

5.0 TECHNICAL & COST PROPOSAL REQUIREMENTS & SPECIFICATIONS

5.1 MINIMUM REQUIREMENTS

This procurement is open to qualifying Vendors that satisfy the Minimum Requirements described in this section.

When completing the TPA Minimum Requirements Table below and ATTACHMENT K: MINIMUM REQUIREMENTS RESPONSE, Vendors must confirm or not confirm, and only when requested, provide information for all Minimum Requirements. Only those Vendors that meet 100% of the Minimum Requirements will be provided (via SFTP) a de-identified medical claims file for repricing, census data and all other exhibits listed in ATTACHMENT A: PRICING. These files are needed to submit technical and cost proposals for consideration and possible Contract award.

The Plan reserves the right to reject proposals deemed incomplete or non-compliance with these Minimum Requirements.

Vendors shall duplicate the TPA Minimum Requirements Table below and provide the page number reference to the location within Vendor's proposal where the minimum requirement has been satisfied.

TPA MINIMUM REQUIREMENTS TABLE		
	Requirement	RFP Section Number and Page Number of Response
1	Vendor shall provide a description of the company, its operations and ownership.	Section 5.1, Minimum Requirements, page 4
2	Vendor shall provide the city and state for each office where the operational and account management resources dedicated to the Plan will be primarily located.	Section 5.1, Minimum Requirements, Attachment D, page 16
3	a) Vendor shall have provided services to at least one (1) public or private self-funded client with more than 100,000 covered lives. b) If confirmed, provide contact information for one (1) such client so the Plan can complete a reference call related to the services in this RFP.	Section 5.1, Minimum Requirements, page 6

4	<p>a) Vendor shall certify without exception the sufficiency of its security standards, tools, technologies, and procedures in providing Services under this Contract.</p> <p>b) All Vendor and/or third-party Data Centers and Information Technology Systems used under this proposed Contract for the purpose of collecting, storing, transmitting, or exchanging Plan Data shall have and maintain, valid, favorable third-party security certification(s) on all related security controls that are consistent with, and can be cross-walked to, the data classification level and security controls appropriate for moderate information system(s) per the National Institute of Standards and Technology (“NIST”) SP 800-53 Rev. 5 or the most recent revision. To satisfy this requirement, reports must have been issued within twelve (12) months prior to the anticipated Contract award date or be supplemented by bridge letters covering no more than two (2) years subsequent to the initial report issuance date. Vendor shall provide a crosswalk document along with full copies of the third-party security certification or assessment report(s), and any necessary bridge letters. Vendor shall also identify which specific system(s) covered by the third-party security certifications or attestations will be used to provide the Services under this Contract. Opinion letters or security certification attestation letters will not be submitted in lieu of full report(s).</p> <p>c) Vendor shall agree that the Plan has the right to independently evaluate, audit, and verify such requirements as part of its evaluation and during the life of the Contract, including requesting the performance of a penetration test with satisfactory results. The State will verify any such</p>	Section 5.1, Minimum Requirements, page 6
---	---	---

	<p>third-party security certification or assessment report yearly during the life of the Contract, and Vendor will be required to provide an updated report or bridge letter verifying that there have been no material changes in the controls reported since the issuance of the last report. Bridge letters will only be accepted for two (2) years after the date of the initial report to satisfy this requirement.</p> <p>d) Vendor shall agree that the Plan has the right to, based upon its evaluation, require that Vendor maintain cyber breach liability insurance coverage in an amount specified by the Plan, and/or commit to obtaining a favorable third-party security certification or assessment report no later than six months prior to the date that Services under this Contract begin as a condition of Contract award. Vendor shall provide documentation of the amount of cyber breach liability insurance that it currently carries for all Vendor and/or third-party Data Centers and Information Technology Systems used to provide the Services under this Contract that will contain Plan Data. If Vendor is currently undergoing a third-party NIST SP 800-53 Rev. 5 (or most recent revision) compliant security assessment of such Data Centers or Information Technology Systems, Vendor shall provide proof of purchase or a copy of its contract with the third-party retained to perform the audit, and the expected date for completion.</p> <p>e) Vendor shall accept, and the Plan understands, that security certification and assessment reports and security information provided to the State for the purpose of this Contract may contain confidential information and/or trade secrets. Refer to Section 14 "Confidential Information" of ATTACHMENT B: INSTRUCTIONS TO VENDORS for information regarding the treatment of Confidential Information.</p>	<p>Section 5.1, Minimum Requirements, page 7</p> <p>Section 5.1, Minimum Requirements, page 7</p>
<p>5</p>	<p>Vendor must demonstrate financial stability. Vendor shall provide audited or reviewed financial statements prepared by an independent Certified Public Accountant (CPA) for the two (2) most recent fiscal years that shall include, at a minimum, a balance sheet, income statement (i.e., profit/loss statement), and cash flow statement and, if the most recent audited or reviewed financial statement was prepared more than six (6) months prior to the issuance of this RFP, the Vendor shall also submit its most recent internal financial statements (balance sheet, income statement, and cash flow statement or budget), with entries reflecting revenues and expenditures from the date of the audited or reviewed financial statement, to the end of the most recent financial reporting period (i.e., the quarter or month preceding the issuance date of this RFP). Vendor is encouraged to explain any negative financial information in its financial statement and is encouraged to provide documentation supporting those explanations.</p> <p>Consolidated financial statement of the Vendor's parent or related corporation/business entity shall not be considered, unless: 1) the Vendor's actual financial performance for the designated period is separately identified in and/or attached to the consolidated statements; 2) the parent or related corporation/business entity provides the State with a document wherein the parent or related corporation/business entity will be financially responsible for the Vendor's performance of the contract and the consolidated statement demonstrates the parent or related corporation's/business entity's financial ability to perform the contract, financial stability, and/or such other financial considerations identified in the evaluation criteria; and/or 3) Vendor provides its own internally prepared</p>	<p>Section 5.1, Minimum Requirements, page 7</p>

	financial statements and such other evidence of its own financial stability identified above.	
6	Vendor shall confirm it agrees to ATTACHMENT C: NORTH CAROLINA GENERAL TERMS AND CONDITIONS without exception.	Section 5.1, Minimum Requirements, Attachment C, page 9
7	Vendor shall complete and submit ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR.	Section 5.1, Minimum Requirements, Attachment D, page 16
8	Vendor shall be financially stable; and complete, sign and submit without exception, ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION.	Section 5.1, Minimum Requirements, Attachment E, page 18
9	Vendor shall complete, sign, and submit ATTACHMENT G: BUSINESS ASSOCIATE AGREEMENT.	Section 5.1, Minimum Requirements, Attachment G, page 19
10	Vendor shall provide sufficient documentation and demonstrate HIPAA compliance through completing, signing, and submitting ATTACHMENT H: HIPAA QUESTIONNAIRE. If Vendor maintains that any information in documents submitted to demonstrate HIPAA compliance is proprietary or otherwise confidential, Vendor may Redact those portions in black.	Section 5.1, Minimum Requirements, Attachment H, page 28
11	Vendor shall complete, sign, and submit ATTACHMENT I: NONDISCLOSURE AGREEMENT.	Section 5.1, Minimum Requirements, Attachment I, page 41
12	Vendor shall complete, sign, and submit ATTACHMENT J: MINIMUM REQUIREMENTS SUBMISSION INFORMATION form.	Section 5.1, Minimum Requirements, Attachment J, page 42
13	Vendor shall confirm it agreed to all performance guarantees as described in Section 6.3 and Schedules I and II.	Section 5.1, Minimum Requirements, page 8

1. Vendor shall provide a description of the company, its operations and ownership.

UMR has a unique advantage of being both large in size, yet flexible in service. Through the power of our parent company, UnitedHealth Group, we have the resources and scale to offer significant network discounts and cutting-edge benefit solutions. We are also able to make substantial capital investments in our systems, which puts us ahead of the curve in implementing changes to meet evolving market expectations and regulatory mandates.

UMR has almost 70 years of experience listening to and answering the needs of self-funded employers. Last year, UMR processed 75,642,795 medical, dental, pharmacy and disability claims, paying \$21,644,284,038. Currently, we are serving 3,644 customers, including 715 public sector and labor customers.

NATIONAL REACH

Based in Wausau, Wisconsin, UMR has offices/operations across the country, allowing us to provide a local presence for our customers and members, whenever possible. We anticipate administering your account primarily from Greensboro, North Carolina.

In addition, we have experienced staff based in the following locations:

- Arkansas – Little Rock

- Colorado – Denver
- Illinois — Rockford
- Kentucky — Lexington
- Missouri – St. Louis
- Nevada – Las Vegas
- New York – Syracuse
- Ohio — Cincinnati, Columbus
- Tennessee – Nashville
- Texas — El Paso, San Antonio
- Washington — Seattle
- West Virginia – Charleston
- Wisconsin — Green Bay, Wausau

BEST-IN-CLASS SELF-FUNDED SOLUTIONS

Our customers range from privately owned companies publicly held corporations and large state governments. Most of these customers ask us to administer multiple, complex benefit designs with varying reimbursement methods. Creating a custom solution that works for our customers is what we do best. Our services include:

- Medical administration
- Network solutions
- Member advocacy
- Customer reporting and analytics
- Stop loss coverage
- COBRA/HIPAA administration
- Pharmacy benefits administration
- UMR Clinical Advocacy Relationships to Empower (CARE)
- Consumer-driven health plans
- Ancillary and specialty solutions

COMPANY OWNERSHIP

UMR is the TPA line of business for UnitedHealthcare, a business unit of UnitedHealth Group. UnitedHealth Group is a publicly held company whose common stock is traded on the New York Stock Exchange as UNH. Headquartered in Minnetonka, Minnesota, UnitedHealth Group offers a broad spectrum of products and services dedicated to making health care work better. Through its family of businesses, UnitedHealth Group serves 146 million individuals worldwide.

2. Vendor shall provide the city and state for each office where the operational and account management resources dedicated to the Plan will be primarily located.

Provided in Attachment D on page 16.

3a. Vendor shall have provided services to at least one (1) public or private self-funded client with more than 100,000 covered lives.

Confirmed.

3b. If confirmed, provide contact information for one (1) such client so the Plan can complete a reference call related to the services in this RFP.

National Rural Electric Cooperative Association
Jodi Fuller, Vice President of Product Development and Management
(703) 907-6020
jodi.fuller@nreca.coop
100,818 current subscriber count

4a. Vendor shall certify without exception the sufficiency of its security standards, tools, technologies, and procedures in providing Services under this Contract.

Confirmed.

4b. All Vendor and/or third-party Data Centers and Information Technology Systems used under this proposed Contract for the purpose of collecting, storing, transmitting, or exchanging Plan Data shall have and maintain, valid, favorable third-party security certification(s) on all related security controls that are consistent with, and can be cross-walked to, the data classification level and security controls appropriate for moderate information system(s) per the National Institute of Standards and Technology (“NIST”) SP 800-53 Rev. 5 or the most recent revision. To satisfy this requirement, reports must have been issued within twelve (12) months prior to the anticipated Contract award date or be supplemented by bridge letters covering no more than two(2) years subsequent to the initial report issuance date. Vendor shall provide a crosswalk document along with full copies of the third-party security certification or assessment report(s), and any necessary bridge letters. Vendor shall also identify which specific system(s) covered by the third-party security certifications or attestations will be used to provide the Services under this Contract. Opinion letters or security certification attestation letters will not be submitted in lieu of full report(s).

