before the current milestone can be approved.
- Duration: Number of weeks to perform the milestone activities and meet the acceptance criteria for the milestone. Vendor required to provide this information as part of proposal submission.

These milestones will form the basis for a significant portion of the project’s payment schedule. Milestone payments will be made only upon the Department’s approval the milestone has been fully achieved in accordance with acceptance criteria provided. For specific deliverables referenced in multiple milestones where the acceptance criteria indicate only relevant sections of the specific deliverable will be reviewed, the relevant sections of the deliverable to be reviewed will be identified and mutually agreed upon by the Vendor and the Department prior to deliverable submission.

Following the award of the contract, the State will work with the Vendor to finalize the timeline and milestones. Any changes to the milestone schedule, acceptance criteria, or associated payments will require a formal contract amendment approved by the State.

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
1	DDI	Planning Complete	Define project scope, timelines, resources, and governance. Assess current state, gather requirements, identify gaps.	Relevant deliverables approved by stakeholders. Roles and responsibilities assigned. Interface Design Strategy finalized and signed off. Requirements documented.	• (MES-DEL-PM-001) Project Management Plan • (MES-DEL-PM-006) Project Work Plan • (MES-DEL-PM-007) Agile Approach • (MES-DEL-STAFF-001) Staffing Plan • (MES-DEL-PM-002) Quality Management Plan • (MES-DEL-COMM-001) DDI Communication Plan • (MES-DEL-PM-003) Risk and Issue Management Plan • (MES-DEL-PM-010) Project Performance Measures • (MES-DEL-PM-004) Change Management Plan and CR Approval Process • (MES-DEL-SEC-002) Privacy & Security Incident Management Plan • (MES-DEL-PM-005) Requirements Traceability Matrix (RTM) (Relevant Parts finalized, s1) • (MES-DEL-INT-001) System Interface Design Strategy • (MES-DEL-AI-001) GenAI Disclosure & Factsheet • (MES-DEL-STAFF-003) Key Personnel Resume	None	
2	DDI	Infrastructure - Design and Approvals Complete	Design target infrastructure architecture and get necessary approvals.	Relevant deliverables approved.	• (MES-DEL-ARCH-005) MES Architecture Documentation (Initial) • (MES-DEL-ARCH-010) System Design Document (Initial)	Milestone 1 Complete	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
					• (MES-DEL-OM-002) Capacity Plan • (MES-DEL-SEC-001) System Security Plan (SSP) • (MES-DEL-SEC-005) Privacy Impact Analysis • (MES-DEL-ARCH-011) User Interface/ Application Design • (MES-DEL-ARCH-009) Business System Design • (MES-DEL-TST-001) Master Test Plan • (MES-DEL-CERT-001) Certification Plan • (MES-DEL-OM-005) Release Management Plan		
3	DDI	Capabilities and Training Enablement - Disaster Recovery and DevOps Set up	Implement DR strategy and configure backup/recovery. Set up CI/CD pipelines, version control, and automation tools.	DR environment configured and tested successfully. DevOps pipelines operational and integrated with source control.	• (MES-DEL-SEC-004) Disaster Recovery Plan • (MES-DEL-SEC-007) Disaster Recovery/Business Continuity Test Report • (MES-DEL-SEC-003) Business Continuity Plan • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Parts finalized,s2) • (MES-DEL-ARCH-010) Technical Design Document (Relevant Parts finalized,s2) • (MES-DEL-ARCH-006) Configuration/Customization Plan • (MES-DEL-TRN-001) Training Plan and Schedule	Milestones 1 and 2 Complete	
4	DDI	Capabilities Enablement and Reports and Dashboards Complete - Data Management,	Set up automated testing for data quality and pipelines and establish data management and governance. All capabilities fully deployed and validated.	Tests implemented and passing in Configuration items/Configuration Data. All milestones completed and signed off. Reports and	• (MES-DEL-ARCH-007) Business Rules Configuration Document • (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Initial)	Milestone 1, 2, and 3 Complete	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
		Governance, and Automated Testing Set Up	Finalize development of reports and dashboards.	dashboards validated against legacy outputs.	• (MES-DEL-CERT-004) Operational Readiness Review Checklist • (MES-DEL-ARCH-005) MES Architecture Documentation (s3, All Parts finalized) • (MES-DEL-ARCH-010) Technical Design Document (s3, All Parts finalized) • (MES-DEL-PM-005) Requirements Traceability Matrix (RTM) (Relevant Parts finalized, s2) • (MES-DEL-ARCH-001) Data Architecture • (MES-DEL-ARCH-004) Data Architecture Document - Logical Data Model (LDM) Document • (MES-DEL-ARCH-002) Data Architecture Document - Conceptual Data Model (CDM) • (MES-DEL-ARCH-008) User Interface Style Guide		
5	DDI	Conversion - Data Conversion and Document Migration Complete	Document and catalog all converted data assets. Convert historical and current data to target platform. Complete document migration.	Data catalog and glossary updated and published. Data conversion completed with reconciliation and validation. Document migration completed with reconciliation and validation.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (s2, All Parts Finalized) • (MES-DEL-ARCH-003) Data Architecture Document - Data Dictionary (Electronic) • (MES-DEL-DATA-002) Data Conversion Test Results (Initial)	Milestones 1 through 4 Complete	
6	DDI	Testing - Security and Penetration Testing Complete	Conduct security assessments and penetration tests.	No critical vulnerabilities found; reports approved.	• (MES-DEL-SEC-008) Penetration Test Report • (MES-DEL-SEC-009) IT System Risk Assessment • (MES-DEL-SEC-006) 3rd Party Privacy Security Assessment	Milestones 1 through 5 Complete	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
					(MES-DEL-ARCH-012) Section 508 Compliance Test Report		
7	DDI	Testing - SIT Complete, Including Reports and Dashboards	System Integration Testing of infrastructure components. SIT for reports and dashboards.	Completion and acceptance of all SIT test results, SIT defect resolution, and functionality in accordance with SIT testing criteria defined in Milestone 2 ((MES-DEL-TST-001) Master Test Plan)	(MES-DEL-TST-003) Testing Results (Initial, Relevant Sections) (MES-DEL-TRN-003) User Documentation	Milestones 1 through 6 Complete	
8	DDI	Testing - UAT Complete, Including Reports and Dashboards	User Acceptance Testing of readiness. UAT for business reports and dashboards.	Completion and acceptance of all UAT test results, UAT defect resolution, and functionality in accordance with UAT testing criteria defined in Milestone 2 ((MES-DEL-TST-001) Master Test Plan)	(MES-DEL-TST-003) Testing Results(Relevant Sections, s2) (MES-DEL-CC-001) Call Center Scripts (MES-DEL-CC-002) IVR Scripts	Milestone 7 Complete	
9	DDI	Final Testing and Cutover - Final Data Migration, Performance Testing, End to End Testing, and Parallel Testing Complete	Validate system performance under load. Full workflow testing from ingestion to reporting. Run legacy and new systems in parallel for comparison. Final sync of data and validation before go-live.	Performance benchmarks met or exceeded, performance defect resolution, and functionality in accordance with performance testing criteria defined in Milestone 2 ((MES-DEL-TST-001) Master Test Plan). Completion and acceptance of all E2E test results, E2E defect resolution, and functionality in accordance with E2E testing criteria defined in Milestone 2 ((MES-DEL-TST-001) Master Test Plan). Parallel Run Results match across systems; discrepancies resolved. Final data load completed and validated.	(PDM-DEL-WKF-001) Workflow Configuration Document (MES-DEL-TST-002) Performance Test Results (MES-DEL-TST-003) Testing Results (s3, All Sections) (MES-DEL-PM-011) Implementation Cutover Plan (MES-DEL-DATA-002) Data Conversion Test Results (s2, Final) (MES-DEL-INT-002) Interface Control Documents (MES-DEL-PM-005) Requirements Traceability Matrix (RTM) (s3, Final) (PDM-DEL-CC-003) Provider Complaint System Policies and Procedures (PDM-DEL-CERT-005) Credentialing Policy Deliverable – Annual Deliverable	Milestones 7 and 8 Complete	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
					• (PDM-DEL-CERT-006) Provider Credentialing Committee Bylaws		
10	DDI	Cutover - Go Live Successfully Completed	Transition to production environment.	System live with monitoring in place and no critical issues.	• (MES-DEL-TRN-002) Training Guides and Materials • (MES-DEL-CERT-002) CMS Operational Report Workbook • (MES-DEL-OM-001) Operations, Maintenance and Configuration Plan • (MES-DEL-OM-004) Operations Procedure Manual • (MES-DEL-COMM-002) Operations Communications Plan	Milestones 1 through 9 Complete	
11	O&M	Weekly Deliverable Submission	Weekly Deliverable	N/A	• (MES-DEL-PM-006): Project Work Plan	N/A	
12	O&M	Monthly Deliverable Submission	Monthly Deliverables	N/A	• (MES-DEL-SEC-011): CMS Information Security Program Plan of Action and Milestones (POA&M) • (MES-DEL-PM-008): SLA Assessment Report • (MES-DEL-OM-003): Decommission Recommendations Report • (MES-DEL-CERT-002): CMS Operational Report Workbook	N/A	
13	O&M	Quarterly Deliverable Submission	Quarterly Deliverables	N/A	• (MES-DEL-ARCH-001): Data Architecture • (MES-DEL-ARCH-002): Data Architecture Document - Conceptual Data Model (CDM) • (MES-DEL-ARCH-003): Data Dictionary (Electronic) • (MES-DEL-ARCH-004): Logical Data Model (LDM) Document • (MES-DEL-ARCH-005): MES Architecture Documentation	N.A	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
					• (MES-DEL-ARCH-006): Configuration/Customization Plan • (MES-DEL-COMM-001): DDI Communication Plan • (MES-DEL-COMM-002): Operations Communications Plan • (MES-DEL-OM-001): Operations, Maintenance and Configuration Plan • (MES-DEL-OM-004): Operations Procedure Manual		
14	O&M	Every Other Year Deliverable Submission	Every Other Year Deliverable	N/A	• (MES-DEL-SEC-006) Third Party Security Assessment	N/A	
15	O&M	March Annual	Every Year in March Deliverables	N/A	• PDM-DEL-CERT-006: Provider Credentialing Committee Bylaws • PDM-DEL-CERT-005: Credentialing Policy Deliverable – Annual Deliverable • MES-DEL-SEC-010: Service Organization Control (SOC) 2 Type II Report • MES-DEL-SEC-009: IT System Risk Assessment	N/A	
16	O&M	June Annual	Every Year in June Deliverables	N/A	• MES-DEL-SEC-008: Penetration Test Report • MES-DEL-SEC-007: Disaster Recovery/Business Continuity Test Report • MES-DEL-SEC-004: Disaster Recovery Plan • MES-DEL-SEC-003: Business Continuity Plan	N/A	
17	O&M	September Annual	Every Year in September Deliverables	N/A	• MES-DEL-SEC-002: Privacy & Security Incident Management Plan • MES-DEL-PM-007: Agile Approach	N/A	

ID	Phase	Milestone	Scope	Acceptance Criteria	Deliverables	Dependencies that need to be met for Milestone to be completable	Duration
					• MES-DEL-AI-001: GenAI Disclosure and Fact Sheet • MES-DEL-CC-001: Call Center Scripts • MES-DEL-CC-002: IVR Scripts		

Table N-2 – Milestones

ATTACHMENT O: BUSINESS CONTINUITY PLAN

Vendor shall provide, in Vendor's response to this RFP, a narrative describing Vendor's approach to business continuity, including the types of information in Vendor's business continuity plan. The narrative should not exceed three (3) pages. A full business continuity plan must be submitted to the Department in accordance with the Implementation Plan.

