



Table of Contents

Required Documents

- a.1 Attachment J: Minimum Requirements Submission Information
- a.2 Signed Copy of Addendum 1
- b.1 Third Party Administrative Services Minimum Requirements Proposal (RFP Section 5.1 TPA Minimum Requirements Table)
- b.2 Minimum Requirements Response Document
- c. Attachment K: Minimum Requirements Response
- d. Attachment C: North Carolina General Contract Terms and Conditions
- e. Attachment D: Location of Workers Utilized by Vendor
- f. Attachment E: Certification of Financial Condition
- g. Attachment G: Business Associate Agreement
- h. Attachment H: HIPAA Questionnaire
- i. Attachment I: Nondisclosure Agreement


Supplemental Items

- S-1 (HQ21 and MR 4) SOC 2 Cover Letter
- S-2 (HQ21 and MR 4) SOC Bridge Letter **REDACTED**
- S-3 (HQ 21 and MR 4) SOC 2 Report **REDACTED**
- S-4 (MR4) Cyber Liability Insurance Certificate
- S-5 (MR5) 2022 2nd Quarter 10Q Financial Report
- S-6 (MR5) 2022 1st Quarter 10Q Financial Report
- S-7 (MR5) 2021 10K Audited Financials
- S-8 (MR5) 2020 10K Audited Financials
- S-9 (HQ 7) Privacy Program Overview **REDACTED**
- S-10 (HQ 11 17 18 23) CVSH Control Standards **REDACTED**
- S-11 (HQ 16) Aetna-2022-HCB-HIPAA-Compliance-Report-20220906-Final **REDACTED**
- S-12 (HQ 25) Subcontractor Business Associate Agreements **REDACTED**

Note: HQ = HIPAA Questionnaire, MR= Minimum Requirements Response Document

Items that have been redacted are noted as “REDACTED”

ATTACHMENT J: MINIMUM REQUIREMENTS SUBMISSION INFORMATION

Vendor Name: Aetna Life Insurance Company		
Street Address: 5000 CentreGreen Way, Suite 350		
City, State, Zip Code: Cary, NC 27513		
Telephone Number: 800-872-3862		
AUTHORIZED REPRESENTATIVES TO BIND VENDOR:		
List individuals with authority to bind Vendor in connection with this Contract and future contractual documents.		
Name: James Bostian	Title: Market President	Email: BostianJ@aetna.com
Name: Nicholas Pypiak	Title: Executive Director, Underwriting	Email: PypiakN@aetna.com
Name: Tami Polsonetti	Title: Assistant Vice President	Email: PolsonettiT@aetna.com
AUTHORIZED REPRESENTATIVE TO RESPOND TO QUESTIONS:		
List individual with the authority to answer questions and provide clarifications concerning Vendor's proposal.		
Name: Catherine Aguirre cc: Craig Baker	Title: Executive Director cc: Proposal Consultant	Email: craguirre@aetna.com cc: bakerc5@aetna.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: Tami Polsonetti	Title: Assistant Vice President	
Vendor's authorized signature: 	Date: 9/20/22	

Date: September 16, 2022

RFP Number: 270-20220830TPAS

RFP Description: Third Party Administrative Services

Addendum Number: 1

Using Agency: The North Carolina State Health Plan for Teachers and State Employees

Purchaser: Vanessa Davison

Opening Date / Time: November 7, 2022 @ 10:00 a.m. ET

INSTRUCTIONS:

1. This Addendum is issued in response to questions submitted.
2. Section 3.4 b) Technical Requirements & Specifications is amended to correct the name of Section 5.2.5 from "Medical Management" to "Medical Management Programs;" and Maximum Points in Section 5.2.4 Product and Plan Design Management from 4 to 41; and is restated in its entirety below:

b) Technical Requirements & Specifications:

Scoring points for the Technical Proposal will be allocated as follows:

TECHNICAL AREAS	MAXIMUM POINTS
Section 5.2.1 Account Management	20
Section 5.2.2 Finance and Banking	19
Section 5.2.3 Network Management	28
Section 5.2.4 Product and Plan Design Management	41
Section 5.2.5 Medical Management Programs	18
Section 5.2.6 Enrollment, EDI, and Data Management	40
Section 5.2.7 Customer Experience	52
Section 5.2.8 Claims Processing and Appeals Management	16
Section 5.2.9 Claims Audit, Recovery, and Investigation	25
Section 5.2.10 Initial Implementation and Ongoing Testing	3
Section 5.2.11 Reporting	48
Total	310

The Vendors will be ranked in descending order based on the total points earned. The Vendor earning the least points out of the total 310 will receive the rank of one (1). The bids will fall in line according to total scored points, with the Vendor earning the most points out of the total 310 receiving the highest rank. Should two (2) Vendors earn the same score in the technical points, they will be given equal rank.

3. Section 5.1 Minimum Requirements, TPA Minimum Requirements Table is amended to remove Minimum Requirement #13 "Vendor shall submit two (2) completed and signed originals of Execution Page" in response to Vendor Questions #2 and #10. Minimum Requirement #14 "Vendor shall confirm it agreed to all performance guarantees as described in Section 6.3 and Schedules I and II." is renumbered as Minimum Requirement #13. The amended TPA Minimum Requirements Table is restated in its entirety below as the First Amended and Restated TPA Minimum Requirements Table.

Vendors shall duplicate the First Amended and Restated 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.