Confirmed. Please note the HITRUST assessments cover over 30 applications. Therefore, the maturity scores represent an aggregate score for all applications. Please refer to the document titled: **UHC 2022 – HITRUST R2 Validated Assessment Rpt Final with Watermark.**

4c. Vendor shall agree that the Plan has the right to independently evaluate, audit, and verify such requirements as part of its evaluation and during the life of the Contract, including requesting the performance of a penetration test with satisfactory results. The State will verify any such third-party security certification or assessment report yearly during the life of the Contract, and Vendor will be required to provide an updated report or bridge letter verifying that there have been no material changes in the controls reported since the issuance of the last report. Bridge letters will only be accepted for two (2) years after the date of the initial report to satisfy this requirement.

Confirmed.

4d. Vendor shall agree that the Plan has the right to, based upon its evaluation, require that Vendor maintain cyber breach liability insurance coverage in an amount specified by the Plan, and/or commit to obtaining a favorable third-party security certification or assessment report no later than six months prior to the date that Services under this Contract begin as a condition of Contract award. Vendor shall provide documentation of the amount of cyber breach liability insurance that it currently carries for all Vendor and/or third-party Data Centers and Information Technology Systems used to provide the Services under this Contract that will contain Plan Data. If Vendor is currently undergoing a third-party NIST SP 800-53 Rev. 5 (or most recent revision) compliant security assessment of such Data Centers or Information Technology Systems, Vendor shall provide proof of purchase or a copy of its contract with the third-party retained to perform the audit, and the expected date for completion.

Confirmed.

4e. Vendor shall accept, and the Plan understands, that security certification and assessment reports and security information provided to the State for the purpose of this Contract may contain confidential information and/or trade secrets. Refer to Section 14 “Confidential Information” of ATTACHMENT B: INSTRUCTIONS TO VENDORS for information regarding the treatment of Confidential Information.

Confirmed.

5. Vendor must demonstrate financial stability. Vendor shall provide audited or reviewed financial statements prepared by an independent Certified Public Accountant (CPA) for the two (2) most recent fiscal years that shall include, at a minimum, a balance sheet, income statement (i.e., profit/loss statement), and cash flow statement and, if the most recent audited or reviewed financial statement was prepared more than six (6) months prior to the issuance of this RFP, the Vendor shall also submit its most recent internal financial statements (balance sheet, income statement, and cash flow statement or budget), with entries reflecting revenues and expenditures from the date of the audited or reviewed financial statement, to the end of the most recent financial reporting period (i.e., the quarter or month preceding the issuance date of this RFP). Vendor is encouraged to explain any negative financial information in its financial statement and is encouraged to provide documentation supporting those explanations.

Consolidated financial statement of the Vendor’s parent or related corporation/business entity shall not be considered, unless: 1) the Vendor’s actual financial performance for the designated period is separately identified in and/or attached to the consolidated statements; 2) the parent or related corporation/business entity provides the State with a document wherein the parent or related corporation/business entity will be financially responsible for the Vendor’s performance of the contract and the consolidated statement demonstrates the parent or related corporation’s/business entity’s financial ability to perform the contract, financial stability, and/or such other financial considerations identified in the evaluation criteria; and/or 3) Vendor provides its own internally prepared financial statements and such other evidence of its own financial stability identified above.

Confirmed.

6. Vendor shall confirm it agrees to ATTACHMENT C: NORTH CAROLINA GENERAL TERMS AND CONDITIONS without exception.

Confirmed.

7. Vendor shall complete and submit ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR.

Confirmed.

8. Vendor shall be financially stable; and complete, sign and submit without exception, ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION.

Confirmed.

9. Vendor shall complete, sign, and submit ATTACHMENT G: BUSINESS ASSOCIATE AGREEMENT.

Confirmed.

10. Vendor shall provide sufficient documentation and demonstrate HIPAA compliance through completing, signing, and submitting ATTACHMENT H: HIPAA QUESTIONNAIRE. If Vendor maintains that any information in documents submitted to demonstrate HIPAA compliance is proprietary or otherwise confidential, Vendor may Redact those portions in black.

Confirmed.

11. Vendor shall complete, sign, and submit ATTACHMENT I: NONDISCLOSURE AGREEMENT.

Confirmed.

12. Vendor shall complete, sign, and submit ATTACHMENT J: MINIMUM REQUIREMENTS SUBMISSION INFORMATION form.

Confirmed.

13. Vendor shall confirm it agreed to all performance guarantees as described in Section 6.3 and Schedules I and II.

Confirmed.

ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS & CONDITIONS

UMR has reviewed Attachment C: North Carolina General Contract Terms & Conditions of your request for proposal (RFP) and is confident in our ability to meet your needs. We are in agreement with the terms stated below.

1. PERFORMANCE AND DEFAULT:

- a) It is anticipated that the tasks and duties undertaken by the Vendor under the contract which results from the State solicitation in this matter (Contract) shall include Services, and/or the manufacturing, furnishing, or development of goods and other tangible features or components, as Deliverables.
- b) 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. The State is authorized to access State Data provided by the State 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 Vendor requiring a separate maintenance or support agreement unless otherwise specifically agreed in writing. User access to the Services shall be routinely provided by Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. In the absence of an SLA, Vendor agrees to provide the Services at least in the manner that it provides accessibility to the services to comparable users.
- c) The State's right to access the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of Vendor or any third party, nor does this right of access transfer, vest, or infer any title or other ownership right in any intellectual property 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 Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use any State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein. 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 users for similar Services. 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 of the Services, but minimally as provided for and specified herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of Vendor. Any training specified herein will be provided by Vendor to specified State users for the fees or costs as set forth herein or in an SLA.
- e) Some Services provided online 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) If Vendor modifies or replaces the Services provided to the State and other comparable users, and if the State has paid all applicable 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.
 - g) If, through any cause, Vendor shall fail to fulfill in timely and proper manner the obligations under the Contract, the State shall have the right to terminate the Contract by giving written notice to Vendor and specifying the effective date thereof. In that event, any or all finished or unfinished deliverable items under the Contract prepared by Vendor shall, at the option of the State, become its property, and Vendor shall be entitled to receive just and equitable compensation for any acceptable work completed as to which the option is exercised. Notwithstanding, Vendor shall not be relieved of liability to the State for damages sustained by the State by virtue of any breach of the Contract, and the State may withhold any payment due Vendor for the purpose of setoff until such time as the exact amount of damages due the State from such breach can be determined. The State reserves the right to require at any time a performance bond or other acceptable alternative performance guarantees from a Vendor without expense to the State.
 - h) In the event of default by Vendor, the State may procure the goods and Services necessary to complete performance hereunder from other sources and hold Vendor responsible for any excess cost occasioned thereby. In addition, in the event of default by Vendor under the Contract, or upon Vendor filing a petition for bankruptcy or the entering of a judgment of bankruptcy by or against Vendor, the State may immediately cease doing business with Vendor, immediately terminate the Contract for cause, and may take action to debar Vendor from doing future business with the State.
 - i) The State may document and take into account in awarding or renewing future procurement contracts the general reputation, performance, and performance capabilities of the Vendor under this Contract.
2. **GOVERNMENTAL RESTRICTIONS:** In the event any Governmental restrictions are imposed which necessitate alteration of the material, quality, workmanship or performance of the goods or Services offered prior to their delivery, it shall be the responsibility of Vendor to notify the Contract Administrator at once, in writing, indicating the specific regulation which required such alterations. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Contract.
3. **AVAILABILITY OF FUNDS:** Any and all payments to Vendor shall be dependent upon and subject to the availability of funds to the agency for the purpose set forth in the Contract.
4. **TAXES:** Any applicable taxes shall be invoiced as a separate item.
- a) The State does not enter into Contracts with Vendors if Vendor 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 Vendor and (3) Systematic exploitation of the market by media-assisted, media-facilitated, or media-solicited means. By execution of the proposal document Vendor certifies that it and all of its affiliates, (if it has affiliates), collect(s) the appropriate taxes.
 - b) The agency(ies) participating in the Contract are exempt from Federal Taxes, such as excise and transportation. Exemption forms submitted by Vendor will be executed and returned by the using agency.

- c) Prices offered are not to include any personal property taxes, nor any sales or use tax (or fees) unless required by the North Carolina Department of Revenue.

5. **SITUS AND GOVERNING LAWS:** This Contract is made under and shall be governed and construed in accordance with the laws of the State of North Carolina, without regard to its conflict of laws rules, and within which State all matters, whether sounding in Contract or tort or otherwise, relating to its validity, construction, interpretation, and enforcement shall be determined.

6. **PAYMENT TERMS:** Payment terms are Net not later than 30 days after receipt of correct invoice or acceptance of goods, whichever is later. The using agency is responsible for all payments to Vendor under the Contract. Payment by some agencies may be made by procurement card, if Vendor accepts that card (Visa, MasterCard, etc.) from other customers, and it shall be accepted by the Vendor for payment under the same terms and conditions as any other method of payment accepted by Vendor. If payment is made by procurement card, then payment may be processed immediately by Vendor.

The State does not agree in advance, in contract, pursuant to Constitutional limitations, to pay costs such as interest, late fees, penalties, or attorney’s fees. This Contract will not be construed as an agreement by the State to pay such costs and will be paid only as ordered by a court of competent jurisdiction.

7. **NON-DISCRIMINATION:** Vendor will take necessary action to comply with all Federal and State requirements concerning fair employment and employment of people with disabilities, and concerning the treatment of all employees without regard to discrimination on the basis of any prohibited grounds as defined by Federal and State law.

8. **CONDITION AND PACKAGING:** Unless otherwise provided by special terms and conditions or specifications, it is understood and agreed that any item offered or shipped has not been sold or used for any purpose and shall be in first class condition. All containers/packaging shall be suitable for handling, storage, or shipment.

9. **INTELLECTUAL PROPERTY WARRANTY AND INDEMNITY:** Vendor shall hold and save the 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 patent-pending invention, article, device, or appliance delivered in connection with the Contract.

- 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) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become non-infringing. If neither of these options can reasonably be taken in Vendor’s judgment, or if further use shall be prevented by injunction, Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.
- c) 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 supplied by Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. Vendor

shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:

- i. That Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii. That 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) 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 results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.
- e) Vendor shall hold and save the 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 patent-pending invention, article, device, or appliance delivered in connection with the Contract.
10. **TERMINATION FOR CONVENIENCE:** If this Contract contemplates deliveries or performance over a period of time, the State may terminate this Contract at any time by providing 60 days' notice in writing from the State to Vendor. In that event, any or all finished or unfinished deliverable items prepared by Vendor under this Contract shall, at the option of the State, become its property. If the Contract is terminated by the State as provided in this section, the State shall pay for those items for which such option is exercised, less any payment or compensation previously made.
11. **ADVERTISING:** Vendor agrees not to use the existence of the Contract or the name of the State of North Carolina as part of any commercial advertising or marketing of products or Services. A Vendor may inquire whether the State is willing to act as a reference by providing factual information directly to other prospective customers.
12. **ACCESS TO PERSONS AND RECORDS:** During and after the term hereof, the State Auditor and any using agency's internal auditors shall have access to persons and records related to the Contract to verify accounts and data affecting fees or performance under the Contract.
13. **ASSIGNMENT:** No assignment of Vendor's obligations nor Vendor's right to receive payment hereunder shall be permitted. However, upon written request approved by the issuing purchasing authority and solely as a convenience to Vendor, the State may:
- a) Forward Vendor's payment check directly to any person or entity designated by Vendor, and
 - b) Include any person or entity designated by Vendor as a joint payee on Vendor's payment check.