When due, the Vendor's proposed business continuity plan must address the following:

1. Introduction – Who the plan is intended for and its purpose.
2. Plan Objectives:
 - a. The essential aspects of the business process supported by the system;
 - b. The way to continue business should the system fail;
 - c. The business recovery procedures for return to operations status; and
 - d. A way to convert back to business as usual after the system is available.
3. System Overview – How the application/system operates and its function.
4. Communication Plan Notification – When the application is unavailable, who is notified and how?
5. Roles, Responsibilities, and Authority – List areas of support and roles of staff involved in this process.
 - a. Example 1:
 - i. Application Support:
 - ii. An Application Analyst is responsible for the following:
 - b. Example 2:
 - i. Hardware Support:
 - ii. A Systems Engineer is responsible for the following:
 - c. Example 3:
 - i. Database Support:
 - ii. A DBA is responsible for the following:
 - d. Example 4:
 - i. Business Recovery Services Vendor for Distributed Platforms
 - ii. Describe services of Business Recovery Services Vendor, if applicable.
6. Plan Initiation

7. Criteria for Restoration of the Business Process due to a Business Disruption – List criteria for invoking the business recovery procedures described in this contingency plan.
8. Business Recovery Procedures – Application Support
 - a. Staffing – Identify staff that needs to be involved in the recovery process;
 - b. Equipment and Components – List equipment and components in their entirety including quantities and attributes. This section shall include all necessary equipment particular to this application;
 - c. Procedures – Includes plans for acquiring, replacing, and alternate siting and any equipment needed;
 - d. Software and Data Backup Procedures – List all software with location and description of how it is backed up;
 - e. Software and Data Recovery Procedures – Describe how the software listed above will be restored;
 - f. Succession Plan – List Application Support Order of Succession including Name, Title, and Phone Number with Area Code; and
 - g. Vendor List – List Suppliers including Name, Product/Service/Commodities, and Phone number with Area Code.
9. Business Recovery Procedures – Hardware Support
 - a. Staffing – Identify staff that needs to be involved in the recovery process;
 - b. Equipment Types – List Equipment and type;
 - c. Client Equipment – Document any specialty equipment for the client, if any. Workstation equipment requirements, if applicable, to this section should be included here. If workstation equipment is not applicable to this section, it must be included in a different section of the Vendor's Plan;
 - d. Application Equipment – Document any application equipment;
 - e. Equipment Recovery Procedures – Describe how equipment is recovered;
 - f. Software and Data Backup Procedures – List steps taken to begin the backup process then document and describe the procedures;
 - g. Software and Data Recovery Procedures – List steps taken to begin the business recover process then document and describe the procedures;
 - h. Succession Plan – List Hardware Support Order of Succession including Name, Title, and Phone Number with Area Code; and
 - i. Vendor List – List Hardware Service Suppliers including Name, Title, and Phone Number with Area Code.

ATTACHMENT P: DISASTER RECOVERY PLAN

Vendor shall provide, in Vendor's response to this RFP, a narrative describing Vendor's approach to disaster recovery, including the types of information in Vendor's Disaster Recovery Plan. The narrative should not exceed three (3) pages. A full Disaster Recovery Plan must be submitted to the Department in accordance with the Implementation Plan.

When due, the Vendor's Disaster Recovery Plan must, at a minimum, include the following information:

Vendor's proposed Disaster Recovery Plan must fully describe the roles, responsibilities, tasks, timings and dependencies that will be crucial to a successful failover. In addition to a narrative description of the people, processes and tools needed, Vendor's proposed Disaster Recovery Plan must include business process modeling notation (BPMN) diagrams to visually depict the processes. The Disaster Recovery Plan must further define the priorities and sequencing for bringing services and integrations online.

1. Application System Summary
 - a. Technical Support Information
 - b. Operating System;
 - c. Programming Language(s); and
 - d. Internet Accessible – Yes or No
2. Hosting Information
 - a. Vendor Name;
 - b. Vendor Support Phone Number and Website;
 - c. Vendor Account and/or Technical Contact Name and Phone Number;
 - d. Server(s) Name;
 - e. Server Type;
 - f. Server OS;
 - g. Server Location;
 - h. IP Address;
3. Technical Support Information
 - a. Server OS;
 - b. Server Location; and
 - c. IP Address.
4. Failover Site Information
 - a. Server(s) Name;

- b. Server Type;
 - c. Server OS;
 - d. Server Location;
 - e. IP Address;
 - f. Warm/Hot Site;
 - g. Server(s) Name;
 - h. Server Type;
 - i. Server OS;
 - j. Server Location;
 - k. IP Address;
 - l. Vendor Access Method; and
 - m. VPN Info
5. Other Information
- a. External File Requirements;
 - b. Seats/Units;
 - c. License Requirements;
 - d. Protocol Requirement;
 - e. Port Requirements;
 - f. Third Party Requirements;
 - g. Code Libraries;
 - h. Known Bottlenecks;
 - i. Batch Processing; and
 - j. Supports Life Safety – Yes, No, or Unknown
6. System Notes
- a. Interface Engine;
 - b. Inbound Interfaces;
 - c. Outbound Interfaces; and
 - d. Other Comments
7. Maintenance and Recovery Procedures
- a. Maintenance; and
 - b. Backup Method/Schedule.
8. Support Personnel
- a. Name (Last/First);
 - b. Identify the following:

- c. System Administrator or Application Administrator;
- d. Site;
- e. System;
- f. Office Phone;
- g. Pager Number;
- h. Home Phone;
- i. Cell Phone; and
- j. Name (Last/First)

9. Procedures – The Vendor must describe their procedures. The description shall, at a minimum, address the following in chronological order:

- a. Recovery Procedures
 - i. Assumptions;
 - ii. System Architecture- Insert a drawing/process flowchart depicting the application architecture
 - iii. Software;
 - iv. Hardware – Insert hardware drawing with purpose of each item.
 - v. Backup Schedules
- b. Additional Procedures – The Vendor must provide Time and Description for the following:
 - i. Server Recovery Procedures – Server restoration priorities;
 - ii. Application Recover and Validation Procedures;
 - iii. Final Data Integrity Validation Procedures;
 - iv. Security Procedures;
 - v. Customer Recovery Procedures; and
 - vi. System Restoration Checklist –Check all applicable tasks covered by the DR Plan

Restore Task	Checkbox
Restore Servers	
• Hardware	
• Application Modules	
• Databases	
Restore Desktops (If Needed)	
Restore Integrations/Exchanges/Interfaces	
Restore Peripheral Devices	
Validation Steps	
• Add a test Minor Enhancement effort	

ATTACHMENT Q: STATE CERTIFICATIONS

Vendor Certifications Required by North Carolina Law

Instructions: **The person who signs this document should read the text of the statutes and Executive Order listed below and consult with counsel and other knowledgeable persons before signing. The text of each North Carolina General Statutes and of the Executive Order can be found online at:**

Article 2 of Chapter 64: http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_64/Article_2.pdf

a. G.S. 133-32:

<http://www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=133-32>

b. Executive Order No. 24 (Perdue, Gov., Oct. 1, 2009):

<https://ethics.nc.gov/media/242/download?attachment>

c. G.S. 105-164.8(b):

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_105/GS_105-164.8.pdf

d. G.S. 143-48.5:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-48.5.html

e. G.S. 143-59.1:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.1.pdf

f. G.S. 143-59.2:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.2.pdf

g. G.S. 143-133.3:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-133.3.html

h. G.S. 143B-139.6C:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-139.6C.pdf

Certifications

- (1) **Pursuant to G.S. 133-32 and Executive Order No. 24 (Perdue, Gov., Oct. 1, 2009)**, the undersigned hereby certifies that the Vendor named below is in compliance with, and has not violated, the provisions of either said statute or Executive Order.
- (2) **Pursuant to G.S. 143-48.5 and G.S. 143-133.3**, the undersigned hereby certifies that the Vendor named below, and the Vendor's subcontractors, complies with the requirements of Article 2 of Chapter 64 of the NC General Statutes, including the requirement for each employer with more than 25 employees in North Carolina to verify the work authorization of its employees through the federal E-Verify system." E-Verify System Link:

www.uscis.gov .

- (3) **Pursuant to G.S. 143-59.1(b)**, the undersigned hereby certifies that the Vendor named below is not an “*ineligible Vendor*” as set forth in G.S. 143-59.1(a) because:
- (a) Neither the Vendor nor any of its affiliates has refused to collect the use tax levied under Article 5 of Chapter 105 of the General Statutes on its sales delivered to North Carolina when the sales met one or more of the conditions of G.S. 105-164.8(b); **and**
- (b) **[CHECK ONE OF THE FOLLOWING BOXES]**
- ☐ Neither the Vendor nor any of its affiliates has incorporated or reincorporated in a “tax haven country” as set forth in G.S. 143-59.1(c)(2) after December 31, 2001; or
- ☐ The Vendor or one of its affiliates has incorporated or reincorporated in a “tax haven country” as set forth in G.S. 143-59.1(c)(2) after December 31, 2001 but the United States is not the principal market for the public trading of the stock of the corporation incorporated in the tax haven country.
- (4) **Pursuant to G.S. 143-59.2(b)**, the undersigned hereby certifies that none of the Vendor’s officers, directors, or owners (if the Vendor is an unincorporated business entity) has been convicted of any violation of Chapter 78A of the General Statutes or the Securities Act of 1933 or the Securities Exchange Act of 1934 within 10 years immediately prior to the date of the bid solicitation.
- (5) **Pursuant to G.S. 143B-139.6C**, the undersigned hereby certifies that the Vendor will not use a former employee, as defined by G.S. 143B-139.6C(d)(2), of the North Carolina Department of Health and Human Services in the administration of a contract with the Department in violation of G.S. 143B-139.6C and that a violation of that statute shall void the Agreement.
- (6) The undersigned hereby certifies further that:
- (a) He or she is a duly authorized representative of the Vendor named below;
- (b) He or she is authorized to make, and does hereby make, the foregoing certifications on behalf of the Vendor; and
- (c) He or she understands that any person who knowingly submits a false certification in response to the requirements of G.S. 143-59.1 and -59.2 shall be guilty of a Class I felony.