First Amended and Restated 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.	
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.	
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.	
4	a) Vendor shall certify without exception the sufficiency of its security standards, tools, technologies, and procedures in providing Services under this Contract. 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>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 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>	
5	<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</p>	

	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.	
6	Vendor shall confirm it agrees to ATTACHMENT C: NORTH CAROLINA GENERAL TERMS AND CONDITIONS without exception.	
7	Vendor shall complete and submit ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR.	
8	Vendor shall be financially stable; and complete, sign and submit without exception, ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION.	
9	Vendor shall complete, sign, and submit ATTACHMENT G: BUSINESS ASSOCIATE AGREEMENT.	
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.	
11	Vendor shall complete, sign, and submit ATTACHMENT I: NONDISCLOSURE AGREEMENT.	
12	Vendor shall complete, sign, and submit ATTACHMENT J: MINIMUM REQUIREMENTS SUBMISSION INFORMATION form.	
13	Vendor shall confirm it agreed to all performance guarantees as described in Section 6.3 and Schedules I and II.	

4. Requirement 5.2.11.2.x.2j) on page 72 is amended to change the report number from "Report 19: Utilization and Cost-Share by Service Type-Paid Claims." to "Report 18: Utilization and Cost-Share by Service Type-Paid Claims." The Technical Requirement 5.2.11.2.x.2) is restated in its entirety below:
 - 2) Monthly Performance Matrix reports as outlined in Exhibit 12, "Matrix Reports," and listed below:
 - a) Reports 1 and 2: Charge Summary Paid and Incurred Reports.
 - b) Reports 3 and 4: Charge Summary Trend Paid and Incurred.
 - c) Reports 5 and 6: Coinsurance and Deductible, Full Population-Paid and Incurred.
 - d) Reports 7 and 8: Coinsurance and Deductible, Closed Population-Paid and Incurred.
 - e) Reports 9 and 10: Copay-Incurred and Paid.
 - f) Report 11: Copay-Incurred (Claims Run out).
 - g) Reports 12 and 13: Claims Experience Summary by Demographics, Paid/Incurred, Time, etc.
 - h) Reports 14 and 15: Financial Summary-Paid and Incurred.
 - i) Reports 16 and 17: Financial Reconciliation-Paid and Incurred.
 - j) Report 18: Utilization and Cost-Share by Service Type-Paid Claims

5. Return two (2) properly executed originals of this Addendum Number 1 with your Minimum Requirements Proposal. Failure to sign and return this Addendum Number 1 may result in the rejection of your proposal.

Proposal Number: 270-20220830TPAS

Vendor: Aetna Life Insurance Company

Execute Addendum Number 1. RFP Number 270-20220830TPAS:

Vendor: Aetna Life Insurance Company

Authorized Signature: 

Name and Title (Print): Tami Polsonetti

Assistant Vice President

Date: 9/20/22

No.	Reference	Vendor Question	Answer
1.	Federal Tax ID Number, Page 2	Does the Federal Tax ID form need to be submitted with the Minimum Requirements Proposal, the Technical and Cost Proposal, or with both?	The Federal Tax ID form on page 2 of the RFP should be submitted with the Technical and Cost Proposal.
2.	Execution Form, pages 3-4	Can you confirm the Execution Pages do not need to be included with the Minimum Requirements response, but only with the Technical and Cost Proposal Response?	Confirmed. Vendor shall submit Execution Pages with its Technical and Cost Proposal. (See the First Amended and Restated TPA Minimum Requirements Table in Instruction #3 above.)
3.	1.1 Vision Overview (page 8)	What is the percentage of claims and percentage of dollars currently accessing the Clear Pricing (CPP) network vs. BCBSNC network?	Currently, 38.1% of the network claims are CPP. 18.6% of the allowed network cost is CPP.
4.	1.1 Vision Overview (page 8)	Please confirm within the Vision Statement (paragraph 2), that outlines the current and projected initiatives are part of the Minimum Requirements.	The Vision Statement is background information. The requirements are outlined in Sections 5.1 and 5.2.
5.	1.2 Overview of the State Health Plan (page 9)	Please confirm the Humana Group Medical Advantage PPO Base Plan - 143,197 enrollees and the Humana Group Medical Advantage PPO Enhanced Plan - 17,977 enrollees are not in scope for this request for proposal (RFP)?	State Health Plan Members enrolled in the Humana Group Medicare Advantage Plans are not in scope for this RFP.
6.	2.7.1, page 15	Can bidders restart page numbering with each separate requested document?	Yes, Vendors can determine if and how they number their submission. However, Vendors shall adhere to instructions in Section 2.7 (a)-(f).
7.	2.7.1, page 15	Can you confirm the copy we provide of Attachment C: North Carolina General Contract Terms and Conditions does not need to be physically signed?	Confirmed, Attachment C: North Carolina General Contract Terms and Conditions does not require a signature. Vendor shall insert its company name at the top of each page in the space provided.
8.	5.1 Minimum Requirements, TPA Minimum Requirements Table (page 34)	Please clarify instructions regarding listing the RFP Section Number and Page Number of Response column. Since page numbers within the RFP response/questionnaire will change with the final technical response. Does the page number requested refer to the page number in the RFP section or the response within the technical response?	Vendor shall provide the Section Number and Page Number of where the Plan can find the Vendor's response to the Minimum Requirement in the Vendor's Minimum Requirements proposal.
9.	5.1 Minimum Requirements, TPA Minimum Requirements Table (page 34)	Please clarify instructions regarding listing the RFP Section Number and Page Number of Response column. Can we provide responses within the RFP Section Number and Page Number of the Response column in lieu of referencing a the RFP Section Number and Page Number of Response?	Vendor shall provide a "Minimum Requirements" proposal that includes responses to each Minimum Requirement in the TPA Minimum Requirements Table. Vendor shall list the Section Number and Page Number in the TPA Minimum Requirements Table where the Plan