In no event shall such approval and action obligate the State to anyone other than Vendor and Vendor shall remain responsible for fulfillment of all Contract obligations. Upon advance written request, the State may, in its unfettered discretion, approve an assignment to the surviving entity of a merger, acquisition or corporate reorganization, if made as part of the transfer of all or substantially all of Vendor's assets. Any purported assignment made in violation of this provision shall be void and a material breach of the Contract.

14. **INSURANCE:**

- a) **COVERAGE** - During the term of the Contract, Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Contract. As a minimum, Vendor shall provide and maintain the following coverage and limits:
 - i. **Worker's Compensation** - Vendor 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 \$500,000.00, covering all of Vendor's employees who are engaged in any work under the Contract in North Carolina. If any work is sub-contracted, Vendor shall require the sub-Contractor to provide the same coverage for any of his employees engaged in any work under the Contract within the State.

- ii. **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$1,000,000.00 Combined Single Limit. Defense cost shall be in excess of the limit of liability.
- iii. **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired, and non-owned vehicles, used within North Carolina in connection with the Contract. The minimum combined single limit shall be \$250,000.00 bodily injury and property damage; \$250,000.00 uninsured/under insured motorist; and \$2,500.00 medical payment.

- b) **REQUIREMENTS** - Providing and maintaining adequate insurance coverage is a material obligation of Vendor and is of the essence of the 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. Vendor shall at all times 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 the Contract. The limits of coverage under each insurance policy maintained by Vendor shall not be interpreted as limiting Vendor's liability and obligations under the Contract.

15. GENERAL INDEMNITY: Vendor 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 the 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 Vendor in the performance of the Contract and that are attributable to the negligence or intentionally tortious acts of Vendor provided that Vendor is notified in writing within 30 days from the date that the State has knowledge of such claims. Vendor 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 Vendor goods or Services to the State. As part of this provision for indemnity, if federal funds are involved in this procurement, the Vendor warrants that it will comply with all relevant and applicable federal requirements and laws, and will indemnify and hold and save the State harmless from any claims or losses resulting to the State from the Vendor's noncompliance with such federal requirements or law in this Contract. The representation and warranty in the preceding sentence shall survive the termination or expiration of the Contract. The State does not participate in indemnification due to Constitutional restrictions, or arbitration, which effectively and unacceptably waives jury trial. See, G.S. 22B-3, -10.

16. ELECTRONIC PROCUREMENT:

- a) Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Service. Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract.
- b) Reserve.
- c) Reserve.
- d) Reserve.
- e) Vendor shall at all times maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If Vendor is a corporation, partnership, or other legal entity,

then Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges by 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 Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by email. Vendor shall cooperate with the State and the Supplier Manager to mitigate and correct any security breach.

17. **SUBCONTRACTING:** Performance under the Contract by Vendor shall not be subcontracted without prior written approval of the State's assigned Contract Administrator. Unless otherwise indicated, acceptance of a Vendor's proposal shall include approval to use the Subcontractor(s) that have been specified therein.
18. **CONFIDENTIALITY:** Vendor information that cannot be shown to be, e.g., a trade secret, may be subject to public disclosure under the terms of the State Public Records Act (SPRA), beginning at N.C.G.S. § 132.1. Blanket assertions of confidentiality are not favored, but confidentiality of specific material meeting one or more exceptions in the SPRA will be honored. Vendors are notified that if the confidentiality of material is challenged by other parties, the Vendor has the responsibility of defending the assertion of confidentiality.

Any State information, data, instruments, documents, studies, or reports given to or prepared or assembled by or provided to Vendor under the Contract shall be kept as confidential, used only for the purpose(s) required to perform the Contract and not divulged or made available to any individual or organization without the prior written approval of the State.

19. **CARE OF STATE DATA AND PROPERTY:** Vendor agrees that it shall be responsible for the proper custody and care of any data owned and furnished to Vendor by the State (State Data), or other State property in the hands of Vendor, for use in connection with the performance of the Contract or purchased by or for the State for the Contract. Vendor will reimburse the State for loss or damage of such property while in Vendor's custody.

The State Data in the hands of Vendor shall be protected from unauthorized disclosure, loss, damage, destruction by a natural event or other eventuality. Such State Data shall be returned to the State in a form acceptable to the State upon the termination or expiration of this Agreement. Vendor shall notify the State of any security breaches within 24 hours as required by N.C.G.S. § 143B.1379. See N.C.G.S. § 75-60 et seq.

20. **OUTSOURCING:** Any Vendor 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 contact center services are being provided.

If, after award of a contract, Vendor wishes to relocate or outsource any portion of performance to a location outside the United States, or to contract with a subcontractor for any such the 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.

Vendor shall give notice to the using agency of any relocation of Vendor, employees of Vendor, subcontractors of Vendor, or other persons providing performance under a State contract to a location outside of the United States.

21. **COMPLIANCE WITH LAWS:** Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and its performance in accordance with the Contract, including those of federal, state, and local agencies having jurisdiction and/or authority.
22. **ENTIRE AGREEMENT:** This RFP and any documents incorporated specifically by reference represent the entire agreement between the parties and supersede all prior oral or written statements or agreements. This RFP, any addenda hereto, and Vendor's proposal are incorporated herein by reference as though set forth verbatim.

All promises, requirements, terms, conditions, provisions, representations, guarantees, and warranties contained herein shall survive the contract expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable Federal or State statutes of limitation.

- 23. ELECTRONIC RECORDS:** The State will digitize all Vendor responses to this solicitation, if not received electronically, as well as any awarded contract together with associated procurement-related documents. These electronic copies shall constitute a preservation record, and shall serve as the official record of this procurement with the same force and effect as the original written documents comprising such record. Any electronic copy, printout, or other output readable by sight shown to reflect such record accurately shall constitute an "original."
- 24. AMENDMENTS:** This Contract may be amended only by a written Amendment duly executed by the State and Vendor. No changes in the technical requirements & specifications, time for performance, or other contractual terms shall be effective without a written Amendment.

Notwithstanding this requirement, (1) if needed or applicable, the addition of BRDs or Implementation Plans or ADMs may be developed or modified in writing and signed by Vendor's Contract Administrator for day to day activities or other individual authorized to bind Vendor, and the Plan's Contract Administrator for day to day activities or other designee approved by the Plan's Executive Administrator; and (2) due dates referenced in the technical requirements & specifications as "to be determined by the Plan" will be established in writing by the Plan's Contract Administrator for day to day activities through either the Implementation Plan, a BRD or an ADM. Such documents are incorporated into the Contract when signed and are given the precedence as set forth in RFP Section 4.13 "Contract Documents".

- 25. NO WAIVER:** Notwithstanding any other language or provision in the Contract, nothing herein is intended nor shall be interpreted as a waiver of any right or remedy otherwise available to the State under applicable law. The waiver by the State of any right or remedy on any one occasion or instance shall not constitute or be interpreted as a waiver of that or any other right or remedy on any other occasion or instance.
- 26. 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.
- 27. SOVEREIGN IMMUNITY:** Notwithstanding any other term or provision in the Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity or other State or federal constitutional provision or principle that otherwise would be available to the State under applicable law.
- 28. PERFORMANCE BOND:** Vendor shall provide contract performance security based upon ten percent (10%) of the estimated contract total based on Vendor's cost proposal. This security will be in the form of a surety bond licensed in North Carolina with a Best's rating of no less than A-. The contract performance surety will be provided to the Plan's Contracting Section within 30 calendar days from the date of execution of the contract. This security must remain in effect for the entire term of the contract. A new surety bond must be issued if the contract is renewed or extended.

ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR

Vendor shall detail the location(s) at which performance will occur, as well as the manner in which it intends to utilize resources or workers outside of the United States in the performance of The Contract.

Vendor shall complete items 1 and 2 below.

1. Will any work under this Contract be performed outside of the United States? YES NO

If "YES":

a) List the location(s) outside of the United States where work under the Contract will be performed by the Vendor, any subcontractors, employees, or any other persons performing work under the Contract.

Not applicable.

b) Specify the manner in which the resources or workers will be utilized:

Not applicable.

2. Where within the United States will work be performed?

We anticipate providing claim processing, member service and account management for The Plan primarily from Greensboro, North Carolina.

UMR has offices/operations across the country, allowing us to provide a local presence for our customers and members whenever possible. This includes teams based in the following locations:

- Arkansas – Little Rock
- Colorado – Denver
- Illinois — Rockford
- Kentucky — Lexington
- Missouri – St. Louis
- Nevada – Las Vegas
- New York – Syracuse
- Ohio — Cincinnati, Columbus
- Tennessee – Nashville
- Texas — El Paso, San Antonio
- Washington — Seattle
- West Virginia – Charleston
- Wisconsin — Green Bay, Wausau

NOTES:

1. The State will evaluate the additional risks, costs, and other factors associated with the utilization

of workers outside of the United States prior to making an award.

2. Vendor shall provide notice in writing to the State of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing services under the Contract to a location outside of the United States.
3. All Vendor or subcontractor personnel providing call or contact center services to the State of North Carolina under the Contract shall disclose to inbound callers the location from which the call or contact center services are being provided.

ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION

Name of Vendor UMR, Inc.

The undersigned hereby certifies that: [check all applicable boxes]

Vendor is in sound financial condition and, if applicable, has received an unqualified audit opinion for the latest audit of its financial statements.

Date of latest audit: 01/01/2021 (if no audit within past 18 months, explain reason below.)

Vendor has no outstanding liabilities, including tax and judgment liens, to the Internal Revenue Service or any other government entity.

Vendor is current in all amounts due for payments of federal and state taxes and required employment-related contributions and withholdings.

Vendor is not the subject of any current litigation or findings of noncompliance under federal or state law.

Vendor has not been the subject of any past or current litigation, findings in any past litigation, or findings of noncompliance under federal or state law that may impact in any way its ability to fulfill the requirements of this Contract.

He or she is authorized to make the foregoing statements on behalf of Vendor.

Note: This shall constitute a continuing certification and Vendor shall notify the Contract Administrator within 30 days of any material change to any of the representations made herein.

If any one or more of the foregoing boxes is NOT checked, Vendor shall explain the reason(s) in the space below. Failure to include an explanation may result in Vendor being deemed non-responsive and its submission rejected in its entirety.

Item 2 response:

The lien arose because UMR was incorrectly assessed penalties by the IRS. It appears that the incorrect assessment was due to a IRS system error. UMR has engaged legal counsel to resolve this matter, which has been delayed due to IRS staffing issues resulting in a lien being assigned against UMR.