Vendor’s Name: _____

Vendor’s
Authorized Agent: Signature _____ Date _____

Printed Name _____ Title _____

Witness: Signature _____ Date _____

Printed Name _____ Title _____

The witness should be present when the Vendor's Authorized Agent signs this certification and should sign and date this document immediately thereafter.

ATTACHMENT R: Federal Certifications

The undersigned states that:

1. **He or she is the duly authorized representative of the Vendor named below;**
2. **He or she is authorized to make, and does hereby make, the following certifications on behalf of the Vendor, as set out herein:**
 - a. **The Certification Regarding Nondiscrimination;**
 - b. **The Certification Regarding Drug-Free Workplace Requirements;**
 - c. **The Certification Regarding Environmental Tobacco Smoke;**
 - d. **The Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier Covered Transactions;**
and
 - e. **The Certification Regarding Lobbying.**
3. **He or she has completed the Certification Regarding Drug-Free Workplace Requirements by providing the addresses at which the contract work will be performed;**
4. **[Check the applicable statement]**

[] He or she **has completed** the attached **Disclosure of Lobbying Activities** because the Vendor **has made, or has an agreement to make**, a payment to a lobbying entity for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action;

OR

[] He or she **has not completed** the attached **Disclosure Of Lobbying Activities** because the Vendor **has not made**, and **has no agreement to make**, any payment to any lobbying entity for influencing or attempting to influence any officer or employee of any agency, any Member of Congress, any officer or employee of Congress, or any employee of a Member of Congress in connection with a covered Federal action.

5. Describe how the Vendor can require its subcontractors, if any, to make the same certifications and disclosure.

Signature

Title

Vendor Name

Date

[This Certification Must be Signed by the Same Individual Who Signed the Proposal Execution Page]

I. Certification Regarding Nondiscrimination

The Vendor certifies that it will comply with all applicable federal statutes, executive orders, and regulations, including but not limited to: Title VI of the Civil Rights Act of 1964; Title IX of the Education Amendments of 1972; Section 504 of the Rehabilitation Act of 1973; the Age Discrimination Act of 1975; the Drug Abuse Office and Treatment Act of 1972; the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970; Title VIII of the Civil Rights Act of 1968; the Food Stamp Act and USDA policy; and any other applicable nondiscrimination statutes.

II. Certification Regarding Drug-Free Workplace Requirements

1. The Vendor certifies that it will provide a drug-free workplace by:
 - a. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the Vendor's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
 - b. Establishing a drug-free awareness program to inform employees about:
 - i) The dangers of drug abuse in the workplace;
 - ii) The Vendor's policy of maintaining a drug-free workplace;
 - iii) Any available drug counseling, rehabilitation, and employee assistance programs; and
 - iv) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
 - c. Making it a requirement that each employee be engaged in the performance of the agreement be given a copy of the statement required by paragraph (a);
 - d. Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the agreement, the employee will:
 - i) Abide by the terms of the statement; and
 - ii) Notify the employer of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such conviction;
 - e. Notifying the Department within ten days after receiving notice under subparagraph (d)(ii) from an employee or otherwise receiving actual notice of such conviction;
 - f. Taking one of the following actions, within thirty (30) days of receiving notice under subparagraph (d)(ii), with respect to any employee who is so convicted:
 - i) Taking appropriate personnel action against such an employee, up to and including termination; or

- ii) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency; and
- g. Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e), and (f).
- 2. The sites for the performance of work done in connection with the specific agreement are listed below (**list all sites; add additional pages if necessary**):

Address:

Street

City, State, Zip Code

Street

City, State, Zip Code

- 3. Vendor will inform the Department of any additional sites for performance of work under this agreement.
- 4. False certification or violation of the certification may be grounds for suspension of payment, suspension or termination of grants, or government-wide Federal suspension or debarment. 45 C.F.R. 82.510.

III. Certification Regarding Environmental Tobacco Smoke

Public Law 103-227, Part C-Environmental Tobacco Smoke, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by Federal grant, contract, loan, or loan guarantee. The law does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, and portions of facilities used for inpatient drug or alcohol treatment. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1,000.00 per day and/or the imposition of an administrative compliance order on the responsible entity.

The Vendor certifies that it will comply with the requirements of the Act. The Vendor further agrees that it will require the language of this certification be included in any subawards that contain provisions for children's services and that all subgrantees shall certify accordingly.

IV. Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier Covered Transactions Instructions

[The phrase "prospective lower tier participant" means the Vendor.]

1. By signing and submitting this document, the prospective lower tier participant is providing the certification set out below.
2. The certification in this clause is a material representation of the fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the Department or agency with which this transaction originate may pursue available remedies, including suspension and/or debarment.
3. The prospective lower tier participant will provide immediate written notice to the person to whom this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
4. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549, 45 CFR Part 76. You may contact the person to whom this proposal is submitted for assistance in obtaining a copy of those regulations.
5. The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter any lower tier covered transaction with a person who is debarred, suspended, determined ineligible or voluntarily excluded from participation in this covered transaction unless authorized by the Department or agency with which this transaction originated.
6. The prospective lower tier participant further agrees by submitting this document that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or voluntarily excluded from covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Non-Procurement List.
8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
9. Except for transactions authorized in paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the Department or agency with which this transaction originated may pursue available remedies, including suspension, and/or debarment.

Certification

1. The prospective lower tier participant certifies, by submission of this document, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal Department or agency.
2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

V. Certification Regarding Lobbying

The Vendor certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federally funded contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form SF-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.
3. The undersigned shall require that the language of this certification be included in the award document for subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) who receive federal funds of \$100,000.00 or more and that all subrecipients shall certify and disclose accordingly.
4. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000.00 and not more than \$100,000.00 for each such failure.

VI. Disclosure of Lobbying Activities

Instructions

This disclosure form shall be completed by the reporting entity, whether sub-awardee or prime Federal recipient, at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Use the SF-LLL-A Continuation Sheet for additional information if the space on the form is inadequate. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying activity is and/or has been secured to influence the outcome of a covered Federal action.
2. Identify the status of the covered Federal action.
3. Identify the appropriate classification of this report. If this is a follow-up report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.
4. Enter the full name, address, city, state and zip code of the reporting entity. Include Congressional District, if known. Check the appropriate classification of the reporting entity that designates if it is, or expects to be, a prime or sub-award recipient. Identify the tier of the sub-awardee, e.g., the first sub-awardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grants.

5. If the organization filing the report in Item 4 checks "Sub-awardee", then enter the full name, address, city, state and zip code of the prime Federal recipient. Include Congressional District, if known.
6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizational level below agency name, if known. For example, Department of Transportation, United States Coast Guard.
7. Enter the Federal program name or description for the covered Federal action (Item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans, and loan commitments.
8. Enter the most appropriate Federal Identifying number available for the Federal action identified in Item 1 (e.g., Request for Proposal (RFP) number, Invitation for Bid (IFB) number, grant announcement number, the contract grant, or loan award number, the application/proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP-DE-90-001."
9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the prime entity identified in Item 4 or 5.
10. (a) Enter the full name, address, city, state and zip code of the lobbying entity engaged by the reporting entity identified in Item 4 to influence the covered Federal action.
(b) Enter the full names of the individual(s) performing services and include full address if different from 10(a). Enter Last Name, First Name and Middle Initial (MI).
11. Enter the amount of compensation paid or reasonably expected to be paid by the reporting entity (Item 4) to the lobbying entity (Item 10). Indicate whether the payment has been made (actual) or will be made (planned). Check all boxes that apply. If this is a material change report, enter the cumulative amount of payment made or planned to be made.
12. Check the appropriate boxes. Check all boxes that apply. If payment is made through an in-kind contribution, specify the nature and value of the in-kind payment.
13. Check the appropriate boxes. Check all boxes that apply. If other, specify nature.
14. Provide a specific and detailed description of the services that the lobbyist has performed, or will be expected to perform, and the date(s) of any services rendered. Include all preparatory and related activity, not just time spent in actual contact with Federal officials. Identify the Federal official(s) or employee(s) contacted or the officer(s), employee(s), or Member(s) of Congress that were contacted.
15. Check whether or not a SF-LLL-A Continuation Sheet(s) is attached.
16. The certifying official shall sign and date the form, print his/her name, title, and telephone number..
Public reporting burden for this collection of information is estimated to average 30 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0046), Washington, D. C. 20503.

**Disclosure of Lobbying Activities
(Approved by OMB 0344-0046)**

1.Type of Federal Action: a.contract b.grant c.cooperative agreement d.loan e.loan guarantee f.loan insurance	2.Status of Federal Action: a.Bid/offer/application b.Initial Award c.Post-Award	3.Report Type: a.initial filing b.material change For Material Change Only: Year _____ Quarter _____ Date of Last Report: _____
4.Name and Address of Reporting Entity: Prime Sub-awardee Tier (if known) _____ Congressional District (if known) _____		5.If Reporting Entity in No. 4 is Sub-awardee, Enter Name and Address of Prime: Congressional District (if known) _____
6.Federal Department/Agency:	7.Federal Program Name/Description: CFDA Number (if applicable)	
8.Federal Action Number (if known)	9.Award Amount (if known) \$	
10.a.Name and Address of Lobbying Entity <i>(if individual, last name, first name, MI):</i> <i>(attach Continuation Sheet(s) SF-LLL-A, if necessary)</i>	10.b.Individuals Performing Services <i>(including address if different from No. 10a.) (last name, first name, and MI):</i> <i>(attach Continuation Sheet(s) SF-LLL-A, if necessary)</i>	

11.Amount of Payment (<i>check all that apply</i>): \$ _____ ☐ actual ☐ planned		13.Type of Payment (<i>check all that apply</i>): a.retainer b.one-time fee c.commission d.contingent fee e.deferred f.other; specify:	
12.Form of Payment (<i>check all that apply</i>): a.cash b.In-kind; specify: Nature _____ Value _____			
14.Brief Description of Services Performed or to be Performed and Date(s) of Services, including officer(s), employee(s), or Member(s) contacted, for Payment Indicated in Item 11(<i>attach Continuation Sheet(s) SF-LLL-A, if necessary</i>):			
15.Continuation Sheet(s) SF-LLL-A attached: Yes or No			
16.Information requested through this form is authorized by title 31 U. S. C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U. S. C. 1352. This information will be reported to the Congress semi-annually and will be available for public inspection. Any person who fails to file the required disclosure shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.		Signature: ____ Print Name: ____ Title: _____ Telephone No: _____ Date: _____	
Federal Use Only		Authorized for Local Reproduction Standard Form - LLL	

ATTACHMENT S: BUSINESS ASSOCIATE AGREEMENT

NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is made between North Carolina Department of Health and Human Services, Division of Health Benefits (“Covered Entity”) and [Enter Name of Contractor] (“Business Associate”) (collectively the “Parties”).