			can find the Vendor's response to the Minimum Requirements.
10.	5.1 Minimum Requirements, TPA Minimum Requirements Table; 2.7.2; Technical and Cost Proposal Contents, item a) (page 34)	Item 13 indicates "Vendor shall submit two (2) completed and signed originals of Execution Page." However, under Section 2.7.2 a), it indicates "Completed and signed version of Execution Pages along with the body of the RFP..." Should the Execution Page be returned with the Minimum Requirements or with the Technical and Cost Proposal that will follow, or both?	Vendor shall submit Execution Pages with its Technical and Cost Proposal. (See the First Amended and Restated TPA Minimum Requirements Table in Instruction #3 above.)
11.	Section 5.1, 4	Is the State willing to amend/negotiate this requirement?	No. Minimum Requirement #4 in Section 5.1 regarding data security is non-negotiable.
12.	Section 5.1, 5	Is the State willing to amend/negotiate this requirement?	No. Minimum Requirement #5 in Section 5.1 regarding financial stability is non-negotiable.
13.	Section 5.1, 6	Vendor agrees mutually acceptable terms and conditions to define the nature of the administrative services to be provided by Vendor is a necessity. Vendor has a standard Administrative Services Only (ASO) agreement which includes additional operational provisions that will need to be included in a contract with the State. Is the State agreeable to utilizing and/or incorporating the ASO agreement as part of the Contract between the State and Vendor?	Bidders must accept the Terms and Conditions as written. The Plan will not incorporate the Vendor's ASO agreement or any part of the Vendor's ASO agreement into this Contract.
14.	Section 5.1, 8	Is the State willing to amend this requirement? Recognizing, in an industry where lawsuits are a commonplace, we are mostly involved in lawsuits arising in the course of ordinary business. Please refer to Form 10-K and Form 10-Q for an updated description of material legal proceedings. These documents are available online: [Link removed by the Plan to maintain Vendor question anonymity.]	No, the Plan is not willing to amend Minimum Requirement #8 regarding Attachment E: Certification of Financial Condition.
15.	Section 5.1, 9	Vendor includes a standard business associate agreement (BAA) part of our Administrative Services Organization (ASO) agreement. Is the State agreeable to utilizing our standard BAA?	No, the Plan is not willing to utilize the Vendor's standard BAA.
16.	Section 5.1, 10	Is the State willing to amend this requirement? Recognizing some of the questions would require the State sign an NDA and some of the requests are proprietary and confidential and cannot be distributed externally.	No, the Plan is not willing to amend Minimum Requirement #10 regarding Attachment H: HIPAA Questionnaire.
17.	Section 5.1, 11	Is the State willing to accept redlines to this document?	No, the Plan is not willing to accept redlines to Minimum Requirement #11 regarding Attachment I: Nondisclosure Agreement.

18.	5.1 Minimum Requirements Table, 8,9,10,11,12	Are digital signatures acceptable on the execution pages, attachments and other signature-requiring forms?	Yes, digital signatures are acceptable and binding for all forms requiring signatures including the Execution Pages.
19.	5.1 Minimum Requirements Table, 13	Are there specific requirements for the original signatures? i.e. wet signature, blue ink	Vendors shall either provide wet signatures, preferably in blue ink or digital signatures.
20.	Section 5.1.1 Medicare primary members	Are you also reviewing fully insured Medicare Advantage plans as a part of this RFP?	No, the Plan is not reviewing fully insured Medicare Advantage Plans as part of this RFP. The awarded Vendor will, however, be responsible for Medicare primary Members that are not enrolled in the Plan's Group Medicare Advantage Plans.
21.	5.1.1.d	Vendor has a "firewall" between its TPA services operations and any other service operations, such as a PBM, consulting group, or any other services. Can the Plan please provide a definition of what you mean by "firewall".	Vendors may have multiple lines of business, including but not limited to TPA services, pharmacy benefit management services, Medicare Advantage Plans and/or consulting services. This RFP is for the TPA services outlined in the requirements; therefore, Vendors' other services should not have access to nor impact the services under this Contract. This requirement also applies to Vendors that may already have a Contract with the Plan for other services.
22.	5.1.2.a, page 37	In addition to claim recoveries, would any other types of transactions be made to the Depository Account?	The Plan does not anticipate other types of deposits, but often payments to the Plan are misdirected to the incorrect vendor and automatically deposited. In these instances, the Vendor notifies the Plan of the deposit so that it can be applied to the appropriate account.
23.	5.1.2.b, page 37	Is inline check processing an acceptable form of preprinted check stock?	The Plan is not familiar with inline check processing.
24.	5.1.3.c	Vendor will work with the Plan to develop and implement provider specific alternative payment arrangements. Please provide examples of alternative payment arrangements other than those currently in effect.	See Requirements 5.1.3.e., 5.1.3.g and 5.2.3.2.b.xii. for more examples of the types of alternative payment arrangements the Plan may be interested in pursuing.
25.	5.1.3.h., and 5.1.3.i	If the Plan implements a Medicare-based reimbursement model, Vendor will adjust any payment and/or medical policies required to better align with Medicare pricing guidelines If the Plan implements a Medicare-based reimbursement model, Vendor will administer any other Medicare medical and payment policies adopted by the Plan.	When administering a Medicare-based reimbursement model, it is sometimes necessary to align both medical and payment policies with Medicare in order to pay the claims. For example, for a provider to be reimbursed for durable medical equipment (DME) under Medicare