Item 4 response:

Because of the nature of our business, we are routinely subject to lawsuits alleging various causes of action. Although the results of pending litigation are always uncertain, we do not believe the results of any such actions, currently threatened or pending, individually or in the aggregate, will have a material adverse effect on our consolidated financial position or the results of our operations. Any material litigation or legal actions are disclosed in our financial statements available on the UnitedHealth Group Incorporated (UnitedHealth Group) website: www.unitedhealthgroup.com. UnitedHealth Group is our parent company.



Signature

09/16/2022

Date

Scott Hogan, President and Chief Executive Officer
Name

Title Printed

[This Certification must be signed by an individual authorized to speak for Vendor]

ATTACHMENT G: BUSINESS ASSOCIATE AGREEMENT

This Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Business Associate Agreement ("BAA" or "Agreement") is entered into between the North Carolina State Health Plan for Teachers and State Employees ("Plan"), a division and Covered Healthcare Component of the North Carolina Department of State Treasurer ("DST"), and [INSERT NAME OF ENTITY] (hereinafter "Contractor"), referred to as "Party" or collectively as "Parties." This BAA is effective when signed by the Parties and, except as otherwise required, shall remain in effect for the term of the Contract, including any extensions or renewals.

BACKGROUND

DST includes, as a division, the Plan. The Plan is a health benefit plan which, standing alone, would be a covered entity under HIPAA. DST includes several divisions that do not qualify as covered entities and whose functions are not regulated by HIPAA, and thus has designated itself a "Hybrid Entity." The Parties believe that the relationship between Contractor and the Plan is such that Contractor is or may be a Business Associate as defined by the HIPAA Privacy and Security Rules.

The purpose of this BAA between Contractor and the Plan is to protect Plan Member information in accordance with the HIPAA Privacy and Security Rules. The Parties enter this BAA with the intent to comply with HIPAA provisions that allow: 1) a Covered Healthcare Component of a Hybrid Entity (the Plan) to disclose Protected Health Information ("PHI") to a Business Associate; and 2) a Business Associate (i.e., Contractor) to create, maintain, transmit, or receive PHI on behalf of the Plan after the Plan obtains satisfactory assurances that Contractor will appropriately safeguard the information.

Specifically, Sections 261 through 264 of the Federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," direct the United States Department of Health and Human Services to develop standards to protect the security, confidentiality, and integrity of health information. 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 (Pub. L. 111-5)) modified and amended the Administrative Simplification provisions. Pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services ("Secretary") issued regulations modifying 45 C.F.R. Parts 160 and 164 (the "HIPAA Rules"), as further amended by the Omnibus Final Rule (78 Fed. Reg. 5566), (hereinafter, the Administrative Simplification provisions, HITECH, such rules, amendments, and modifications, including any that are subsequently adopted, will be collectively referred to as "HIPAA").

The Parties wish to enter into an agreement through which Contractor will provide certain services and/or products to the Plan. Pursuant to such agreement, Contractor may be considered a Business Associate of the Plan as defined by HIPAA in that Contractor may have access to PHI to meet the requirements of the Contract. The Parties agree as follows:

I. GENERAL TERMS AND CONDITIONS

- A. **Definitions**: Except as otherwise defined herein, any and all capitalized terms or abbreviations of capitalized terms in this Agreement shall have the definitions set forth by HIPAA. In the event of an inconsistency between the provisions of this BAA and mandatory provisions of HIPAA, HIPAA shall control. Where provisions of this BAA are different from those mandated by HIPAA, but are nonetheless permitted by HIPAA, the provisions of this BAA shall control.
- B. **Ambiguous Terms**: In case of ambiguous, inconsistent, or conflicting terms within this BAA, such terms shall be resolved to allow for compliance with HIPAA.
- C. **Application of Civil and Criminal Penalties**: Contractor acknowledges that it is subject to 42 U.S.C. 1320d-5 and 1320d-6 in the same manner as such sections apply to a Hybrid Entity, to the extent that Contractor violates §§ 13401(a), 13404(a), or 13404(b) of the HITECH Act and 45 C.F.R. §164.502(e)

and 164.504(e). Furthermore, Contractor is liable for the acts of its own Business Associates under 45 C.F.R. §160.402(c), who are considered Subcontractors when they have access to Plan PHI.

- D. **Assignment:** Contractor shall not assign or transfer any right or interest in this BAA. Any attempt by Contractor to assign or transfer any right or interest in this BAA is void and has no effect.
- E. **Forum:** The laws of the State of North Carolina shall govern this BAA and any and all interpretations of this BAA. The venue for any claim, demand, suit, or causes of action shall be in the state and federal courts located in North Carolina.
- F. **Hybrid Entity:** HIPAA defines a Hybrid Entity as one that uses or discloses PHI for only a part of its business operations. DST has taken the designation of Hybrid Entity because it includes the Plan as a division.
- G. **Indemnification:** Any Breaches of HIPAA or this BAA shall be subject to the indemnification clause which can be found in Section 15, "General Indemnity" of Attachment C, "North Carolina General Contract Terms and Conditions" of the Contract.
- H. **Regulatory References:** Any reference in this BAA to a federal or state statute or regulation (whether specifically or generally) means that statute or regulation which is in effect on the date of any action or inaction relating to the BAA section which refers to such statute or regulation.
- I. **Stricken Provisions:** In the event any portion of this BAA is determined by a court or other body of competent jurisdiction to be invalid or unenforceable, that portion alone will be deemed void, and the remainder of the BAA will continue in full force and effect.
- J. **Termination of BAA:** Except as otherwise provided below, either Party shall have the right to terminate the Contract if either Party determines that the other Party has violated any material term of this BAA. Upon either Party's belief of a material breach of this BAA by the other Party, the non-breaching Party:
 - 1. Shall give written notice of belief of material breach within a reasonable time after forming that belief. The non-breaching Party shall provide an opportunity for the breaching Party to cure the breach or end the violation and, if the breaching Party does not cure the breach or end the violation within the time specified by the non-breaching Party, the non-breaching Party may exercise such rights as are specified in the Contract; or
 - 2. May immediately exercise such rights as are specified in the Contract if the breaching Party has breached a material term of this BAA and cure is not possible; or
 - 3. Shall report the violation to the Secretary of the United States Department of Health and Human Services if neither termination nor cure is possible. The Plan shall abide by Federal reporting regulations.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

- A. Contractor acknowledges and agrees that all PHI created, maintained, transmitted, received, or used by Contractor in relation to the Contract shall be subject to this BAA. This obligation to protect Plan Member privacy and to keep such PHI confidential survives the termination, cancellation, expiration, or other conclusion of the BAA as set forth below.
- B. Contractor agrees it is aware of and will comply with all provisions of HIPAA that are directly applicable to Business Associates.
- C. Contractor shall use or disclose any PHI solely as would be permitted by HIPAA if such use or disclosure were made by Covered Entity: (1) for meeting its obligations as set forth in the Contract, or any other agreements between the Parties evidencing their business relationship; or (2) as required

by applicable law, rule or regulation, or by accrediting or credentialing organization to whom Covered Entity is required to disclose such information or as otherwise permitted under this Agreement, the Contract (if consistent with this Agreement and HIPAA), or HIPAA. All such uses and disclosures shall be subject to the limits set forth in 45 CFR § 164.514 regarding limited data sets and 45 CFR § 164.502(b) regarding the minimum necessary requirements.

- D. Contractor shall develop, document, implement, maintain, and use appropriate administrative, physical, and technical safeguards to prevent unauthorized use or disclosure of PHI, and to protect the integrity, availability, and confidentiality of that PHI. The safeguards that Contractor implements shall meet the requirements set forth by the United States Department of Health and Human Services including, but not limited to, any requirements set forth in HIPAA and North Carolina state law as applicable.
- E. Contractor shall implement security policies and procedures, and provide the Plan's HIPAA Privacy Officer ("HPO") with a copy of such.
- F. Contractor agrees that if it enters into an agreement with any agent or Subcontractor, under which PHI could or would be disclosed or made available to the agent or Subcontractor, Contractor shall have an appropriate BAA that conforms to applicable law, and is consistent with this Agreement. The terms of a BAA that Contractor enters into with its agent or Subcontractor shall meet or exceed the protections of this BAA. The BAA shall be in place with the agent or Subcontractor before any PHI is disclosed or otherwise made available to the agent or Subcontractor.
- G. Contractor shall disclose to the Plan a list of any and all agents or Subcontractors who will have access to or use of PHI on behalf of the Contractor for the benefit of the Plan. These disclosures shall be made prior to or upon signing this BAA. Any subsequent changes or additions to this list must be approved in writing by the Plan prior to any new agent or Subcontractor being provided access to PHI on behalf of the Plan.
- H. If Contractor provides PHI created, maintained, transmitted, or received by the Plan to any agent or Subcontractor, the agent or Subcontractor shall agree that with respect to such information, the same or greater restrictions and conditions that apply through this BAA to Contractor shall also apply to the agent or Subcontractor.
- I. Contractor shall obtain and document "satisfactory assurances" of any agent or Subcontractor to whom it provides PHI on behalf of the Plan through a written contract or other agreement with Contractor that meets the requirements of 45 C.F.R. §164.504(e).
- J. Contractor agrees that if and to the extent it conducts in whole or part Standard Transactions on behalf of the Plan, Contractor shall comply, and shall require any and all agents or Subcontractors involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Parts 160 and 162 and the HITECH Act as if they were the Plan. Contractor shall not enter into (or permit its agents or Subcontractors to enter into) any trading partner contracts in connection with the conduct of Standard Transactions for or on behalf of the Plan that:
 - 1. Changes the definition, data condition, or use of data element or segment in Standard Transaction;
 - 2. Adds any data element or segment to the maximum defined data set;
 - 3. Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification;
or
 - 4. Changes the meaning or intent of the Standard Transaction's implementation specification.
- K. If Contractor receives a request for access to inspect or obtain a copy of PHI in a designated record set from a Member or representative of the Member, Contractor shall alert the Plan of such request

within three business days. At the request of the Plan and in a reasonable time and manner, Contractor shall provide access to PHI in a Designated Record Set (to the extent Contractor maintains PHI in a Designated Record Set) to the Plan, or (as directed by the Plan) to an individual or an individual's personal representative, for inspection and copy in order to meet obligations under 45 C.F.R. § 164.524. This paragraph applies only to that PHI that is in Contractor's care, custody, or control.

- L. At the request of the Plan or an individual or that individual's Personal Representative and in the time and manner requested, Contractor shall make any amendment(s) to PHI in a Designated Record Set (to the extent Contractor maintains PHI in a Designated Record Set) that the Plan directs or agrees to pursuant to 45 C.F.R. § 164.526. This paragraph applies only to the PHI that is in Contractor's care, custody, or control.
- M. Contractor agrees that the Plan shall have the right to audit its policies, procedures, and practices related to the use and disclosure of the Plan's PHI.
- N. Contractor shall provide the Plan with copies of all policies, procedures, and practices related to the use and disclosure of Plan PHI prior to or upon execution of this BAA.