1. BACKGROUND

- a. Covered Entity and Business Associate are parties to an agreement entitled RFP #30-2025-054 PDM/CVO, whereby Business Associate agrees to perform certain services for or on behalf of Covered Entity.
- b. Covered Entity is an organizational unit of the North Carolina Department of Health and Human Services (the “Department”) that has been designated in whole or in part by the Department as a health care component for purposes of the HIPAA Privacy Rule.
- c. The relationship between Covered Entity and Business Associate is such that the Parties believe Business Associate is or may be a “business associate” within the meaning of the HIPAA Privacy Rule.
- d. The Parties enter into this Business Associate Agreement as an attachment to the Contract with the intention of complying with the HIPAA Privacy Rule provision that a covered entity may disclose Protected Health Information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

2. DEFINITIONS

Unless some other meaning is clearly indicated by the context, the following terms shall have the following meaning in this Agreement:

- a. “Electronic protected health information” or “ePHI” shall have the same meaning as the term “Electronic protected health information” in 45 C.F.R. § 160.103.
- b. “HIPAA” means the Administrative Simplification Provisions, Sections 261 through 264, of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as modified and amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.
- c. “Individual” shall have the same meaning as the term “individual” in 45 C.F.R. § 160.103 and shall include a Person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- d. “Person” shall have the same meaning as the term “person” in 45 C.F.R. § 160.103 and shall include a human being that is born alive, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- e. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164.

- f. "Protected Health Information" or "PHI" shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. § 160.103, limited to the information compiled, created, or received by Business Associate from or on behalf of Covered Entity.
- g. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
- h. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or the Person to whom the authority involved has been delegated.
- i. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subpart C.
- j. Unless otherwise defined in this Agreement, terms used herein shall have the same meaning as those terms have in the Privacy Rule.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

- a. Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required By Law.
- b. Business Associate agrees to use appropriate safeguards and comply, where applicable, with subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of the ePHI other than as provided for by this Agreement.
- c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- d. Business Associate agrees to comply with all applicable requirements of the Security Rule (45 C.F.R. Part 164, Subparts A and C) with respect to electronic protected health information.
- e. Business Associate shall implement physical, administrative and technical safeguards that reasonably protect the confidentiality, integrity and availability of any ePHI that it creates, receives, maintains or transmits on behalf of the NCDHHS.
- f. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410.
- g. Business Associate agrees, in accordance with 45 C.F.R. § 164.502(e)(1) and § 164.308(b)(2), to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.
- h. Business Associate agrees to make available PHI as necessary to satisfy Covered Entity's obligations in accordance with 45 C.F.R. § 164.524.
- i. Business Associate agrees to make available PHI for amendment and incorporate any amendment(s) to PHI in accordance with 45 C.F.R. § 164.526.
- j. Unless otherwise prohibited by law, Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- k. Business Associate agrees to make available the information required to provide an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

4. PERMITTED USES AND DISCLOSURES

- a. Except as otherwise limited in this Agreement or by other applicable law or agreement, if the Contract permits, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract, provided that such use or disclosure:
 - 1) would not violate the Privacy Rule if done by Covered Entity; or
 - 2) would not violate the minimum necessary policies and procedures of the Covered Entity.
- b. Except as otherwise limited in this Agreement or by other applicable law or agreements, if the Contract permits, Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that:
 - 1) The disclosures are Required By Law; and
 - 2) Business Associate obtains reasonable assurances from the Person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the Person, and the Person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- c. Except as otherwise limited in this Agreement or by other applicable law or agreements, if the Contract permits, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- d. Notwithstanding the foregoing provisions, Business Associate shall not use or disclose PHI if the use or disclosure would violate any term of the Contract or other applicable law or agreements.

5. TERM AND TERMINATION

- a. **Term.** This Agreement shall be effective as of the effective date of the Contract and shall terminate when the Contract terminates.
- b. **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, at its option:
 - 1) Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement and services provided by Business Associate, to the extent permissible by law, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
 - 2) Immediately terminate this Agreement and services provided by Business Associate, to the extent permissible by law; or
 - 3) If neither termination nor cure is feasible, report the violation to the Secretary as provided in the Privacy Rule.
- c. **Effect of Termination.**
 - 1) Except as provided in paragraph (2) of this section or in the Contract or by other applicable law or agreements, upon termination of this Agreement and services provided by Business Associate, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
 - 2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction not feasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. GENERAL TERMS AND CONDITIONS

- a. This Agreement amends and is part of the Contract.
- b. Except as provided in this Agreement, all terms and conditions of the Contract shall remain in force and shall apply to this Agreement as if set forth fully herein.
- c. In the event of a conflict in terms between this Agreement and the Contract, the interpretation that is in accordance with the Privacy Rule shall prevail. In the event that a conflict then remains, the Contract terms shall prevail so long as they are in accordance with the Privacy Rule.
- d. A breach of this Agreement by Business Associate shall be considered sufficient basis for Covered Entity to terminate the Contract for cause.

IN WITNESS WHEREOF, Business Associate agrees to and executes this Agreement as of the Effective Date of the Contract.

BUSINESS ASSOCIATE

Name
Title

Date

COVERED ENTITY

Melanie Bush
Deputy Secretary

Date

ATTACHMENT T: TECHNICAL / MANAGEMENT PROPOSAL

The Technical / Management Proposal is comprised of responses to selected sections of the RFP and Specifications listed in the following tables. Provide the section responses in the order found in the tables with the instructions provided before each table. Label each RFP section within the body of the technical / management proposal.

By signing the Execution Page of this RFP, the Vendor agrees to meet all Requirements in the tables provided in Section 3.5.1. If any of these Requirements cannot be met, the State will disqualify the Vendor from further evaluation.

Vendor to provide a detailed narrative, diagrams, process flows, exhibits, examples, sketches, relevant descriptive literature, or other information to demonstrate how the Vendor's solution(s) will address each section area listed in the table below. Please be as detailed as possible while keeping within the page limitation listed for each section.		
RFP Section	Area	Page Limitation
Section 3.1.1	Scope of Work: Business Operations	10
Section 3.1.2	Scope of Work: Technical and Information Architecture Requirements	15
Section 3.1.3	Scope of Work: Project Management and System Development Requirements	10
Section 3.1.4	Scope of Work: Certification	10
Section 3.1.5	Scope of Work: Customer Relationship Management and Provider Call Center	5
Section 3.1.6	Scope of Work: Operations, Maintenance and Configuration Requirements	5
Section 3.4.2	Architecture Diagrams	n/a
Section 4.2	Payment Schedule	n/a
Section 7.1	Vendor Utilization of Workers Outside the US	2
Section 7.4	Vendor's License or Support Agreements	n/a
Section 7.6	Disclosure of Litigation	2
Section 7.11	Project Management	5

Vendor to provide a response for all Specifications in the tables provided in Section 3.6.1. Each Specification must have a response provided in a format with a header to include two columns: a) the Specification number as provided in the RFP, and b) the Specification Description as provided in the RFP, and then an area following the header that contains the narrative response to the Specification. The narrative can contain diagrams, process flows, exhibits, examples, sketches,
--

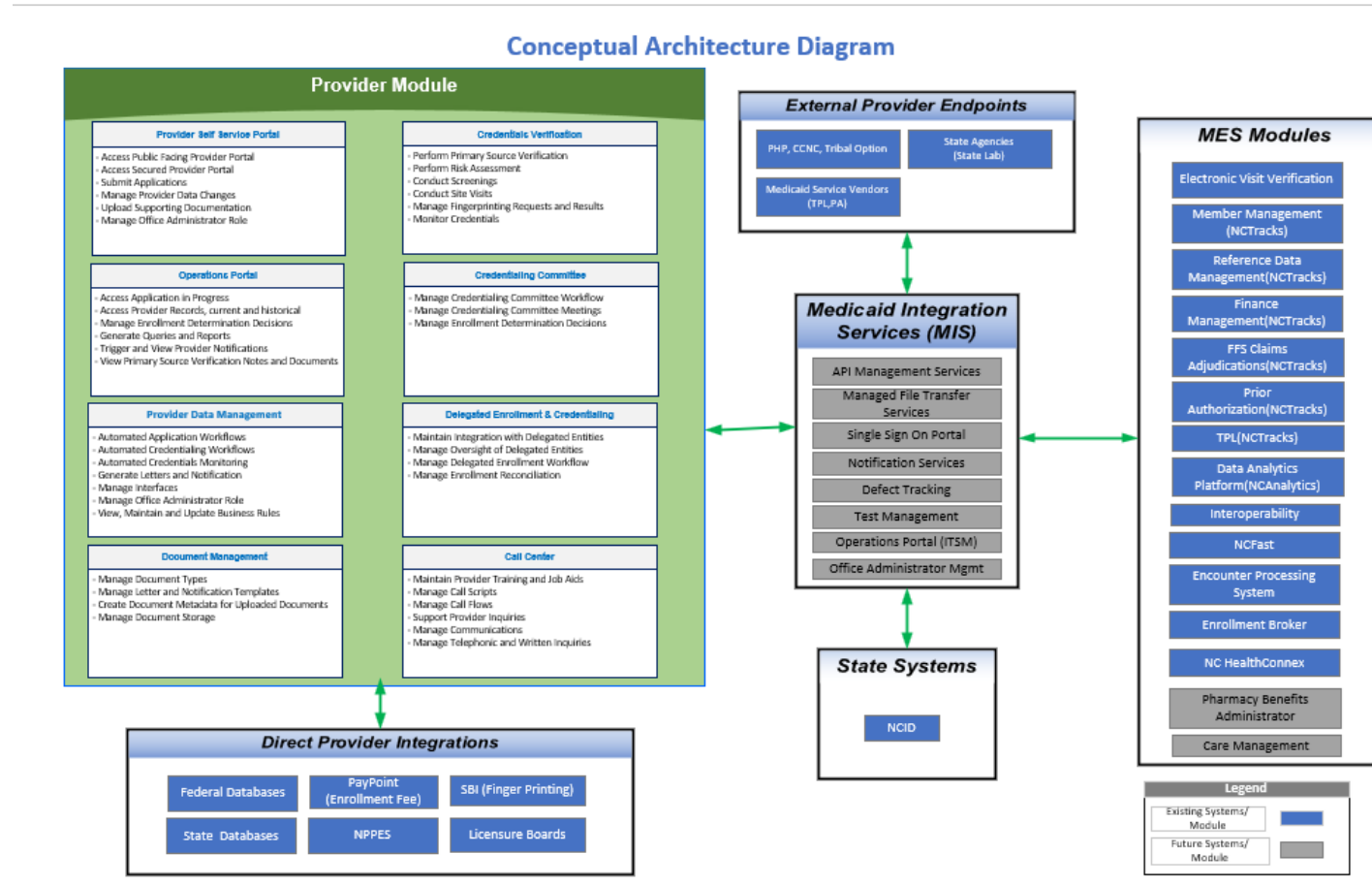
relevant descriptive literature, or other information to demonstrate how the Vendor's solution(s) will address each Specification.