		<p>Please provide the Plan's definition of the following terms:</p> <ul style="list-style-type: none"> • Medical Policy • Payment Policies 	<p>they must be licensed and credentialed as a DME vendor. Licensing and credentialing may not be a requirement for DME under the Vendor's commercial business, but to administer the Medicare payment, it would be required. That is an example of a payment policy change. In that same scenario, the TPA may have DME medical policy that includes medical necessity that is not needed because of the payment policy. There will also be instances where a Medicare payment policy, for example, would require certain procedures to be performed only in an inpatient setting, while the Plan may not follow that requirement.</p>
26.	5.1.3.l	<p>Vendor will administer other reference-based pricing models, if requested by the Plan. Can the Plan please provide a definition of what you consider to be a reference-based pricing model?</p>	<p>A reference-based pricing model determines reimbursement based on the fee schedule reference. For example, reimbursing professional services at 160% of Medicare. Medicare doesn't have to be the reference, although is the most common.</p>
27.	5.1.3.j Page 38	<p>With regards to 5.1.3.j., how is the NC State Health Plan looking for carrier partners to work with Optum Insight? What data elements are needed to be provided between the two parties? What is the frequency of data to be transferred?</p>	<p>If the Plan decides to implement a Medicare based reference-based pricing reimbursement model, the Vendor will need a repricing partner to ensure all claims are paid at the appropriate percentage of Medicare. It is not required to be Optum Insight, but would need to be a reasonable replacement.</p>
28.	Section 5.1.4.a Benefit Administration	<p>Are there any other plan types that the vendor will administer? Eg. A fully insured Medicare Advantage plan?</p>	<p>Requirements for a self-funded Group Medicare Supplement Plan are outlined in Requirement 5.2.4.2.b.xi. While there are currently no plans to implement a Medicare Supplement Plan on January 1, 2025, this requirement may be exercised at sometime during the life of the Contract.</p>
29.	5.1.5.c	<p>Vendor will customize any of the Medical Management programs, if requested by the Plan. Can the Plan please provide a definition of what you consider to be "Medical Management programs"?</p>	<p>Medical Management includes programs the Vendor may have to address and manage Members' medical and behavioral health needs and when appropriate limit utilization. See Requirement 5.2.5.2.b.ii.</p>
30.	5.1.8.a	<p>Vendor will comply with all requirements set forth in Article 29B of Chapter 90 of the North Carolina General Statutes. As required, Vendor will validate provider enrollment in North Carolina's Health Information Exchange (NC HealthConnex) prior to paying Plan Member claims. If prohibited by the</p>	<p>The Plan is aware of challenges in operationalizing and supporting the requirements set forth in Article 29B of Chapter 90 of the General Statutes. The Plan continues to promote legislation to ensure, to the extent</p>

		<p>Statewide Health Information Exchange Act, Vendor must deny any claims received from providers that are not in compliance on the date of service. Will the Health Information Exchange provide a list of non-compliant providers?</p>	<p>possible, that an efficient and effective operational solution is created. However, the Plan does not have authority over the information to be provided by the Health Information Exchange.</p>
31.	5.2.3.2. vii and viii	<p>Will NC State Health plan be providing the contracts, rates, policies and procedures of their current Clear Pricing / Reference based pricing as a baseline for possible future arrangements with other carriers?</p>	<p>Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.</p>
32.	5.2.3.2 vii and viii	<p>Will the NC State Health Plan provide a listing of the current providers in their network and the Clear Pricing contracts with the participating providers</p>	<p>Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.</p>
33.	5.2.3.2 vii and viii	<ul style="list-style-type: none"> • Will the NC State Health Plan (NCSHP) provider contracts and rates transfer to Vendor for both designated Clear Pricing Project (CPP) and NCSHP? Can NCSHP provide Vendor a list of all CPP provider participants by service type (hospital, ancillary, physicians)? What percentage of the NCSHP network currently is designated as CPP? • Is it NCSHP expectation that Vendor will negotiate direct NCSHP agreements and renewals on behalf of NCSHP? • Is it assumed that all terms in CPP and NCSHP contracts, including policies, will also transfer? Will NCSHP provide Vendor all contract terms to review, including contract exceptions? If Vendor cannot administer and/or adjudicate specific terms in the contracts, will NCSHP agree to amend to allow Vendor policy and terms to be applied? • Is it NCSHP expectation that Vendor will "customize" any policy, program, contract arrangement, etc. (e.g. value-based ACOs, earned incentive programs) upon request from NCSHP? What is NCSHP expectation if Vendor cannot administer the request? • Are there any specific contract and network policies, provisions, network solutions, reimbursement terms, payment 	<p>Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.</p>