III. BREACH NOTIFICATION REQUIREMENTS

- A. Upon discovery by Contractor of a suspected or actual Breach of Unsecured PHI, Contractor must notify the Plan's HPO, in writing, within three business days. For purposes of this section, "discovery" means having obtained knowledge in any manner from any source and in any form, including from an agent or Subcontractor. This notice does not need to be a final report, but must inform the Plan's HPO of an approximate number of individuals affected by the Breach, whether there is an ongoing risk of improper disclosure, and what steps are being taken to mitigate the Breach and/or ongoing risk of disclosure. See "Attachment A" for the Plan's HPO's contact information.
- B. Contractor is not required to report Unsuccessful Security Incidents. For purposes of this BAA, Unsuccessful Security Incidents is defined as pings and other broadcast attacks on Contractor's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, use, or disclosure of PHI.
- C. Upon discovery of a Breach, Contractor shall conduct any risk assessment necessary to determine whether notification is required and will maintain any related records in accordance with Contractor's internal policies and procedures and the applicable provisions of the Breach Notification Rule as interpreted by Contractor. The risk assessment must consider the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated. The risk assessment must be thorough, conducted in good faith, and reach a reasonable conclusion. Contractor shall provide the Plan with a final signed copy of the risk assessment or report within three business days of its completion, no later than ten business days after discovery (unless otherwise agreed to by the Plan's HPO).
- D. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI by Contractor in violation of the requirements of this BAA or HIPAA.
- E. Contractor shall submit a formal report to the Plan's HPO without unreasonable delay, but no later than ten business days after discovery. The formal report shall include, to the extent possible, the following:
 - 1. A brief description of what happened (identify the nature of the non-permitted use or disclosure), including the date of the Breach, the date of the discovery of the Breach, and the date the Breach was reported to the Contractor's Privacy Official;

2. A description of the nature of the Unsecured PHI that was involved in the Breach (e.g., Member's full name, Social Security number, date of birth, home address, account number, etc.);
 3. Identify who made the non-permitted use or disclosure;
 4. Identify the recipient(s) of the non-permitted use or disclosure;
 5. A description of what Contractor did or is doing to investigate the Breach;
 6. A description of what Contractor did or will do to mitigate risks, harmful effects, and losses of the non-permitted use or disclosure;
 7. Identify what corrective action Contractor took or will take to prevent and protect against further Breaches;
 8. Identify the steps Members should take to protect themselves from potential harm resulting from the Breach;
 9. Contact procedures for Members to ask questions of or learn additional information from the Contractor, which shall include a toll-free telephone number, e-mail address, Web site, or postal address; and
 10. Provide such other information related to the Breach as the Plan may reasonably request.
- F. If Contractor determines that a Breach of Unsecured PHI has occurred, Contractor shall provide written notice, on behalf of the Plan, without unreasonable delay, but no later than thirty calendar days following the date the Breach of Unsecured PHI is or reasonably should have been discovered by Contractor, or such later date as is authorized under 45 C.F.R. §164.412, to:
11. each individual whose Unsecured PHI has been, or is reasonably believed by Contractor to have been, accessed, acquired, used, or disclosed as a result of the Breach; and
 12. the media, to the extent required under 45 C.F.R. §164.406.
- G. Contractor shall send notices to individuals using the last known address of the individual on file with Contractor, unless the individual has agreed to electronic notice as set forth in 45 C.F.R. §164.404. If the notice to any individual is returned as undeliverable, Contractor shall alert the Plan, and take such action as is required by the Breach Notification Rule.
- H. Contractor shall be responsible for the drafting, content, form, and method of delivery of each of the notices required to be provided by Contractor under this section. Contractor shall comply, in all respects, with 45 C.F.R. § 164.404 and any other applicable notification provisions of the Breach Notification Rule, including without limitation 45 C.F.R. Part 164 Subpart D, Section 13402 of the HITECH Act, and applicable state law, as interpreted by Contractor.
- I. Contractor notices must be reviewed and approved by the Plan's HPO before being sent to Plan Members, published to the media, or otherwise made public to any person or entity that is not a Party to this Agreement.
- J. Any notices required to be delivered by Contractor shall be at the expense of Contractor.
- K. Contractor shall provide to the Plan or an individual, in the reasonable time and manner requested by the HPO, information collected in accordance with Section III of this BAA, to permit the Plan to respond to a request by an individual or that individual's Personal Representative for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

- L. Contractor shall provide the Plan with an annual report of all suspected or actual Breaches of Unsecured PHI by Contractor, and by any agent or Subcontractor of Contractor within sixty days of January 1 of the year following the Breaches.

IV. ACCOUNTING FOR DISCLOSURES AND SALE OF DATA

- A. If applicable, Contractor shall comply with HITECH Act provisions regarding accounting for disclosures of PHI and Electronic Health Records (“EHR”).
- B. Contractor shall comply with the prohibition on the sale of PHI and EHR set forth in 42 U.S.C. § 17935(d).
- C. Contractor shall not sell PHI or any derivation thereof, including deidentified data, without the express written approval of the Plan.
- D. Contractor shall use and disclose PHI for Marketing purposes only as expressly directed by the Plan, and in accordance with 42 U.S.C. § 17936(a).
- E. Contractor agrees that the Plan shall review all Marketing materials given to, prepared, or assembled by Contractor prior to its disclosure in order to meet obligations under HITECH Act, Title XIII, Subtitle D, Section 13406, and 45 C.F.R. §§ 164.501, 164.508, and 164.514.

V. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

- A. Except as otherwise limited in this BAA, Contractor may use or disclose PHI on behalf of, or to provide services to, the Plan as described in RFP#270-20220830TPAS Third Party Administrative Services (“Contract”).
- B. Except as otherwise limited in this BAA, Contractor may use PHI for the proper management and administration of the Contract or to carry out the legal responsibilities of Contractor.
- C. Including all disclosures permitted or required by law, any use or disclosure of PHI or data derived from PHI (including De-Identified Data and Limited Data Sets) not related to the Contractor fulfilling its obligations to the Plan under the Contract will be reported to the Plan in writing within thirty days. Such notice shall include information about what data was used or disclosed, for what purpose the data was used or disclosed, the date(s) the data was used or disclosed, and any other information reasonably requested by the Plan.
- D. Except as otherwise limited in this BAA, Contractor may disclose PHI for the proper management and administration of the Contract, if disclosures are required by law; or if Contractor obtains reasonable assurances by means of a written agreement from the person or entity to whom the information is disclosed that it shall remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the entity. The person or entity must notify Contractor of any instances it is aware of that the confidentiality of the information has been Breached.
- E. To the extent provided for under the Contract, and except as otherwise limited in this BAA, Contractor may use PHI to provide Data Aggregation services to the Plan as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- F. Contractor may use PHI to report violations of law to appropriate federal and state authorities, as permitted by 45 C.F.R. § 164.502(j)(1).
- G. Contractor shall make internal practices, books, and records - including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created, maintained, transmitted, or received by Contractor on behalf of the Plan - available to the Plan, or to the Secretary, in a time and manner requested or designated by the Secretary or the Plan, for purposes of determining the Plan’s and Contractor’s compliance with HIPAA.

- H. If an individual or an individual's personal representative requests an accounting of disclosures of PHI (in accordance with 45 C.F.R. § 164.528), Contractor shall provide documentation of disclosures of PHI (and information related to such disclosures) in the same manner as would be required of the Plan. Contractor shall alert the Plan of any such request within ten business days of its receipt.
- I. Contractor shall limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request if performing any function or act on behalf of the Plan. 45 C.F.R. §164.502(b).
- J. Contractor shall be in compliance with the HIPAA minimum necessary provision (45 C.F.R. § 164.502) if it limits its uses, disclosures, or requests of PHI to a limited data set to the extent practicable or, if needed, to the minimum necessary to accomplish an intended purpose.
- K. The Minimum Necessary Standard does not apply to such uses, disclosures, and requests set forth in 45 C.F.R. § 164.502(b)(2).
- L. Contractor is prohibited from receiving direct or indirect remuneration (subject to certain enumerated exceptions) in exchange for any PHI of a Member, unless a valid authorization has been obtained from the Member in accordance with 45 C.F.R. § 164.508. A valid authorization includes, in accordance with such section, a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Member.

VI. OBLIGATIONS OF THE PLAN

- A. The Plan shall notify Contractor of any limitation(s) in the Plan's notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Contractor's use or disclosure of PHI.
- B. The Plan shall notify Contractor of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Contractor's use or disclosure of PHI.
- C. The Plan shall notify Contractor of any restriction to the use or disclosure of PHI that the Plan has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Contractor's use or disclosure of PHI.
- D. The Plan shall not request that Contractor use or disclose PHI in any manner that would be impermissible by the Plan under HIPAA.

VII. TRANSITION, RETENTION, AND DESTRUCTION OF RECORDS AND DATA

- A. **Transition of Records and Data:** Upon termination, cancellation, expiration, or other conclusion of the Contract, Contractor shall assist the Plan, upon written request, in transitioning all PHI to the Plan or other entity designated by the Plan in a format determined by the Plan.
- B. **Retention, Destruction, and Return of non-PHI Records and Data:** Contractor and its agents or Subcontractors shall retain all documentation (including documentation in electronic form) required under 45 C.F.R. § 164.530(j)(1) for six years from the date of its creation or the date when it last was in effect, whichever is later. 45 C.F.R. §164.530(j)(2).
- C. **Return or Destruction of PHI:** Within a reasonable time after termination, cancellation, expiration, or other conclusion of the Contract, Contractor and its agents or Subcontractors shall:
 - 1. Return to the Plan or destroy any and all PHI, in whatever form or medium (including any electronic medium under Contractor's and its agents' or Subcontractors' custody or control), that Contractor and its agents or Subcontractors created or received while carrying out a function on behalf of the Plan. Such return or destruction shall occur within a reasonable time period after the termination,

cancellation, expiration, or other conclusion of the Contract as agreed to by the Parties. If the Parties cannot mutually agree upon a reasonable time period for such return or destruction, Contractor and its agents or Subcontractors shall return or securely destroy all Plan PHI no later than 90 days after the termination, cancellation, expiration, or other conclusion of the Contract. The Plan will communicate such time period to Contractor in a Contract closeout letter.

- a) Guidelines for Destruction: Contractor and its agents or Subcontractors shall destroy PHI in accordance with the approved methods outlined by the National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, or the most current subsequent update.
- b) Certificate of Data Sanitization: No later than thirty days after all PHI has been destroyed, an authorized representative of Contractor and its agents or Subcontractors with knowledge of the data destruction shall complete, sign, and return to the Plan an attestation of destruction supplied by the Plan.. Contractor shall return the signed attestation by email to the Manager of Contracts and Compliance, or designee.

VIII. SECURITY OF PHI

- A. Contractor shall comply with the provisions of 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 relating to implementation of administrative, physical, and technical safeguards with respect to Electronic PHI in the same manner that such provisions apply to a HIPAA Covered/Hybrid Entity.
- B. Contractor shall obtain security-related written assurances from HIPAA covered Subcontractors by way of business associate agreements conforming to applicable law and consistent with the terms under this Agreement.
- C. Contractor shall implement and maintain policies and procedures for compliance with the Security Rule.
- D. Contractor shall follow all documentation and maintenance requirements under the Security Rule.
- E. Contractor shall also comply with any additional security requirements contained in the HITECH Act that are applicable to a HIPAA Covered/Hybrid Entity.