Note: The Specification tables in Section 3.6.1 in this RFP are ranked in descending order of importance.

RFP Section	Area	Page Limitation
Section 3.6.1: Table S1	Business Operations	n/a
Section 3.6.1: Table S2	Security	n/a
Section 3.6.1: Table S3	Certification	n/a
Section 3.6.1: Table S4	Data	n/a
Section 3.6.1: Table S5	Solution	n/a
Section 3.6.1: Table S6	Workflow	n/a
Section 3.6.1: Table S7	Communications	n/a
Section 3.6.1: Table S8	Architecture	n/a
Section 3.6.1: Table S9	Conversion	n/a
Section 3.6.1: Table S10	Integration	n/a
Section 3.6.1: Table S11	Testing	n/a
Section 3.6.1: Table S12	Project Management	n/a
Section 3.6.1: Table S13	Operations and Maintenance	n/a
Section 3.6.1: Table S14	Staffing	n/a
Section 3.6.1: Table S15	Call Center	n/a
Section 3.6.1: Table S16	Training	n/a

ATTACHMENT U: CONCEPTUAL ARCHITECTURAL DIAGRAMS

The following are conceptual architectural diagrams relating to the future state of the PDM/CVO Solution



ATTACHMENT V: MEDICAID INTEGRATION SERVICES CORE CAPABILITIES

Introduction

The North Carolina Department of Health and Human Services, Division of Health Benefits (Department) is in the process of implementing a Medicaid Integration Services platform (MIS) that will provide module vendors with a common infrastructure, which may consist of State developed and third-party solutions and tools, to communicate and integrate using a consistent standards-based approach.

The MIS will be configured and set up to run in the cloud and provides core shared services to be leveraged by the different module vendors and systems. The following provides additional details of these core services:

Core MIS Services

1. Application Program Interface (API) Management

The MIS platform provides **API Management capability** to support lifecycle management, covering the design, deployment and management of APIs that will be the primary means of integration of MIS components and MES vendor modules. API management **includes API Gateway and API traffic management capability** including rate-limiting to control impact on backend services.

The API Management infrastructure will provide a graphical web portal interface that allows the management of the entire lifecycle of interfaces connecting MES modules via the MIS. The MIS will use the **API Management Portal** to design, secure, publish, monitor, manage, and deploy interfaces across multiple vendor cloud environments. Using the portal, the MIS team will define integration across module API contracts, fulfill contract implementation, define access control and usage policies, set rates and limits, and deploy the API for testing and later operations.

The MIS platform provides **API Management capability** to support lifecycle management, covering the design, deployment, and management of APIs that will be the primary means of integration across the MES. API management **includes API Gateway and API traffic management capability** including rate-limiting to control impact on backend services.

S No.	Type of API	Description	MIS API Gateway	MIS API Management Portal	Module Vendor Interaction
1	Module Vendor Internal Application	These are APIs that the vendor uses within their module for	Not Applicable	Recommended to be available to support discoverability	Publish their APIs in the Open API specification format

S No.	Type of API	Description	MIS API Gateway	MIS API Management Portal	Module Vendor Interaction
	Specific API	completing the required functionality			
2	Module Vendor External Facing APIs	These are the APIs that vendor exposes for other entities to interact and integrate with the module	API is managed through the gateway for governance, security, and traffic management	Yes. – Other module vendors can use this to discover and learn about the API	Act as a publisher for an API also known as API provider Act as a consumer for the other module vendor APIs
3	Third Party APIs	These are external APIs that may be published by federal agencies and other trusted sources and are identified as useful to integrate in the Medicaid business operations	API Gateway provides the access end point. Not all external APIs may be governed through the API Gateway	Yes	Discover and learn about these API on the API Management Portal Register Module Application to have access to these APIs
4	MIS Service APIs	These are APIs that provide access to the MIS core capabilities or are APIs that may be developed to support integration requests between different MES modules	Yes	Yes	Discover and learn about these API on the API Management Portal Register Module Application to have access to these APIs

a. API Standards

The MIS platform **recommends the use of API first style-based integration approach** for module interactions and integration points. The MIS promotes the following standards and architectural practices.

S No.	Area	Preferred Standard/Style
1	API Architectural Style	REST
2	API Specification	Open API Specification (OAS) 3.0
3	Security	OAUTH 2.0 and OIDC where applicable
4	Payload	JSON

The MIS also **supports Simple Object Access Protocol (SOAP)-based web services** and other integration approaches like **message queues**. The MIS platform supports the following standards for these.

S No.	Area	Preferred Standard/Style
1	SOAP	SOAP 1.2
2	Web Services	Web Services Description Language (WSDL) 1.2
3	SAML	Security Assertion Mark Up Language 2.0

The MIS preferred and recommended style is to use Representational State Transfer (REST)-based APIs for integration.

2. Managed File Transfer

The MIS provides support for exchanging data through a managed file transfer mechanism. The Managed File Transfer (MFT) service platform supports modules to reliably exchange electronic data with other modules and systems in a secure way. The MFT services provides full visibility to these data exchanges including ability to see who is transferring files, what is being shared, and the volume passing through the system. The MFT service can proactively identify events like delays and failed transfers before they impact downstream modules or missed Service-Level Agreements (SLAs).

The following table identifies the high level MFT capability and the recommendation for use for the module vendor.

S No.	MFT Capability Access Mode	Recommendation for Module Vendor
1	Use of MIS published standards (upload, download etc.) to support file transfer capabilities	Preferred way to interact with MFT capability and use it for checking status, progress, and errors
2	Use of MFT provided Web Interface	Only for ad-hoc situations

3	Use of MFT provided native interfaces such as SFTP and SCP	Preferred only in case of large data files. Also, will be used where the trading partner (federal agency, other module vendors) requires the use of data files
---	--	--

a. Authentication and Security

All service accounts for the Module Vendors using the MFT capability will be managed and provisioned using the MIS platform's Identity Credential and Access Management (ICAM) service infrastructure.

b. Supported Protocols

The Managed File Transfer service will support the following standards:

- i. Secure FTP (SFTP (SSH File Transfer Protocol, FTPS, and Secure Copy Protocol (SCP)) for protected file transfer;
- ii. AS2, AS3 and AS4 messages with support for multiple file attachments.

3. ICAM

Identity Credential and Access Management (ICAM) is an Authentication and Authorization Service.

The ICAM solution will work in conjunction with State of NC's enterprise-IAM platform, i.e., NCID (North Carolina Identity Management Service), in a federated model using the Security Assertion Markup Language (SAML) 2.0 protocol.

The following table identifies the role of each system as it pertains to user identity:

S No.	System	Roles
1	NCID	- Identity Provider (IdP) for users in the system - All users will be registered in the NCID system first
2	Module Vendor	Act as a Service Provider (SP) to NCID

The MES Portal has been developed to provide an MES Landing Page which gives users a single point of entry into the Department's MES Medicaid system and displays the MES module tiles to which a user has access based on the coarse-grained authorization. To facilitate this functionality, modules / applications are required to utilize a State developed API to push coarse-grained authorization to the user's NCID profile.

Fine-grained authorization will be maintained and provided by the modules / applications to give the user the appropriate access within the application.

The architectural diagram showing the design for NCID coarse-grained authorization and SAML flow for single-sign-on is provided in Figure V1 below.

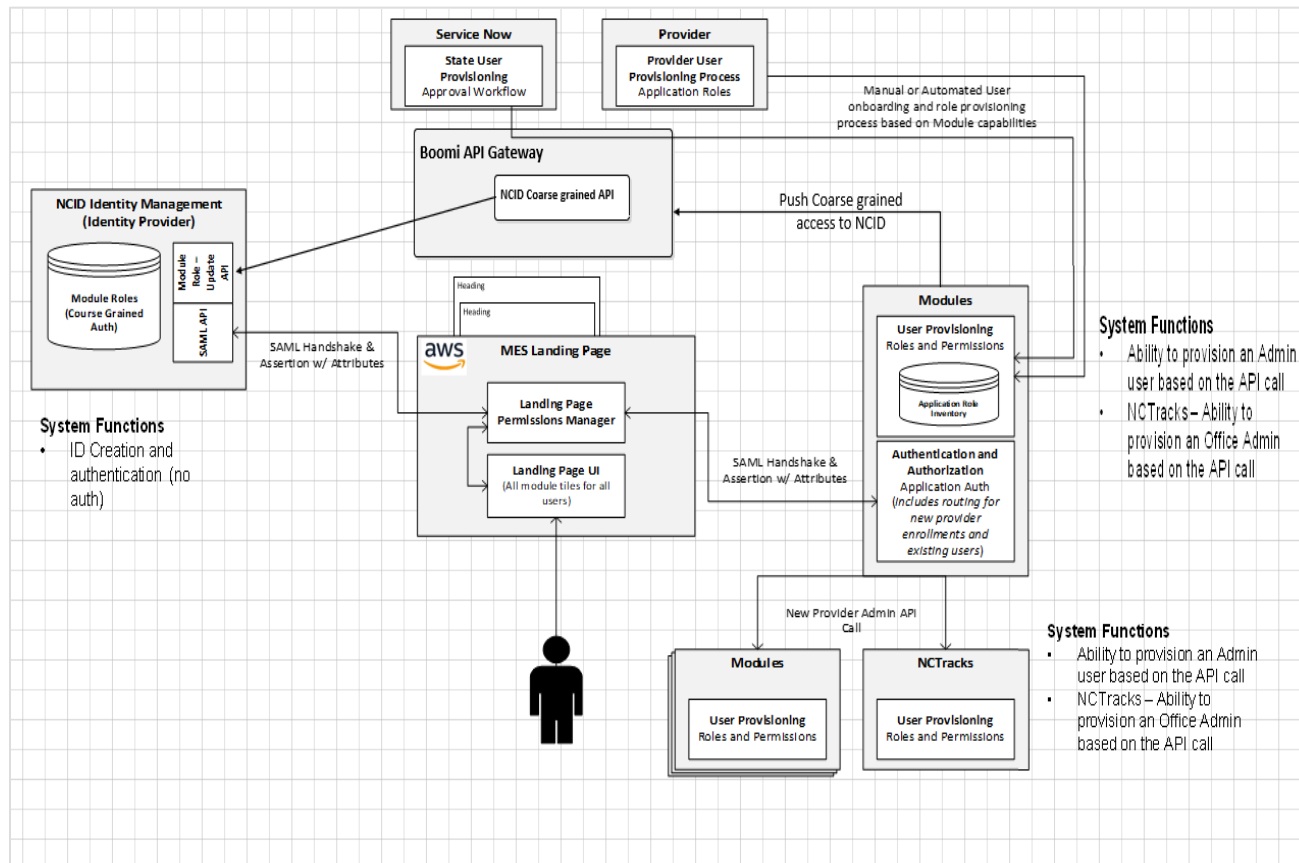


Figure V1 – Architectural Diagram showing NCID and SAML

4. Operation Portal with Centralized Information Technology Service Management (ITSM) Capabilities

The State provides a unified web-based operations portal to allow for performing various operations including request, monitor, configure, control and report on each of the MIS platform services. The operations portal will **provide a module specific view** of all relevant transactions flowing through the MIS platform.