		methodologies, etc. that are consider absolute to NCSHP without flexibility?	
34.	5.2.5.2 Services	xi. Vendor will transition specific specialty pharmacy medication coverage to the Plan's PBM, if requested by the plan.	Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.
35.	5.2.5.2 Services	xii. Vendor will provide claims and analytical data to support the transition of specific specialty medications to the Plan's PBM.	Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.
36.	Attachment C, Page 96	#28. Performance Bond – please confirm if a bond will be required for this bid and if so, will it be required at the proposal submission or upon award notification?	Vendors are required to provide a performance bond. See Section 6.3.5 Third Party Administration Performance Guarantees Schedule I, that requires Vendor to provide proof of purchase of bond within 30 State Business Days of execution of Contract.
37.	Attachment D	Does the vendor currently have any work done outside the United States (US)? If applicable, please provide details of the type of work outside the US.	The subcontractors for the Plan's current TPA are not relevant to this Contract. However, the Plan would not support any Member-facing work being performed outside of the USA.
38.	Attachment I: Nondisclosure Agreement, item 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/SpecialPublication/NIST.SP.800-88r1.pdf . (page 115) Can you please define "Plan Data"?	All Plan enrollment and claims data is considered Plan data. If the Plan develops any custom networks or provider reimbursement models, this data may also be deemed Plan data.
39.	Attachment K Minimum Requirements Response - 5.1.3 Network Management Minimum Requirements (page 2)	Please confirm the intent of this section. Is it to confirm the vendors capabilities to perform and/or meet these requirements?	Vendor must agree and be able to support all the requirements in this section.
40.	Attachment K, page 117	Can you confirm that the Attachment K- Minimum Requirements Response Document that was posted to the Ariba site only needs to be returned in the Hard Copy/UBS submission once complete, and does not need to be reposted to the Ariba site?	Confirmed. Vendors shall submit Attachment K: Minimum Requirements Response in hard copy and on flash drives in accordance with Section 2.6.2 "Minimum Requirements Proposal Submission."

41.	Attachment K, Page 5	Please clarify if the Plan is looking to carve out specialty pharmacy.	The Plan is not looking to carve out specialty pharmacy. As noted in Requirement 5.2.5.2.a.i. the Plan expects the Vendor to handle specialty pharmacy and pass 100% of the rebates to the Plan. In Requirement 5.2.5.2.b.xi., the Plan addresses the possibility of transitioning specific specialty medications to the PBM.
42.	Attachment K	<ul style="list-style-type: none"> • 5.1.2.d – What is the average weekly claims funding amount for 2022 that the Plan has approved? Are there any requirements on how long it takes for the Plan to approve the disbursements? • 5.1.3.g – Does the Plan currently have Medicare-based reimbursement in place with their Vendor? If applicable, what services and providers are included? Does it apply to certain tiers and/or plans? • 5.1.3.l – Please describe the other possible reference-based pricing models the Vendor will need to consider? • 5.1.5.a – Does the Plan currently received 100% of the medical specialty pharmacy rebates? • 5.1.5.c – Does the Plan currently have a customized medical management program? If applicable, please describe in detail. • 5.1.6 – Does the Plan or the Vendor currently cover the cost of the data feeds? 	<p>1) Because of the transition to a new benefits administration system in 2022, the first quarter disbursements were not typical. The Plan generally disburses between \$50,000,000.00 - \$60,000,000.00 per week. Disbursement approval will be received by 4:00 p.m. ET on the day prior to disbursement.</p> <p>2) The Plan currently has Medicare base reimbursements in place for CPP providers. This applies to all services provided by these providers. The North Carolina State Health Plan Network is utilized for all three (3) plan designs.</p> <p>3) The Plan has not determined what other types of reference-based models may be utilized.</p> <p>4) The Plan currently receives 100% of the specialty pharmacy rebates.</p> <p>5) The Plan currently has a customized population health management program. Whether or not the program will be customized in the new Contract will depend on the Vendor's programs and the Plan's needs.</p> <p>6) The ongoing cost of vendor data feeds is included in the administrative fees of each Vendor's contract.</p>
43.	Attachment L	5.2.1.2.b – Does the Plan currently have dedicated resources from the Vendor? If applicable, please list their roles and responsibilities.	Questions pertaining to Section 5.2 "Technical Proposal Requirements and Specifications" and Attachment L "Technical Requirements Response" should be submitted by Vendors that pass the Minimum Requirements as set forth in Section 2.4 RFP Schedule.

Minimum Requirements Table

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.

First Amended and Restated 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.	Minimum Requirements Response Document-Page 1
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.	Minimum Requirements Response Document-Page 1
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.	Minimum Requirements Response Document-Page 2

Minimum Requirements Table

<p>4</p>	<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 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>Minimum Requirements Response Document- Page 4</p>
----------	---	--

Minimum Requirements Table

First Amended and Restated TPA MINIMUM REQUIREMENTS TABLE		
	Requirement	RFP Section Number and Page Number of Response
	<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>	
5	<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 financial statements and such other evidence of its own financial stability identified above.</p>	<p>Minimum Requirements Response Document-Page 5</p>