IX. SURVIVAL OF OBLIGATION TO PROTECT PHI

- A. If return or destruction of any PHI is not feasible after termination, cancellation, expiration, or other conclusion of the Contract, Contractor shall extend the protections of this BAA to the PHI retained, and limit its further use or disclosure of such PHI to those purposes that make return or destruction of that information infeasible.
- B. Contractor shall sign an attestation as to why the PHI cannot be returned or destroyed, and affirm in writing that the protections of this BAA will be indefinitely extended to the retained PHI.
- C. If destruction of the retained PHI occurs at any point after Contractor has stated that return or destruction of PHI is not feasible, Contractor shall provide the Plan with an attestation of destruction which will include the date(s) of destruction, method(s) of destruction, and the reason(s) for destruction.

[SIGNATURE PAGE FOLLOWS]

The Plan and Contractor have executed this Business Associate Agreement in two originals, one of which is retained by Contractor, and one by the Plan.

North Carolina Department of State Treasurer

By: Dale R. Folwell, CPA or Delegate

Signature: _____

Title: State Treasurer of North Carolina

Date: _____

North Carolina State Health Plan for Teachers and State Employees

By: Dee Jones

Signature: _____

Title: Executive Administrator

Date: _____

[INSERT NAME OF CONTRACTOR]

By: Scott Hogan

Signature: _____

Title: President and Chief Executive Officer

Date: _____

ATTACHMENT H: HIPAA QUESTIONNAIRE

As a covered entity, it is the responsibility of the North Carolina State Health Plan (Plan) to ensure its Members' health information is protected from use and disclosures not allowed under the Health Insurance Portability and Accountability Act (HIPAA), as well as applicable state and federal laws. The Plan takes this responsibility very seriously.

The purpose of this HIPAA Questionnaire is to allow the Plan to evaluate the HIPAA compliance of a prospective or current vendor who may request or require Member data containing protected health information (PHI). As a threshold to being considered to do business with the Plan, the Vendor must demonstrate that it meets the Plan's expectations for HIPAA compliance. The information provided below will be used by the Plan to determine the Vendor's level of understanding of HIPAA privacy and security rules, as well as its compliance status.

The Vendor is encouraged to thoroughly respond to all questions to the best of its ability and provide copies of all requested documentation. The Plan encourages the Vendor to have its privacy officer or other compliance specialist complete this questionnaire. Any incomplete responses may negatively impact the Plan's evaluation of the Vendor's HIPAA compliance, including a determination that the Vendor does not meet the Plan's expectations.

All responses must be typed. Handwritten responses will not be accepted.

If the Vendor maintains that any information contained in requested documentation is proprietary or otherwise confidential, the Vendor may redact these portions and supply the un-redacted portions for review.

Vendor Information:

Company name: UMR, Inc.

Address (city, state, and zip code): 115 W. Wausau Ave. Wausau, WI 54401-2875

Website URL: www.umar.com

Name of person completing form, and role: Jeff Giadone

Email address: jgiadone@uhc.com

Phone number: (714) 226-4108

Fax number: Not applicable

HIPAA compliance person's name, title, phone number, and email address, if different than person completing form:

Brian DuPerre

Chief Privacy Officer, Deputy General Counsel, Senior Vice President
UnitedHealthcare

(860) 702-7095

Brian_Duperre@uhc.com

Date you are completing this form: 9/14/2022

**** Please note that you must update the contact information provided in this questionnaire within 30 days of any change in personnel. ****

For all questions, if more detail is needed than the space provided allows for, please attach a separate page.

Compliance Questionnaire

- 1. Details of the individual responsible for HIPAA Compliance (if this designated position does not exist, provide the details of the employee who typically handles HIPAA privacy and security issues within your company or organization).**

Name: Brian DuPerre

Title: UnitedHealthcare Chief Privacy Officer, Deputy General Counsel, Senior Vice President

Address: 185 Asylum Street, Hartford CT 06103

Phone number: (860) 702-7095

E-mail address: Brian_Duperre@uhc.com

Certification designation (e.g., CHC, CISSP, CIPP, CHP, CHPSE, etc.): Certified Information Privacy Professional (CIPP)

Date certified: 10/19/2009

- 2. If they are not certified, provide detailed information regarding training that has been provided to the person responsible for HIPAA compliance (e.g., date last received training, name of company or person that provided training, etc.).** Not applicable.

Employee HIPAA Training

- 3. Which employees receive HIPAA training? How frequently is their training refreshed?**

All full-time and part-time new hires and applicable contractors are required to complete UnitedHealth Group's Information Security and Privacy training as part of the onboarding process and annually.

All UMR employees undergo initial and annual Health Insurance Portability and Accountability Act (HIPAA) training to ensure they understand the policies and procedures that support HIPAA compliance. The training covers a variety of topics, such as transmitting protected health information (PHI) safely and securely, by either electronic or paper-based means; appropriate conduct when discussing PHI with a co-worker or supervisor; protecting PHI at their workstations; and appropriate storage of PHI data. We also have extensive safeguards in place to protect our facilities and IT systems to ensure safe transfer and storage of PHI-related data.

- 4. Do all the above employees receive comprehensive training (i.e., training which covers the privacy and security of PHI; both physical and technical)?** Yes No

a. If no, provide details of the level of training made available to employees.

Not applicable.

- 5. When was HIPAA training last updated? When is the next planned update?**

We implement necessary actions for timely compliance with the American Recovery and Reinvestment Act (ARRA) provisions. To the extent that the law requires modifications to our current practices, policies, training or systems, we effectively adopt and implement revised practices, policies, training and systems to meet the various compliance effective dates outlined in the law and subsequent regulations. We also closely monitor Health and Human Services (HHS) Office for Civil Rights (OCR) on the ARRA for additional guidance from provisions and to make appropriate adjustments to our practices, policies, training and systems.

- 6. Are there internal HIPAA privacy policies and procedures in place which govern the privacy practices of the organization and its employees?** Yes No

- 7. Attach a copy of all internal/employee-facing privacy policies and procedures.**

Please refer to the document titled: UnitedHealth Group - Privacy – UHGPrivacyPolicyManual.

a. Note when the privacy policies were last reviewed or updated:

May 2022

- 8. **Are employees trained on the privacy policies and procedures? Yes X No**
- 9. **Are employees required to sign an agreement stating they have read and understand the privacy policies and procedures? Yes X No**
- 10. **Are there internal HIPAA security policies and procedures in place which govern the security practices of the organization and its employees? Yes X No**
- 11. **Attach a copy of all internal/employee-facing security policies and procedures.**

Please refer to the documents titled:

- UnitedHealth Group - Policies - Information Security - Enterprise Information Security Policy
- UnitedHealth Group - Policies - Information Security - 1A Security Program Management

a. Note when the security policies were last reviewed or updated:

These documents were updated on 1/5/2022 and 7/31/2022, respectively.

- 12. **Are employees trained on the security policies and procedures? Yes X No**
- 13. **Are employees required to sign an agreement stating they have read and understand the security policies and procedures? Yes X No**
- 14. **Can you provide documentation that all employees have completed training? Yes X No**
- 15. **Has your organization received any certifications regarding HIPAA compliance? (If yes, please provide copies of the certification and the date when the certification was awarded.)**

Our last Health Information Trust Alliance (HITRUST) certification was April 30, 2021 and is valid for two years. Please refer to the documents titled:

- Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
- Optum_2021-_HITRUST_Interim_Letter
- UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

- 16. **When was the last time your company was audited to determine HIPAA compliance? Provide date the audit was performed and the name of the company who performed it. Provide copies of the audit findings.**

We have a continuous/revolving HIPAA audit model. Our Enterprise Information Security staff is continuously making HIPAA security assessments. HITRUST is annual, and we have over 70 SOC audits each year. Internal audit has various areas tested each year, Deloitte does baselines as a part of their certification of our financials, and we do regular HIPAA program maturity assessments. CMS and the Departments of Insurance (and some self-insured customers) test various elements regularly, and for special purposes, we engage Price Waterhouse Coopers (PWC) and others to conduct reviews.

The results of most assessments are confidential to UnitedHealth Group and are not typically shared outside the company.

Our last HITRUST certification was April 30, 2021 and is valid for two years. Please refer to the documents titled:

- Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
- Optum_2021-_HITRUST_Interim_Letter
- UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

Data Security

17. Provide details of the methods the company employs to secure and render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

At all times, employees are required to apply the Minimum Necessary rule when using, sending, or sharing PHI to perform business functions. UnitedHealth Group requires business associates to appropriately safeguard individually identifiable health information and have established HIPAA compliant contractual agreements with our trading partners and other business associates.

The Minimum Necessary rule applies when sending or sharing PHI internally within our organization and externally with customers and their trading partners. We limit the disclosure of PHI to that which is permitted or required by law and is necessary to administer our business, provide quality service, and meet regulatory requirements. UnitedHealth Group's offshore vendors use the same systems as domestic sites and have access to the same information. UnitedHealth Group employs a number of access control features to secure systems and information including:

- User authentication by ID and password
- User access on a need-to-know basis
- Prescribed network and application-level security.

These safeguards are reviewed on a regularly scheduled basis by our internal auditors, as well as, independent auditors. Managers are responsible for determining access levels required for the end-user to perform his/her job function. Inactive/terminated users are purged. Platform level access is revoked immediately if a user is terminated for cause or on the last day of employment. Policies and standards require that user IDs, date/time for logoff, successful/unsuccessful system, data, and resource access attempts are logged and retained.

CONFIDENTIALITY OF INFORMATION

With respect to confidentiality, UnitedHealth Group employs the same standards used in our onshore sites to govern our offshore sites (both UnitedHealth Group sites and those of third-party vendors). UnitedHealth Group's training, quality, and management personnel are a frequent on-site presence at global locations to ensure that operations meet our standards for security and decorum. Offshore personnel receive the same training provided to our domestic employees. The curriculum includes a detailed unit on confidentiality, security, and privacy concerns. Additionally, in compliance with HIPAA regulations, the following training is provided based on job type to all offshore staff:

- HIPAA overview
- HIPAA protected health Information (PHI) course
- HIPAA privacy individual rights process
- HIPAA privacy clarifying scenarios
- Handling HIPAA calls in Intelligent Desktop (IDT)
- Review of confidentiality job aid

BACKGROUND CHECKS AND EMPLOYEE SCREENING

Just as in UnitedHealth Group's domestic hiring process, all offshore resources, whether UnitedHealth Group employees or third-party vendors must undergo background screenings prior to receiving an offer of employment.

OTHER SECURITY CONTROLS

UnitedHealth Group's security controls are designed to satisfy best business practices and regulatory and business requirements to ensure protection of information and business process efficiencies. These security controls include:

- Firewall management
- Intrusion detection
- Vulnerability assessments
- Policy and standard definitions and refinements
- Encryption
- Security administration management tools

Ongoing audits initiated internally or by customers and/or regulatory agencies provide the checks and balances to identify gaps and plan for remediation.

18. Describe security procedures – physical, technical, and administrative – in place to ensure the confidentiality of PHI internally, and when transmitting data externally to the Plan or to Plan vendors.