The Solution will follow the State provided ITSM solutions in the following business areas:

- Change Management
- Incident Management
- Problem Management
- Release Management

a. Change Management

All State initiated change(s) or changes that impact Medicaid production operations will be tracked in the State provided change management solution. All module vendors will be required to use this solution to facilitate cross module collaboration, centralized approvals and tracking deployment of changes to the production environment.

b. Incident Management

The module vendors will raise incidents that impact the overall MES Enterprise operations to facilitate cross-module tracking and resolution of incidents. These incidents will be reported in this State provided Incident Management system for review and to manage communication and escalation to the appropriate module vendor partner for resolution.

c. Problem Management

Problems will primarily be managed by the State Central Technical Operations team. The module vendors reporting incidents will be prompted to link new incidents to existing problems if known. The module vendors will support the State Central Technical Operations team in managing the life cycle of the problem.

d. Release Management

The module vendors must follow the State provided and defined Release Management process.

5. Defect Tracking

The module vendors will use their existing defect tracking systems to manage their development and product defects, but the State will require the use of the State provided defect tracking system for module-to-module integration testing and User acceptance testing for modules.

6. Test Management

The Solution must utilize the State provided test management infrastructure and service to support centralized test management across all MES modules, MIS, and the Medicaid partners. This service will allow NCDHHS to monitor and report on testing progress. The module vendors will be required to provide data to the centralized test management system to support consolidated reporting including generation of key metrics and reporting progress.

ATTACHMENT W: WORK PRODUCTS

1.0 WORK PRODUCTS

Work products are incidental artifacts created during the performance of the contract. Work Products submitted by the Vendor should follow industry standards, best practices, and the description provided. *NOTE: Work Products are NOT separately priced. The efforts and time required to develop work products must be factored into the overall cost and timeframe of project implementation and operations.*

Table W-1 – Work Products lists the work products to be provided by the Vendor for this project. The information for each work products includes:

- Work Product ID: Unique identifier of the work product.
- Title: Name of the work product.
- Description: A summary of the elements to be included in the work product.
- Phase / Stage: The phase of the project when the work product is expected to be delivered.
- Frequency / Updates: Indicates how often the work product is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the work product. The meaning of the values is as follows:
 - None – No preferred template exists. The Vendor is free to provide the deliverable in its own format and content.
 - State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Work Product ID.

Note: The Work Product ID assigned to each work product in *Table W-1 Work Products* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
MES-WP-CERT-001	O&M	Certification Crosswalk Report	O&M	Ad Hoc	Document that describes how the Vendor's deliverables and other documentation align with federal certification requirements and milestone reviews. The Vendor must produce reports on this crosswalk at the direction of the Department.
MES-WP-OM-001	DDI, O&M	Major Minor Release Notes	Effective Date + 15-days	Ad Hoc	Electronic notifications including detailed release notes for Major and Minor version, patches, updates and fixes deployed to the production environment.
MES-WP-OM-002	O&M	Release Milestones and Updates	Immediately after go-live	Weekly	Document containing the schedule of system releases, updates, maintenance, and milestones for the next 45 days. This will be submitted to the Department weekly on Fridays.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
MES-WP-OM-003	O&M	Root Cause Analysis	As needed	As needed	Document that adheres to the format defined by the Department. The RCA must detail the causes, impacts, downtime, and remediations required to resolve any issue. The Vendor must ensure the RCA includes mitigations and corrective actions to prevent future interruptions. The RCA must be submitted within seventy-two hours following the resolution of the failure.
MES-WP-PM-001	Contract award	Vendor Kickoff Presentation	Contract Award	Once	A presentation jointly developed by the Vendor and the Department which will be presented by the Vendor to the Department. The presentation will provide a clear overview of the project implementation plan, and module overview which marks the formal kickoff of the project with the business.
MES-WP-PM-002	DDI	Meeting Agenda, Minutes, and Documentation	Effective Date + 15 Days	Ad Hoc	Documents which contain all meeting agendas, notes, outcomes, and next steps.
MES-WP-PM-003	DDI, O&M	Lessons Learned (with Evaluation) Report	Effective Date + 90-days	End of each project phase or milestone	Document that records all lessons learned throughout the project. The lessons learned will be ongoing and will be used to enhance build strategies on subsequent builds to gain greater efficiency and effectiveness into process. Lessons learned will be shared among the DDI team in partnership with the Department. Lessons learned will be incorporated into the Vendor's overall quality management process. Lessons learned will also be a key element of our approach to configuration/change management and process improvement. The Vendor must also hold a walk-through meeting of the results and provide an evaluation report for all engagements.
MES-WP-PM-004	DDI	Program Increment (PI) Release Plan	Design	Submitted approximately quarterly (will depend on sprint length), meant to give an outlook on the next 3 sprints	Release Plan submitted within five business days of completing each PI Planning Session. This Release Plan must include, at minimum: • Number of expected sprints • Estimated sprint duration • Targeted features for each sprint • Planned completion dates for features / Milestones and Key deliverables, major checkpoints, reviews • Dependencies across features • Scope changes or variance • Capacity allocation – expected team velocity, allocation by team/role and how capacity is planned across sprints • Risk and Mitigation Plan – anticipated risks technology, dependency, resourcing etc. and mitigation strategies

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Integration and Deployment Plan – how increments will be integrated and tested and deployed - Metrics and Tracking – PI level indicator – predictability, scope stability, velocity, defect leakage - Change Management and Communication Plan – how changes to scope or timeline are communicated - Release readiness Criteria – what must be achieved before release or PI. Work product submission schedule will be determined in collaboration between the Vendor and the Department. Most organizations conduct PI planning events every 8-12 weeks.
MES-WP-PM-005	DDI	Sprint Retrospective	After first sprint	After each spring	Document compiled at the conclusion of every sprint. It captures the collective insights, performance metrics, and improvement actions identified during retrospective sessions across Agile teams. This work product supports continuous improvement by consolidating lessons learned and providing visibility into team dynamics, delivery challenges, and process enhancements. The document must include: - Sprint Overview: A brief summary of each sprint, including goals, key accomplishments, and any deviations from planned outcomes. - Progress Metrics - Mechanisms for tracking sprint progress to assess performance (Velocity trends, defect rates, test coverage, and automation percentages) to be reported on within the weekly project status. - Risks and Issues - Summary of any risks/issues encountered during the sprint, including their mitigation plan. - Retrospective Summary - Key takeaways from the sprint retrospective, including: - What Went Well: Highlights of successful practices, team collaboration, and delivery achievements. - What Didn't Go Well: Challenges encountered, including blockers, inefficiencies, or misalignments. - What To Improve: Actionable recommendations for process, tooling, or communication improvements. - Velocity tracking - story points completed vs. committed, with historical comparison to prior sprints.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					• Change log - updates on any new scope added, descoped, or deferred during the sprint • Commitment status - updates on specific features, integrations, or milestones tied to the sprint • Stakeholder engagement - feedback captured in Sprint Reviews or mid-sprint demos This work product ensures that Agile teams reflect on their performance regularly and that insights are translated into tangible improvements. It also provides program-level stakeholders with a consolidated view of team health and delivery maturity.
MES-WP-PM-006	DDI	Program Increment (PI) Inspect and Adapt	After first sprint	Submitted after the first 4 sprints and then every 2 sprints afterwards (approximately quarterly, will depend on sprint length)	Document submitted in coordination with the Inspect and Adapt session conducted at the conclusion of the Agile Program Increment. It serves as a formal retrospective and continuous improvement artifact documenting key insights, performance metrics, and actionable recommendations. The report should include: • Program Performance Review: A summary of objectives met, features delivered, and metrics tracked during the PI, including velocity, quality, and predictability indicators. • Problem-Solving Workshop Outcomes: Documentation of systemic issues identified during the PI, root cause analysis, and proposed corrective actions. This section highlights cross-team collaboration and resolution strategies. • Lessons Learned: A detailed account of successes and areas for improvement gathered from Agile teams, Product Management, and stakeholders. Topics include team dynamics, planning accuracy, dependency management, tooling effectiveness, and stakeholder engagement. • Improvement Backlog: A prioritized list of improvement items to be addressed in future PIs, including process enhancements, tooling upgrades, and training needs. • Business value achieved - comparison of planned PI Objectives vs. actual business value delivered

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Trend analysis - comparison with prior PIs to show improvement or recurring challenges (e.g., predictability, scope stability). - Team health check - qualitative assessment of team morale, collaboration, and alignment with program values. - User feedback - insights gathered from demos, reviews, or user satisfaction surveys if any conducted during the PI. This report is intended to inform leadership, guide future PI planning, and reinforce a culture of transparency and continuous learning.
MES-WP-STAF-001	DDI, O&M	Organization Staffing Charts	Effective Date + 15-days	Ad Hoc	Organization charts showing the number and type of staff resources to be assigned to a) the transition to Solution and b) subsequent operations, and maintenance. The former chart will focus on the requirements gathering and design phase of the project, while the latter will address steady-state operations. Each staffing chart must include: - Roles and qualifications of each proposed team member. - Include and identify any subcontractors and their proposed function. - Identify the geographic location of each proposed team member. - Identify any known changes throughout the term of the Contract (i.e. changes between implementation and steady-state operations). - Identify aggregate full-time equivalent projections and the assumptions used to generate those projections. - Include the named individual, the role they are filling and the time frame or project phases during which each individual/role will be required.
MES-WP-TEST-001	DDI	Test Summary Result Report	Ad hoc	Aligned with test phases	For each test phase listed in Section 7.17 of the contract, the Vendor must submit a Test Summary Result Report and obtain Department approval to close the current test phase. This is comprehensive report that includes the following: - Overview of testing activities/Test Phase/Test Dates/Test Environment (configuration) - Total Number of Test Cases Executed

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					• Test Case Final Execution Status (Passed/Failed/NA/Deferred/Date/Evidence of completion) • Total Number of defects Logged • Defect Final Execution Status (Passed/Failed/NA/Deferred/Date/Evidence of completion) • List of requirements covered during the test phase
MES-WP-TEST-002	DDI	SIT/Parallel Test Scenarios and Cases	During Development	Weekly	Document that details test scenarios and test cases for SIT / Parallel Tests. The document must include: • Positive and negative scenarios (which must include error handling and stressing the system with bad and invalid data) • Step-by-step instructions • Expected results • Actual results
PDM-WP-CC-001	DDI	Customer Service Support Workflow Processes	30 Days Prior to go-live	Once	The vendor must develop workflow processes for customer service support activities.