Minimum Requirements Table

First Amended and Restated TPA MINIMUM REQUIREMENTS TABLE		
	Requirement	RFP Section Number and Page Number of Response
6	Vendor shall confirm it agrees to ATTACHMENT C: NORTH CAROLINA GENERAL TERMS AND CONDITIONS without exception.	Minimum Requirements Response Document-Page 6
7	Vendor shall complete and submit ATTACHMENT D: LOCATION OF WORKERS UTILIZED BY VENDOR.	Minimum Requirements Response Document-Page 6
8	Vendor shall be financially stable; and complete, sign and submit without exception, ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION.	Minimum Requirements Response Document-Page 6
9	Vendor shall complete, sign, and submit ATTACHMENT G: BUSINESS ASSOCIATE AGREEMENT.	Minimum Requirements Response Document-Page 6
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.	Minimum Requirements Response Document-Page 7
11	Vendor shall complete, sign, and submit ATTACHMENT I: NONDISCLOSURE AGREEMENT.	Minimum Requirements Response Document-Page 7
12	Vendor shall complete, sign, and submit ATTACHMENT J:MINIMUM REQUIREMENTS SUBMISSION INFORMATION form.	Minimum Requirements Response Document-Page 7
13	Vendor shall confirm it agreed to all performance guarantees as described in Section 6.3 and Schedules I and II.	Minimum Requirements Response Document-Page 7

Minimum Requirements Response Document

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

Aetna is an industry leading, diversified health solutions company with more than 165 years of experience providing quality, reliable services to businesses, individuals and the government. Our services include medical, dental, vision, pharmacy, student health, voluntary, Medicare, Medicaid and other consumer-directed health benefits. We were founded in 1853 and acquired by CVS Health in 2018.

As CVS Health’s health care benefits business, we offer a broad range of traditional, voluntary and consumer-directed health insurance products and related services to help our members achieve their best health in an affordable, convenient and comprehensive manner. Combining the assets of our health insurance products and services with CVS Health’s unrivaled presence in local communities and their pharmacy benefits management capabilities, we’re joining members on their path to better health and transforming the health care landscape in new and exciting ways every day.

Our ultimate parent company of all Aetna affiliated companies is CVS Health Corporation, a publicly traded Delaware corporation.

- 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.
-

Operational and account management resources will be located at the following locations:

- 4050 Piedmont Parkway, High Point, NC 27265
 - 5000 CentreGreen Way, Suite 350, Cary, NC 27513
 - 151 Farmington Avenue, Hartford, CT
 - 261 N University Dr, Plantation, FL 33324
 - Home-based employees located throughout United States
-

State of North Carolina

Minimum Requirements Response Document

- 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.

Confirmed.

-
- 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.
-

State of Illinois

Contact Name: Chris Owsley
Division Manager, Benefits Management – Bureau of Benefits
801 South 7th Street, 2nd Floor
Springfield, IL 62703
Phone: (217) 558-1833
Cell: (217) 685-0993
Fax : (217) 524-1460
chris.owsley@illinois.gov

Minimum Requirements Response Document

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

Minimum Requirements Response Document

- 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.
- 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.

Confirmed.

Please also refer to our most recent SOC 2 Report, our SOC 2 Bridge Letter, and our Cyber Insurance Liability Certificate of Coverage under Tabs S-1, S-2, S-3, and S-4 in the Supplemental Items section of our response.

Minimum Requirements Response Document

- 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. We have included our two most recent audited financial statements and our two most recent quarterly financials under Tabs S-5, S-6, S-7, and S-8 in the Supplemental Items section of our response.

Minimum Requirements Response Document

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

Confirmed. We agree with Attachment C without exception and have included the completed attachment in the letter “d” tab.

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

Confirmed. We agree with Attachment D without exception and have included the completed attachment in the letter “e” tab.

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

Confirmed. We agree with Attachment E without exception and have included the completed attachment in the letter “f” tab.

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

Confirmed. We agree with Attachment G without exception and have included the completed attachment in the letter “g” tab.

Minimum Requirements Response Document

- 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. We have completed Attachment H and submitted it and have included the completed attachment in the letter "h" tab.

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

Confirmed. We agree with Attachment I without exception and have included the completed attachment in the letter "i" tab.

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

Confirmed. We agree with Attachment J without exception and have included the completed attachment in the letter "a" tab.

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

Confirmed. We agree in full to all performance guarantees in Section 6.3 and Schedules I and II.

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.

5.1.1 Account Management Minimum Requirements

- a. Vendor has one (1) or more current or former administrative services only (ASO) clients with more than 25,000 Medicare primary members.

Confirm Does Not Confirm

- b. Vendor will exercise loyalty and a duty of care to the Plan and its Members in performing its responsibilities under this Contract. Vendor must assume and exercise the same fiduciary responsibility established in N.C.G.S. § 135-48.2 for the State Treasurer, Executive Administrator, and the Board.

Confirm Does Not Confirm

- c. Vendor will provide subject matter experts, in addition to account management resources, to work directly with Plan and Plan vendor staff.

Confirm Does Not Confirm

- d. Vendor has a “firewall” between its TPA services operations and any other service operations, such as a PBM, consulting group, or any other services.

Confirm Does Not Confirm

5.1.2 Finance and Banking Minimum Requirements

- a. Vendor will comply with N.C.G.S. § 147-77 regarding the deposit of funds belonging to the Plan and confirm agreement that all receipts and other moneys belonging to the Plan that are collected or received by Vendor shall be deposited daily to the Plan’s bank account(s) as designated by the State Treasurer and reported daily to the Plan.