Optum complies with all applicable HIPAA rules, including the current applicable HIPAA privacy requirements. We implement appropriate and reasonable controls to protect the privacy and security of confidential and sensitive information, including PHI and ePHI. In addition, Optum continues to follow all applicable federal and state laws that affect the confidentiality of consumer information. We continually assess and enhance our HIPAA privacy and security program to the controls and safeguards as necessary. For additional details please refer to the document titled: UnitedHealth Group - Policies - Information Security - 13A Data Classification and Protection.

TRANSMITTING DATA EXTERNALLY

UnitedHealth Group's Information Security Policies and Standards require that standard encryption solutions and protocols be employed in the external transmission of confidential and proprietary information. This includes but is not limited to:

- SSH
- SFTP (FTP over SSH)
- HTTPS (HTTP over SSL)

Information Security Policies, standards, procedures, technical protocol, and operation protocols ensure the control of secured information transmissions. Selected encryption algorithms used to protect data must be industry tested and peer-reviewed according to best practice standards (i.e. Advanced Encryption Standard (AES)-256). This provides verification of strength against known attacks along with validation of sufficient key length and random key distribution to minimize brute force attack and mathematical analysis of keys.

In addition, UnitedHealth Group encryption technology standards require a minimum key length of 256-bits for secret (symmetric) encryption and 2048-bits for public/private (asymmetric) encryption. These are the minimum standards. Longer key lengths may have been implemented within specific environments, based on risk. Secure hash algorithms are used to create a message digest with a minimum length of 256 bits.

19. Do you have procedures to identify and respond to suspected or known security incidents; mitigate (to the extent possible) harmful effects of known security incidents; and document incidents and their outcomes? Please describe.

Yes. UnitedHealth Group's Security Incident Response Team provides oversight in the handling of security and privacy related incidents across the enterprise. Forensic investigation and preservation of evidence are included as part of this team's responsibilities. Each UnitedHealth Group business segment Information Security Officer and Privacy Officer serves as members of the Security Incident Response Team.

The Security Incident Response Team has the following responsibilities:

- Coordinating incident detection, analysis, containment, mitigation, recovery, and final reporting efforts to assure timely resolution of all security and privacy incidents upon identification.
- Coordinating any/all notification to required entities as an outcome of a security/privacy related incident.
- Participating in the activities and decisions across cross-functional workgroups in developing the security/privacy incident response requirements, conducting gap-analysis, recommending compliance action plans, reporting, tracking security and privacy incident trends, and providing process improvement recommendations.

Please refer to the document titled: UnitedHealth Group - Incident Response - Incident Response Process Overview - Customer Copy.pdf

20. Has the company conducted a risk assessment and gap analysis to address any findings?

Yes No

If yes: Date: Performed by:

The company's IT environment is audited by various internal and external entities. UnitedHealth Group contracts with various third party vendors to perform assessments on behalf of management of its internal IT controls via ICFR (Internal Controls over Financial Reporting) and SSAE (Statement on Standards for Attestation Engagements) audits. These audits are inclusive of platform and application controls and are performed continuously to ensure operating effectiveness throughout each year.

UnitedHealth Group's businesses self-assess their control environment (both IT and operational controls, where applicable) via Internal Audits and HITRUST assessments, which are spread throughout each year. Various regulatory agencies, as well as, UnitedHealth Group customers perform audits of UnitedHealth Group throughout each year, which include a review of key IT and operational controls.

The results of most assessments are confidential to UnitedHealth Group and are not typically shared outside the company, with the exception of, but not limited to SSAE SOC 1 Type 2 reports, where allowed and penetration test result summaries. SSAE SOC 1 Type 2 is the audit standard under which our independent auditor issues our SSAE SOC 1 Type 2.

21. Can you provide a copy of a SOC2, Type 2 security assessment report or a report performed under another security framework that can be cross-walked to the appropriate NIST-800-53 security control requirements (e.g., ISO 27001, HITRUST) for each service component used/involved in the proposed services? Yes (please attach) No

Please refer to the documents titled:

- Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
- Optum_2021-_HITRUST_Interim_Letter
- UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

a. How often does the company conduct these types of audits?

HITRUST certification is issued by HITRUST – an independent organization, and is valid for a two-year period with annual validations for ongoing compliance. We maintain several HITRUST certifications to cover different in-scope systems/environment.

22. Provide the number of HIPAA violations reported to the Office of Civil Rights (OCR) in the last five years, the details of the violation, and include the amount of the fine incurred (if any).

We have not responded to any HIPAA complaints from the Office of Civil Rights that would make us unable to perform services described in this proposal.

For confidentiality reasons we are unable to disclose detailed information. We understand the sensitivity and seriousness of a privacy or security incident, regardless of the cause. We also recognize that not all

reported incidents are actual incidents and that not all actual incidents are the result of an inappropriate or malicious intent. Our commitment is to make sure that we appropriately manage and thoroughly investigate all reported incidents.

23. Does the company have in place procedures for the destruction of PHI compliant with the standards set forth in NIST Special Publication 800-88 Revision 1 (or most recent update) located at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>? Yes X No

a. If yes, please describe the procedure for that destruction.

UnitedHealth Group’s media destruction policy and control standards align with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization or U.S Department of Defense (DoD) manual 5220.22:

- Overwrite all addressable locations with a seven pass process
- Verify and document that the overwrite has been performed
- Physically destroy media which cannot be properly overwritten

Domestically, all vendors and third parties that UnitedHealth Group utilizes for destruction services are either National Association for Information Destruction (NAID) certified or certify that their operational process exceeds requirements of NAID certification. In addition, vendors are screened and evaluated for strict compliance to our security requirements. Vendors are required to attest that all Electronic media and/or Memory are sanitized or destroyed according to their process.

UnitedHealth group has the right to review a vendor’s sanitization/destruction of electronic media/memory process at any time. Upon request by UnitedHealth Group, the vendor is required to provide evidence of design and effectiveness for their sanitization/destruction of electronic media/memory processes.

From a media perspective the following occurs:

- Hard drives:
 - All hard drives are subject to the seven pass DoD wipe
 - If the hard drives will not be re-used after complete sanitization they are shredded onsite as witnessed by an employee
 - Serial numbers of hard drives are documented and retained as a destruction record
- Tape media:
 - Tapes are not reused
 - Tapes are degaussed and shredded
 - The tape management system is updated to reflect status and a destruction record retained
- Removable media:
 - Utilization is by exception only via a formal process
 - All media is shredded when no longer required

Subcontractor Information

24. Do you outsource work to Subcontractors who would have access to Plan data and PHI and who may qualify as Business Associates as defined by HIPAA? Provide the names of the companies, contact information, and details of what they are contracted to do.

Yes. We provide most of our core services directly through the UnitedHealth Group family of companies. This enables us to offer affordable solutions through integrated data elements and systems, streamlined implementations and unified account management support. While most services are performed in-house or through sister companies, there are times we partner with external vendors for certain services. In these cases, we will remain fully responsible for these services and for the performance of these vendors or subcontractors. We hold our vendors and subcontractors to the same standards and requirements that we accept under our agreement with The Plan.

Below is a partial list of subcontractors. Because of the broad spectrum of UnitedHealth Group businesses and vendor relationships, we are unable to provide a complete list of proposed vendors/subcontractors and/or the level of detail you are requesting. Where vendors/subcontractors are required to support a customer relationship, we would typically select the vendors/subcontractors based upon the customer's specific requirements.

REDACTED

25. Have you entered into Business Associate Agreements (BAAs) with all Subcontractors who may qualify as Business Associates to your company or the Plan for this work? If yes, provide copies of the executed BAA(s).

Yes. We include a business associate agreement (BAA) in our Master agreement with suppliers. The Enterprise Supplier Risk & Performance Management Program provides the structure and framework to consistently identify, document and mitigate third-party supplier risks and to enforce contractual obligations and performance standards.



While we can identify the names of subcontractors, the actual subcontractor arrangements are considered proprietary. UMR will be responsible for services performed by our affiliates or subcontractors to the same extent that we would have been had the services been performed by us.

While the contracts signed between UMR and our subcontractors are considered proprietary and are not available for proposal purposes, upon award of business, The Plan will be permitted to conduct an on-site, closed door, white-room review of the contracts, at our office. UMR will schedule the appropriate visit upon request.

In addition, the UnitedHealth Group external facing website, <https://www.unitedhealthgroup.com/suppliers>, contains publicly available information related our organization's expectations and requirements for suppliers.

26. How do you enforce and monitor HIPAA policies with Subcontractors and Business Associates? What penalties or fixes are in place for violations?

Prior to selecting subcontractors, UMR completes a thorough review of qualifications. In order to contract with us, vendors must agree to and meet specific service-level expectations for quality, security, accuracy and pricing. We conduct both physical and electronic security checks of the vendors' facilities to ensure compliance with HIPAA regulations as well as our own security standards. Additionally, our standard contract requires vendors to file a business continuity plan to demonstrate how they would continue operating should a disastrous event occur.

UNITEDHEALTH GROUP ENTERPRISE INFORMATION SECURITY ASSESSMENT

UnitedHealth Group requires that effective information security controls be in place for External Parties. External Parties are defined as contractors, vendors, suppliers, business venture parties, auditors or assessors, cloud service providers, research agreements, government entities, or others who are involved in this Scope of Services.

External Parties must be assessed by Enterprise Information Security (EIS) prior to initiating any Scope of Services. EIS will utilize a risk and location-based approach to determine the level of information security assessment required. External Parties must demonstrate sufficient information security controls based on the Scope of Services, risks, locations, and relevant factors.

EIS may directly assess an External Party, and/or may accept the certification(s) achieved by External Parties to satisfy this requirement. The following are some of the certifications or third party assessments that will be considered:

- HITRUST certification
- International Standards Organization (ISO)-27001
- Service Control Organization 2 (SOC2) Type 2 mapped to HITRUST
- Third party or certification standard as contractually required

Certifications must be maintained for the duration of the relationship with the UnitedHealth Group. Remediation activities required by EIS or required to maintain the accepted certification must be implemented by the External Party within the timeframes prescribed.

External parties must acknowledge their responsibility for safeguarding the UnitedHealth Group's information technology (IT) systems and information assets via a formally written and legally binding agreement. Such agreements must follow applicable UnitedHealth Group policies, including Enterprise Sourcing & Procurement and Delegation of Authority policies. UnitedHealth Group maintains a standardized Security Exhibit template when Protected Information is in scope for the business engagement. Any negotiated modifications to the Security Exhibit must be approved by the UnitedHealth Group's Corporate Legal Department and Enterprise Information Security (EIS).

Where applicable, a Business Associate Agreement (BAA) is also required when a Business Associate (BA) of any of UnitedHealth Group's covered entities will create, receive, maintain, or transmit electronic Protected Health Information (ePHI) for or on behalf of UnitedHealth Group.

If the BA requires connectivity to the UnitedHealth Group information technology (IT) systems, information assets, or information entrusted to

UnitedHealth Group, modifications to the BAA must also be approved by the Enterprise Information Security (EIS) Organization.

Additional agreements other than a BAA may be required depending on business or legal requirements.