Table W-1 – Work Products

ATTACHMENT X: REQUEST FOR PROPOSED MODIFICATIONS TO THE TERMS AND CONDITIONS

As provided in Section 1.3.3, Offeror may submit proposed modifications to the terms and conditions of the RFP for consideration by the Department. The proposed modifications do not alter the terms and conditions of the RFP and have no force or effect on the RFP or any resulting Contract unless accepted by the Department and incorporated through a BAFO, negotiation document, addenda to the RFP or amendment to the Contract.

The Department at its sole discretion may consider any proposed modifications submitted in this Attachment.

The Offeror must check one of the boxes below to indicate whether it is proposing modifications to the terms and conditions of the RFP:

- ☐ The Applicant **DOES NOT** propose modifications.
- ☐ The Applicant **DOES** propose modifications as provided in the following table:

	RFP Citation (i.e., section & page number)	Redline of Proposed Modification (i.e., include text as published in RFP and strikethrough words, phrases or sentences proposed to be deleted and underline words, phases, or sentences proposed to be added)
1.		
2.		
3.		
4.		
5.		

ATTACHMENT Y: MINIMUM QUALIFICATIONS

The Offeror must demonstrate it meets the Minimum Qualifications to have its response evaluated by the Department. The Offeror MUST complete this Attachment by selecting and checking a box under each numbered or lettered item, where indicated, and providing any necessary details and documentation to demonstrate it meets each required qualification.

Any Offeror Proposal that does not meet any Minimum Requirement will be disqualified and will not be given any further consideration by the Evaluation Committee, unless it is determined that such disqualification is not in the best interest of the Department.

1. **Agreement to Terms and Conditions**

The Offeror agrees and accepts, without exception all terms and conditions, including confidentiality, privacy and security protections and public records and trade secrets protections, specified in *Attachment B* of this RFP. The Offeror may suggest modifications to the terms and conditions per the instructions in *Section 1.3.3.c* and complete *Attachment X: Request for Proposed Modifications to the Terms and Conditions*, and acknowledges such suggestions are not part of any subsequent Contract unless explicitly accepted by the Department in accordance with *Section 1.3.3.c*.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

2. **Eligibility to Contract**

- a. As of the date of its submission of a response to this RFP, the Offeror is not on the list of vendors debarred from doing business with the State of North Carolina.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

- b. As of the date of its submission of a response to this RFP, the Offeror is not on a federal list of parties that are excluded from participation in Medicare, Medicaid, or other federal health care programs, or from receiving federal contracts, or federal financial or non-financial assistance.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

- c. Offeror agrees to notify the Department immediately if it is debarred or excluded from State or federal contracting, participation in health care programs or receipt of financial or non-financial assistance, prior to the Contract Award date.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

- d. Offeror acknowledges and understands that debarment or exclusion from State or federal contracting, program participation, or assistance will result in immediate disqualification from Contract Award.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

3. **Financial Stability and Legal Disclosure**

The Offeror is financially stable and has disclosed any legal actions that could adversely affect its financial condition or ability to meet the requirements of this RFP as required by *Attachment E: Certification of Financial Condition and Legal Action Summary*.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

4. **Experience Requirements**

The Offeror has a minimum of five (5) years combined experience providing asset verification services similar to those described in this RFP to include other agencies of State government, county government, municipal government, or corporate employer in NC or in other states. All of the Offeror's experience specified in this section must have occurred within the five (5) years immediately preceding the date the RFP is issued by the Department as outlined in the following table. Where Offeror indicates areas of experience that are for services *similar* to those described in this RFP, Offeror must reference the specific RFP requirements and RFP section(s) relating to the similar services and describe, in detail, how the services are similar to be considered. It is the responsibility of the Offeror to clearly demonstrate in detail how services are similar and should be considered in the column titled *Description of Services Provided* below.

Name and Type Entity	Description of Services Provided	Size of population served by program(s)	Period of Experience (Start Date and End Date)	Relevant RFP Requirement Section of the experience (i.e., Section V. D. 1.)

By completing and signing this *Attachment A: Minimum Qualifications Response*, the Offeror affirms adherence to the required Minimums Qualifications and attests the information provided herein is accurate, and the individual signing certifies he or she is authorized to make the foregoing statements on behalf of the Offeror.

Offeror Signature

Date

Printed Name and Title

ATTACHMENT Z: SUBCONTRACTOR IDENTIFICATION FORM

The Contractor must complete this *Attachment Z: Subcontractor Identification Form* for each known Subcontractor, as defined in Attachment A: Definitions, who will be used to meet the Contract requirement or otherwise perform any services pursuant to the Contract (i.e., there should be one form for each Subcontractor). After Contract Award, the *Subcontractor Identification Form* must be submitted by the Contractor to the Department for review and approval of all new subcontractors, in accordance with Attachment C, Section 1, Paragraph 30: Subcontractors.

By executing the Contract, or submitting this Attachment after Contract Execution in accordance with Attachment C, Section 1, Paragraph 30: Subcontractors of the Contract, the Contractor:

1. Certifies that the information provided in this Attachment is true to the best of its information and belief; and
2. Acknowledges the requirements set forth in the Terms and Conditions related to Subcontractors and the resulting obligations, including requiring Department approval of any Subcontractors used in the performance of the Contract; and
3. Agrees to notify the Department of any material changes to the information provided in this Attachment that arise prior to execution or during the term of the Contract.

A: Subcontractor Identification	
1. Business Information. Provide the requested Information in the space provided:	
Legal Name of Subcontractor	Enter text here
Name Used for Business if Different	Enter text here
FEIN/Taxpayer ID	Enter text here
Address	Enter text here
Contract Executed	☐ Yes ☐ No
Term of Contract	Enter text here
Name of Contact Person Title Phone Number Email Address	Enter text here
2. Scope of Subcontracted Services. Identify the scope of services and activities that will be provided by the Subcontractor; cite specific Sections of the Contract as applicable:	

Enter text here
3. Is Subcontractor a government entity?
☐ Yes ☐ No

ATTACHMENT AA: REPORTS

1.0 REPORTS

Table AA-1 Reports List provides a list of the reports to be provided by the Vendor. The information for each report includes:

- Report ID: Unique identifier of the report
- Title: Name of the report
- Description: A summary of the elements to be included in the report.
- Frequency: Indicates how often the report is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the report. The meaning of the values is as follows:
 - None – No preferred template exists. The Vendor is free to provide the report in its own format and content.
 - State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Report ID.

Reports submitted by Vendor should follow industry standards, best practices, and include data elements provided in the report description. *NOTE: Administrative Reports are NOT separately priced. The efforts and time required to develop and provide reports in the frequency shown must be factored into the overall cost and timeframe of project implementation and operations.*

The Vendor must provide reports that meet the following minimum quality standards:

- a. Provide accurate and comprehensive content.
- b. Follow industry standards and best practices.
- c. Appropriately define and reference information.

The reporting deadline by frequency follows:

- a. Daily or Weekly Reports – by the end of the Business Day following the end of the reporting period.
- b. Monthly Reports – by the third Business Day following the end of the reporting period.
- c. Quarterly or Annual reports – by the fifth Business Day following the end of the reporting period.
- d. Annual reports – by the fifth Business Day following the end of the reporting period.

Informal reviews and walkthroughs of draft and final reports are encouraged. The State will provide final approval of the content and layout of all reports listed in *Table AA-1 Reports List*.

Number	Category	Report Name	Frequency	Description
MES-REP-01	Security	User Access Control Report	Annually (minimum, maybe ad hoc)	The Vendor must provide a User Access Control Report annually on a date identified by the State that will minimally include: The list of users who have access and what level of access to the system. Ensure that only legitimate users have access to the system
MES-REP-02	Security	Privileged User Access Control Report	Quarterly (minimum, maybe ad hoc)	The Vendor must provide Privileged User Access Control Reports quarterly that minimally provides: Privileged access that must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know basis.
MES-REP-03	Security	Vulnerability Management Report	Monthly	The Vendor must provide a Vulnerability Management Report that contains: - Report of all servers and systems patched proactively/timely to mitigate the vulnerabilities. - Report of the application components security scanning reports for identifying OWASP TOP 10 vulnerabilities - SAST, DAST, IAST, and RASP testing reports - Cloud security posture management reports
MES-REP-04	Operations	Capacity Planning Report	Monthly	The Vendor must provide Capacity Planning reports monthly. The report must include, at a minimum: - Utilization trends for servers, storage, network, backup hardware and security devices - Thresholds where capacity would be increased - The interval that each of these is measured - Trend of utilization over the previous six months
MES-REP-05	Turnover	Turnover Activities Report	Monthly	The Vendor must provide a Turnover Activities Report documenting that all Vendor turnover activities have been completed on a monthly basis in accordance with the State approved Turnover Plan to include successful transfer of IT inventory, baseline system configuration, financial reconciliation, and operations to the State and successor Contractor as appropriate.
MES-REP-06	O&M	Failed Patching Attempts Report	Monthly	The Vendor must provide patching reports on its failed patching attempts monthly. The report must include: The servers that failed during the week, The number of times each failed, For those that fail two (2) or more consecutive attempts, The number of consecutive attempts, and the remediation plan for each.
MES-REP-07	Call Center	Call Center Metrics Report	Monthly	The Vendor must submit a monthly Call Center Metrics Report that documents key call center statistics in the Department provided format.
MES-REP-08	Project Management	Weekly Status Report	Weekly	The Vendor must submit a weekly status report during DDI and O&M that contains the information defined in the Department's template and guidance document.

Table AA-1 – Reports List

ATTACHMENT AB: INTERFACES

Interface Requirements

The Vendor shall design, develop, and implement interfaces that adhere to recognized **industry standards** and **best practices**, incorporating all required data elements as specified in the provided interface descriptions.

The Vendor is expected to propose and implement interface strategies that enable the required data exchange with trading partners. This shall be achieved through a combination of **migration** of existing interfaces and **re-visioning** of the interface architecture where necessary.

The proposed solution must be fully integrated with the **Medicaid Integration Services (MIS)** platform to support all data exchange functions with other systems and trading partners, as directed by the Department.