Confirm Does Not Confirm

b. Vendor will comply with the Plan’s requirements regarding the disbursement of funds on the Plan’s behalf which are outlined by the Department of State Treasurer’s website:

<https://www.nctreasurer.com/media/3791/open>

Confirm Does Not Confirm

c. If Vendor will be disbursing funds from the Plan’s bank accounts, Vendor must (1) print checks with the Plan’s logo and digitized signature with guidance on the layout from the Department of State Treasurer based upon a standard format; and (2) prepare checks and EFTs for claims and other disbursements to be drawn directly from the Plan’s bank account upon approval and release by the Plan. Vendor must be fully operational at least 30 days prior to January 1, 2025. If Vendor will not be disbursing funds from the Plan bank accounts, Vendor should respond N/A to this requirement.

Confirm Does Not Confirm N/A

d. Vendor will email weekly disbursement requests to the Plan by 9:30 a.m. ET on the first State Business Day of the week and hold disbursements until approved by the Plan.

Confirm Does Not Confirm

e. Vendor will support the State of North Carolina’s financial processing, banking, and reporting requirements which can be found at the following links or exhibits:

i. State banking: <https://www.nctreasurer.com/media/3791/open>

ii. Cash management:

<https://www.osc.nc.gov/state-agency-resources/statewide-cash-management>

iii. Escheats: <https://www.nccash.com/holder-information-and-reporting>

iv. High level daily deposits and disbursements of state funds workflows: Exhibit 1, “Deposits and Disbursement Process.”

Confirm Does Not Confirm

f. Vendor will provide a SOC1, Type II, and if applicable, a bridge letter, upon request by the Plan.

Confirm Does Not Confirm

5.1.3 Network Management Minimum Requirements

a. Vendor agrees the Plan is a government payor.

Confirm Does Not Confirm

b. Vendor will provide a network that will support Plan Members residing in all 100 counties in North Carolina and throughout the United States.

Confirm Does Not Confirm

c. Vendor will work with the Plan to develop and implement provider specific alternative payment arrangements.

Confirm Does Not Confirm

d. Vendor will develop a “narrow” network, at the regional or state level, of lower cost, high quality providers to be paired with a custom Plan Design, if requested by the Plan. This offering may be a full replacement or offered alongside other Plan Design options.

Confirm Does Not Confirm

e. Vendor’s current network includes bundled/episodic payment and clinically integrated network arrangements.

Confirm Does Not Confirm

f. Vendor will work with the Plan to expand, and if necessary, customize bundled/episodic payment arrangements.

Confirm Does Not Confirm

g. Vendor will work with the Plan to develop and administer a custom network for the Plan with a Medicare-based reimbursement methodology model that will include, at a minimum, different reimbursement rates for professional, inpatient, and outpatient services, upon request by the Plan.

Confirm Does Not Confirm

h. If the Plan implements a Medicare-based reimbursement model, Vendor will adjust any payment and/or medical policies required to better align with Medicare pricing guidelines.

Confirm Does Not Confirm

i. If the Plan implements a Medicare-based reimbursement model, Vendor will administer any other Medicare medical and payment policies adopted by the Plan.

Confirm Does Not Confirm

j. Vendor will integrate with Optum Insight or a comparable tool to support and maintain the existing repricing/pricing structure if requested by the Plan.

Confirm Does Not Confirm

k. Upon request, Vendor will supplement the Plan's custom network with other providers contracted directly by Vendor for services such as reference labs, durable medical equipment, and other commodity services as well as to ensure access to care standards are met in North Carolina.

Confirm Does Not Confirm

l. Vendor will administer other reference-based pricing models, if requested by the Plan.

Confirm Does Not Confirm

5.1.4 Product and Plan Design Management Minimum Requirements

a. Vendor will administer the covered benefits and exclusions as outlined in the Enhanced PPO Plan (80/20), Base PPO Plan (70/30) and HDHP benefit booklets. The Plan understands that utilization and Medical Management programs as well as out-of-network processes may vary from the Plan's current programs.

- i. Enhanced PPO Plan (80/20): <https://www.shpnc.org/media/2583/download?attachment>
- ii. Base PPO Plan (70/30): <https://www.shpnc.org/media/2582/download?attachment>
- iii. HDHP: <https://www.shpnc.org/media/2584/open>

Confirm Does Not Confirm

b. Vendor will administer a tiered copay program that will reduce a copay when the Member visits the Primary Care Provider (PCP) listed on his or her ID card or another PCP in the same practice, regardless of practice location. See grid in Exhibit 2, "PCP Copay Incentive Scenarios," for more detailed information about the current program.

Confirm Does Not Confirm

c. Vendor will customize its current value-based and incentive Plan Design features and/or implement new, customized ones, if requested by the Plan.

Confirm Does Not Confirm

d. Vendor will integrate real-time or near real-time deductible and/or out-of-pocket (OOP) accumulators with the Plan's PBM to support a combined Medical/Rx deductible and OOP maximums.

Confirm Does Not Confirm

e. Vendor will administer all benefits as required by Article 3B of Chapter 135 and, to the extent applicable, Chapter 58 of the North Carolina General Statutes and as may be amended from time to time.

Confirm Does Not Confirm

f. Vendor will administer benefits in accordance with all Federal and State requirements and notify the Plan of new mandates, or other requirements, that will require benefit changes to maintain compliance.

Confirm Does Not Confirm

g. Vendor will partner with the Plan to design custom benefits and/or Plan Design features, as requested by the Plan and provide associated financial/actuarial impact analysis.

Confirm Does Not Confirm

5.1.5 Medical Management Programs Minimum Requirements

a. Vendor will pass 100% of specialty pharmacy Rebates to the Plan.

Confirm Does Not Confirm

b. Vendor will carve-out PBM services from this Contract.