Please refer to the document titled: **UnitedHealth Group - Policies - Information Security - 10A External Party Security**

27. Have you conducted an audit of any Subcontractors or Business Associates? Can you provide information as to whether they are HIPAA compliant at this time? Include all available SOC2, Type 2 or substitute reports for Subcontractors and Business Associates.

UMR and UnitedHealth Group conduct both physical and electronic security checks of the vendors' facilities to ensure compliance with HIPAA regulations as well as our own security standards. UnitedHealth Group supports HITRUST, an expansion of the health care industry's use of the Common Security Framework (CSF) Assurance Program. In support of that objective we require third-party suppliers with access to our information systems and/or customer or health plan member data to adhere to the requirements listed in HITRUST to ensure proper security controls.

Please refer to the document titled: **UMR Claim Administration Processing System_CPS 2021 SOC 1 Type 2 Report**

Emergency/Contingency Plans

28. Describe the company's disaster recovery plan for data backup, data recovery, and system testing should a disaster occur (e.g., flood, fire, or system failure).

UnitedHealth Group developed an Enterprise Resiliency & Response Program that minimizes customer impact from disrupted service in a significant event or disaster, while aiding compliance to published regulatory guidelines. As a UnitedHealth Group company, UMR has plans to address all natural and human-caused disasters (i.e. hurricanes, floods, fires, terrorism, and pandemics).

The business continuity plans focus on critical business functions and planning for the worst-case scenario so that we can react quickly and efficiently, adding value to our business and customers through effective risk reduction, compliance with industry, contractual or regulatory standards, and safeguarding of operations and assets.

UnitedHealth Group's business impact analysis and subsequent business continuity plans are written to accommodate the following four scenarios:

- **Loss of Facility:** Complete interruption of facilities without access to its equipment, local data, and content. The interruption may impact a single site or multiple sites in a geographic region. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.
- **Loss of Critical People:** Complete interruption with 100% loss of personnel within the first 24 hours and 50% loss of personnel long-term. The interruption may impact a single site or multiple sites in a geographic area. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.
- **Loss of Critical Systems:** Complete interruption and/or access of critical systems and data located at the various UnitedHealth Group data centers for an extended period of time. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.
- **Loss of Critical Vendor:** Complete interruption in a service or supply provided by a third-party vendor. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

The impact of the operational loss due to one, or all, of these scenarios is assessed as part of the original Business Impact Analysis and annually thereafter. The business continuity plans are updated

quarterly and exercised annually.

Business continuity plans are leveraged as needed to address all forms of emergencies, which may impact business operations including short and long-term events. Examples of short-term events include power outages and winter weather office closings. These plans also address more severe, long-term situations, such as building fires and major hurricanes.

Business functions classified as critical generally provide for near immediate failover of core services by leveraging geographically dispersed, redundant operations and maintaining a recovery time objective of 72 hours or less. The plans are written to respond to a disaster lasting a minimum of 90 days.

In the event a disaster impacts our members, we will comply with any and all emergency orders mandated by the state Department of Insurance, Centers for Medicare and Medicaid Services (CMS), or Health and Human Services (HHS). The Event Management Team continually monitors for natural disasters and the potential impact on healthcare delivery services. If the situation warrants it, emergency provisions may be provided, even if not mandated.

An overview document is available, which describes the governance, strategy, and controls for the entire program. This document is not intended to replace the business continuity or disaster recovery plan review, but does provide the reassurance that UnitedHealth Group has a well-defined program in place to make sure customer impact is minimized during a disaster. Please refer to the document titled: **UnitedHealth Group - BCP-DR - Enterprise Resiliency and Response Customer Response Document.pdf**.

a. Provide the details of any incident that that has required activating the disaster recovery plan within the last two years, and any changes to the plan that were made as a result.

To maintain the confidentiality of our member and employee information, as well as, the integrity of our business operations, UnitedHealth Group considers this information proprietary and confidential.

Additionally, a post-event assessment is performed after any situation, which results in activation of the business continuity plans. This assessment is performed to learn from the experience and enhance business function preparedness and capabilities to respond and recover more effectively and efficiently. The results of our post-event assessments are also considered proprietary and confidential and are not provided to customers.

29. Describe the company's business continuity plan in the event of a disaster (e.g., flood, fire, power failure, system failure).

UnitedHealth Group developed an Enterprise Resiliency & Response Program that minimizes customer impact from disrupted service in a significant event or disaster, while aiding compliance to published regulatory guidelines. We have plans to address all natural and human-caused disasters (i.e. hurricanes, floods, fires, terrorism, and pandemics).

The business continuity plans focus on critical business functions and planning for the worst-case scenario so that we can react quickly and efficiently, adding value to our business and customers through effective risk reduction, compliance with industry, contractual or regulatory standards, and safeguarding of operations and assets.

UnitedHealth Group's business impact analysis and subsequent business continuity plans are written to accommodate the following four scenarios:

- **Loss of Facility:** Complete interruption of facilities without access to its equipment, local data, and content. The interruption may impact a single site or multiple sites in a geographic region. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.
- **Loss of Critical People:** Complete interruption with 100% loss of personnel within the first 24 hours and 50% loss of personnel long-term. The interruption may impact a single site or multiple sites in a geographic area. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical Systems:** Complete interruption and/or access of critical systems and data located at the various UnitedHealth Group data centers for an extended period of time. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.
- **Loss of Critical Vendor:** Complete interruption in a service or supply provided by a third-party vendor. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

The impact of the operational loss due to one, or all, of these scenarios is assessed as part of the original Business Impact Analysis and annually thereafter. The business continuity plans are updated quarterly and exercised annually.

Business continuity plans are leveraged as needed to address all forms of emergencies, which may impact business operations including short and long-term events. Examples of short-term events include power outages and winter weather office closings. These plans also address more severe, long-term situations, such as building fires and major hurricanes.

Business functions classified as critical generally provide for near immediate failover of core services by leveraging geographically dispersed, redundant operations and maintaining a recovery time objective of 72 hours or less. The plans are written to respond to a disaster lasting a minimum of 90 days.

In the event a disaster impacts our members, we will comply with any and all emergency orders mandated by the state Department of Insurance, CMS or HHS. The Event Management Team continually monitors for natural disasters and the potential impact on healthcare delivery services. If the situation warrants it, emergency provisions may be provided, even if not mandated.

An overview document is available, which describes the governance, strategy, and controls for the entire program. This document is not intended to replace the business continuity or disaster recovery plan review, but does provide the reassurance that UnitedHealth Group has a well-defined program in place to make sure customer impact is minimized during a disaster. Please refer to the document titled: **UnitedHealth Group - BCP-DR - Enterprise Resiliency and Response Customer Response Document.pdf.**

- a. **Provide the details of any incident that that has required activating the business continuity plan within the last two years.**

UnitedHealth Group has never needed to implement our disaster recovery plans in response to a catastrophic outage of technology at our production data centers.

To maintain the confidentiality of our member and employee information, as well as the integrity of our business operations, UnitedHealth Group considers this information proprietary and confidential.

I hereby certify that the information provided above and attached hereto is true and correct to the best of my knowledge and belief.

Scott Hogan
Name (Type)



Signature

09/16/2022
Date

ATTACHMENT I: NONDISCLOSURE AGREEMENT

By signing and returning this document, Vendor (*insert company name* UMR, Inc.),

understands and agrees to the following:


1. Upon the Plan's determination that Vendor has met the Minimum Requirements, Vendor will be provided access to Plan Data.
2. This Data is being provided for the sole purpose of assisting Vendor in preparing a responsive and responsible proposal to the TPA Services RFP (RFP#270-20220830TPAS) and is for the purpose of Plan Operations.
3. Vendor shall not use the Data for any purpose other than to assist in preparing a response to the TPA Services RFP and shall treat the Data as confidential.
4. Vendor shall not distribute or share the Data with any person or entity not assisting Vendor in preparing a response to the TPA Services RFP. Vendor shall hold any person or entity assisting in preparing the response to the TPA Services RFP to the same terms of this Nondisclosure Agreement as Vendor is held.
5. If Vendor does not bid on the TPA Services RFP, Vendor shall, upon making that decision, immediately destroy the Data from Vendor's files or records. Vendor shall not retain or maintain any copies of the Data.
6. If Vendor submits a proposal in response to the TPA Services RFP, Vendor shall immediately destroy the Data from Vendor's files or records upon notification that an award has been made or the TPA Services RFP has been cancelled.
7. Vendor shall destroy and dispose of Plan Data using the guidelines outlined in the National Institute of Standards of Technology (NIST) Special Publication 800-88 Revision 1 located at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>.
8. After all Data has been destroyed, an authorized representative of Vendor with knowledge of the Data destruction shall complete, sign, and return the Plan's Certificate of Data Sanitization within 30 days of the event giving rise to Vendor's obligation to destroy the Data. Vendor can obtain a copy of the certificate by e-mailing Chris Almborg at Chris.Almborg@nctreasurer.com with a copy to SHPCContracting@nctreasurer.com.
9. Provide the name, title, and email address of the individual designated to receive Data and Attachment A: Pricing. Do not respond with group/generic names and/or group/generic email addresses as these will not suffice.

Name: Garland Scott


Title: Health Plan Chief Executive Officer

Email: garland_g_scott@uhc.com
10. If during the procurement process it becomes necessary for Vendor to replace the individual previously identified in 9. above, Vendor shall immediately provide a signed and updated NDA that includes the replacement individual's name, title, and email address.

Vendor agrees to the above restrictions on the use of the Data:

BY: 
(Person authorized to bind Vendor)

ATTACHMENT J: MINIMUM REQUIREMENTS SUBMISSION INFORMATION

Vendor Name: UMR, Inc.		
Street Address: 115 W. Wausau Ave.		
City, State, Zip Code: Wausau, WI 54401-2845		
Telephone Number: (714) 226-4108		
AUTHORIZED REPRESENTATIVES TO BIND VENDOR:		
List individuals with authority to bind Vendor in connection with this Contract and future contractual documents.		
Name: Scott Hogan	Title: President and Chief Financial Officer	Email: jgiadone@uhc.com
Name: Garland Scott	Title: Health Plan Chief Executive Officer	Email: jgiadone@uhc.com
Name:	Title:	Email:
AUTHORIZED REPRESENTATIVE TO RESPOND TO QUESTIONS:		
List individual with the authority to answer questions and provide clarifications concerning Vendor's proposal.		
Name: Jeff Giadone	Title: Vice President, Public Sector California UnitedHealthcare	Email: jgiadone@uhc.com
Signature:		
By signing below: You hereby certify that you have the authority to sign on behalf of Vendor named above and acknowledge that if this Contract is awarded to your entity, the responses included in this Minimum Requirements Submission will become a binding portion of the Contract.		
Print name: Scott Hogan	Title: President and Chief Executive Officer	
Vendor's authorized signature: 	Date: 09/16/2022	

ATTACHMENT K: MINIMUM REQUIREMENTS RESPONSE

ATTACHMENT K: MINIMUM REQUIREMENTS RESPONSE is posted on the Ariba landing page and can be accessed at the following link: <http://discovery.ariba.com/rfx/13956411>.

Vendor shall complete ATTACHMENT K by only marking either "Confirm" or Does Not Confirm" as a response for each Minimum Requirement. Under no circumstances will narrative or text from Vendor be accepted as a response.

Confirmed.