The Vendor must factor the **effort, resources, and timeline** required to develop the new interfaces into the **overall cost and schedule** for project implementation and operations. This includes planning for and managing the **decommissioning** of existing interfaces.

Standards and Deliverables

The Vendor must ensure that all interfaces:

1. **Provide accurate, complete, and timely data** to consuming/target systems.
2. **Conform to applicable industry standards and best practices**, including but not limited to:
 - HL7® FHIR®
 - HIPAA X12 EDI transactions
3. **Include comprehensive Interface Control Documents (ICDs)** that describe all functional, technical, and operational aspects of each data exchange.

Interface Types

The Vendor must design and implement interfaces within the following categories. Where trading partners are not currently using these interface types, the Vendor shall include in the scope the effort and time required to assist with their transition.

- a. **Real-Time APIs:** Interfaces (e.g., web services) that transmit data immediately as changes occur, ensuring minimal latency in the target system.
- b. **Near Real-Time APIs:** Interfaces that leverage message queuing to distribute data to one or more consumers for processing as required.
- c. **Mass File Transfer (MFT):** File-based interfaces that exchange data on a scheduled basis between source and target systems.

For **each** interface, an **Interface Control Document (ICD)** is required, aligned with Department requirements and trading partner specifications.

Existing Interfaces Overview

Table AB-1: Provides a high-level scope of the existing interfaces and their approximate volumes. These interfaces currently interact with approximately 28 trading partners.

Vendors must account for:

- The 29 trading partners involved (7 MES modules and 22 additional partners).
- The impact on **design, development timelines, all test cycles, and integration** with the MIS platform.

Table AB-1

Interface Name	Number of Interfaces	Functional description
Payment System Interface	1	The Payment System Interface is a webservice that connects Paypoint to process the Provider Enrollment Fee. This will not go through the MIS.

Bad Debt File	1	The Bad Debt file is an MES module integration with NCTracks. It is a data exchange initiated by the PDMCVO during re-enrollment or revalidation workflows to verify that providers do not have outstanding debt with NCDHHS.
Fee Payment File	1	The Fee Payment file is a data exchange to share with the PDM/CVO from the Financial System (NCTracks) that the provider application fee has been posted. It is an MES module integration to NCTracks.
Provider Network File (PNF) and Response File (PNrF)	2	The Provider Network File (PNF) is used to validate the contracted providers as valid for participation in managed care and consolidate all networks for a provider linked to the provider's source of record. The Provider Network Response File (PNrF) is a response file to return the validation results to the respective health plans. There are 5 Standard Plans, 4 Tailored Plans, 4 Prepaid Inpatient Health Plans (PIHPs), 1 Child and Family Specialty Plan (CFSP), 4 Local Management Entity/Managed Care Organization (LMEs), 1 Tribal Option, and 1 Primary Care Case Management (PCCM) provider networks that will need to be processed following plan specific business rules.
Provider Extract to NCTracks	1	A new Provider extract to NCTracks or replacement system(s) will be required to validate a provider for Fee for Service (FFS) business processes, PMPM capitation payments, management fees, member assignment, and trading partner agreements.
Provider Extract to Data Analytics Platform (DAP)	1	A new module integration with the Data Analytics Platform (DAP) will be needed for a comprehensive extract of provider data extracted from the provider source system to the data warehouse for analysis and reporting.

Provider Extract to Encounter Processing System (EPS)	1	An MES module integration with the Encounter Processing System (EPS) includes an extract that will be sent from the PDM/CVO to the EPS and used to validate a provider for encounter processing for FFS and managed care.
Provider Extract to Interoperability (IO) - Patient Access	1	An MES module integration with Interoperability (IO). The Patient Access extract is used to support Interoperability API requirements for patient access.
Provider Extract to Interoperability (IO) - Provider Directory API	1	An MES module integration with Interoperability (IO). The Provider Directory API extract is used to support Interoperability API requirements for the provider directory. The Patient Access extract is used to support Interoperability API requirements for patient access.
Provider Extract to Pharmacy Benefits Administrator (PBA)	1	An MES module integration with the Pharmacy Benefits Administrator (PBA) which includes an extract is used to validate a provider for pharmacy claims adjudication and Drug Rebate.
Provider Enrollment File (PEF)	1	The Provider Enrollment File (PEF) is used to validate a provider for managed care contracting, claim adjudication, member assignment, and provider directory. A subset of the data used for vendor contracts supporting business functions unrelated to provider enrollment such as third-party recovery. Currently, twenty (20) entities receive this data.
NCFast Provider Directory	1	The NCFast Provider Directory is an MES module integration with NCFast used to validate to support member processes in NCFast including PCP, PHP, and TCM assignments.
Office Admin API	1	An MES Module integration with MIS for an API used to share the user information for the primary and secondary office administrator assigned to a provider to allow the Office Admin (OA) access to all MES modules.

Health Information Exchange (HIE) Provider Assignment File	1	The Health Information Exchange (HIE) Provider Assignment is a file used to populate HIE information as reference data on the provider's source of record.
Provider Directory to the Enrollment Broker (EB)	1	The Provider Directory is a MES Module integration with Enrollment Broker (EB) - this file is used to populate the public facing Enrollment Broker provider directory and the secured directory available to members for Primary Care Provider (PCP) and health plan selection.
Electronic Visit Verification (EVV)	1	The MES Module Electronic Visit Verification (EVV) Provider Extract is an MES Module integration with EVV used to supply the EVV vendor with qualifying providers supporting the EVV system.
NC State Bureau of Investigation (SBI)	1	This interface is with the NC State Bureau of Investigation (SBI) for the purposes of performing fingerprinting analysis. This interface requires restricted access by resources authorized following background check. This will not go through the MIS.
Home and Community Based Services (HCBS)	1	A new interface supporting a DHB monitored provider self-assessment for home and community-based setting providers for compliance with CMS' HCBS Final Rule.

ATTACHMENT AC: GENAI DISCLOSURE AND FACT SHEET

Will you be using or offering GenAI technology, model, or service (collectively, “Solution”)?

☐ Yes ☐ No (If ‘No’, skip to the signature section of this form. If ‘Yes’, provide details regarding the Solution’s GenAI.)

Failure to disclose the use and purpose of GenAI technology to the State as it relates to the Solution requested in this solicitation and submittal of this completed attachment may result in disqualification and may void any resulting contract. Please provide a response to the items listed in each section where indicated.

1. Technical Specifications: – Address the following items in your response:

- a. **Model Name, Version & Number of Parameters:** The unique identifier or name assigned to the specific GenAI model or service.
- b. **Model Owner:** The name of the organization or entity responsible for creating or deploying the GenAI model or service.
- c. **Overview:** A concise summary of the GenAI model’s purpose, functionality, and key characteristics.
- d. **Purpose:** The intended use or goal of the GenAI model (e.g., image recognition, natural language processing, text summarization).
- e. **Intended Domain:** The context, subject matter or domain for which the GenAI model is designed to operate effectively.
- f. **Training Data:** Information used to train the GenAI model (e.g. labeled images, text corpora)
- g. **Model Information:** Details about the architecture, parameters and configuration of the GenAI model.
- h. **Inputs and Outputs:**
 - i. Inputs: The data or features provided to the model for prediction (e.g., images, text).
 - ii. Outputs: The GenAI model’s predictions or results (e.g., class labels, probabilities).
- i. **Customization and Flexibility:** Details on how the solution can be customized to meet specific needs including fine-tuning capabilities.
- j. **Integration Capabilities:** Compatibility with existing systems, API’s and platforms.
- k. **Scalability:** Details on how the solution scales with increased usage or data volume.

Vendor’s Response for Section 1

2. Data Handling and Privacy – Address the following items in your response:

- a. **Data Requirements:** Types of data needed for the solution to function effectively.
- b. **Data Security:** Measures in place to protect data during transit and storage, including encryption standards.
- c. **Data Privacy:** Compliance with data privacy regulations (e.g., GDPR, CCPA) and policies on data ownership and usage.
- d. **Anonymization:** Techniques used to anonymize personal data, if applicable.

Vendor's Response for Section 2

3. **Ethical Considerations** – Address the following items in your response:

- a. **Ethical Guidelines:** Adherence to ethical AI guidelines and principles.
- b. **Impact Assessments:** Regular assessments of the AI's impact on various stakeholders.
- c. **Transparency:** Level of transparency regarding how the AI models make decisions.
- d. **Accountability:** Processes in place for addressing errors or unintended consequences.
- e. **Bias and Fairness:** Methods for detecting and mitigating biases in the AI models.
- f. **Optimal Conditions:** The ideal environment or context for the GenAI model to perform optimally.
- g. **Poor Conditions:** Scenarios or conditions where the GenAI model's performance may degrade.

Vendor's Response for Section 3

4. **Operational Details** – Address the following items in your response:

- a. **Deployment Options:** Available deployment models (cloud, on-premises, hybrid).
- b. **Maintenance and Support:** Support services, including SLAs, and frequency of updates and patches.
- c. **Training and Documentation:** Availability of training materials, user manuals, and ongoing support.

Vendor's Response for Section 4

5. **Cost and Licensing** – Address the following items in your response:

- a. **Pricing Model:** Detailed breakdown of costs, including licensing fees, usage-based fees, and any additional charges.
- b. **Licensing Terms:** Terms and conditions of the software license, including duration, renewal, and termination clauses.

Vendor's Response for Section 5

6. **Performance Metrics** – Address the following items in your response:

- a. **Definition:** Quantitative measures (e.g., accuracy, F1-score) used to evaluate the GenAI model's performance.
- b. **Assessment:** Determines how well the GenAI model meets its intended purpose.
- c. **Continuous Monitoring Plan:** Establishes a plan for continuous monitoring and evaluation of the GenAI model's performance.
- d. **Benchmarks:** Performance benchmarks and KPIs used to measure the solution's effectiveness.
- e. **Case Studies and References:** Examples of previous implementations and references from existing clients.

Vendor's Response for Section 6

7. **Regulatory Compliance** – Address the following items in your response:

- a. **Regulatory Standards:** Compliance with industry-specific regulations and standards (e.g., HIPAA for healthcare, IRS Pub 1075, SSA and SAMSHA).

Vendor's Response for Section 7

8. **Innovation and Roadmap** – Address the following items in your response:

- a. **Future Plans:** Vendor's roadmap for future development and innovation in their GenAI solutions.
- b. **Partnerships and Ecosystem:** Collaborations with other technology providers and integration within a broader AI ecosystem.

Vendor's Response for Section 8

9. Explain how you are ensuring the GenAI system is not adversely affecting decisions that materially impact access to, or approval for, housing or accommodations, education, employment, credit, health care, and criminal justice.

Vendor's Response for Section 9

10. Additional Information that you may like to share:

Offeror Signature

Date

Printed Name and Title