Confirm Does Not Confirm

c. Vendor will customize any of the Medical Management programs, if requested by the Plan.

Confirm Does Not Confirm

5.1.6 Enrollment, EDI, and Data Management Minimum Requirements

a. Vendor will support the Plan's Group set-up structure which includes establishing, maintaining, and reporting on more than 400 individual Employing Units, the Retirement Systems Group, the Direct Bill Group, the Sponsored Dependent Group, and the COBRA Group. A list of the Plan's current Group structure, which includes Group and Entity identifiers, can be found in Exhibit 3, "Group Structure."

Confirm Does Not Confirm

b. Vendor will support the addition of new Groups throughout the year and assist with any Group name changes or reporting requirements, as needed.

Confirm Does Not Confirm

c. Vendor will have the capability to accept at least 500,000 transactions in a single file transmission.

Confirm Does Not Confirm

d. Vendor will have the capability to extract and send up to 500,000 transactions to Plan vendors in a single file.

Confirm Does Not Confirm

e. Vendor will accept and load a daily industry standard and/or custom data files from the Plan's EES vendor. The data file will be received between 5:00 – 9:00 p.m. ET each night and must be processed and loaded by Vendor by 8:00 a.m. ET the following State Business Day.

Confirm Does Not Confirm

f. Vendor will produce recurring outbound data files for Plan vendors, the Plan and/or Plan Partners. For inbound and outbound data flows, see Exhibit 4, "Vendor Data Feeds."

Confirm Does Not Confirm

g. Vendor's daily outbound data file to the Plan's EES vendor must be sent by 12:00 p.m. ET on the first day after the daily data file from the Plan's EES vendor is received.

Confirm Does Not Confirm

h. Vendor will support the receipt of monthly Audit Files from the Plan's EES vendor and work with the Plan and the EES vendor to review and correct discrepancies. Refer to Exhibit 5 "Monthly Audit & Reconciliation" for Vendor audit process.

Confirm Does Not Confirm

i. Vendor will agree to other enrollment audits, as requested by the Plan, to address specific issues.

Confirm Does Not Confirm

j. Vendor will enroll and accurately process claims for both Medicare primary and Non-Medicare primary Members within the same Group and Plan Design.

Example: Employing Unit – Department of State Treasurer

Enhanced PPO Plan (80/20) includes:

- Non-Medicare primary Members
- Medicare primary Members

Base PPO Plan (70/30) includes:

- Non-Medicare primary Members
- Medicare primary Members

Confirm Does Not Confirm

k. Vendor will serve as the Plan's Responsible Reporting Entity (RRE) under Section 111 of the Medicare, Medicaid, and SCHIP Extension Act of 2007 (MMSEA) Expanded Reporting Option.

Confirm Does Not Confirm

l. As an Expanded Reporter, Vendor will submit, at a minimum, a quarterly Query-Only File to CMS to obtain Part A, B, and C information on Plan Members and perform a quarterly Medicare Primacy audit with Plan Enrollment data in Vendor's system. Vendor shall utilize the results of the audit in conjunction with the Plan's Medicare rules, to determine which Plan Members' Medicare information requires updating.

Confirm Does Not Confirm

m. Vendor will update Vendor's system with the necessary updates from the Medicare audit and send Members' updated Medicare information to the Plan's EES vendor.

Confirm Does Not Confirm

n. Vendor will store and utilize the Medicare Beneficiary Identifier (MBI), in addition to other Member identification numbers, such as Social Security Number (SSN).

Confirm Does Not Confirm

o. Vendor will maintain Medicare Eligibility effective and termination dates as well as Medicare Part A and Part B effective and termination dates.

Confirm Does Not Confirm

p. Vendor will maintain Medicare primacy effective and termination dates.

Confirm Does Not Confirm

q. Vendor will maintain multiple Medicare entitlement reasons.

Confirm Does Not Confirm

r. Vendor will collect, store, and utilize other commercial insurance information to coordinate benefits for Plan Members. The EES Vendor will only collect Medicare information. All other commercial insurance information will be managed by the TPA.

Confirm

Does Not Confirm

s. Vendor will enroll split-contracts where the family Members are split between Vendor and another carrier (i.e., Medicare primary Subscriber enrolled in a Medicare Advantage plan with another carrier and non-Medicare primary Dependents are enrolled on a Plan provided by Vendor).

Confirm

Does Not Confirm

t. Vendor will support enrollments where one or more family Members are enrolled in one Plan Design as Medicare primary and other family Member(s) are enrolled in another Plan Design as Non-Medicare primary, or vice versa.

Confirm

Does Not Confirm

u. Vendor will provide a PCP selection tool that can be integrated with the Plan's EES vendor's enrollment portal to facilitate the Members' PCP elections. See Exhibit 6, "PCP Selection Tool and Maintenance," for PCP selection overview.

Confirm

Does Not Confirm

v. Vendor will routinely perform provider maintenance of PCP data to ensure that the PCP selection tool contains the most current PCP data and that only valid PCPs may be elected. See Exhibit 6, "PCP Selection Tool and Maintenance" for high level overview of PCP maintenance requirements.

Confirm

Does Not Confirm

w. Vendor will implement workflows that support the maintenance of the PCPs which may require that Vendor notify Members if their elected PCP is no longer in network and notify the EES vendor, via the daily return file to the EES vendor, if any PCP code information, including provider termination, has occurred. The Member communication should include instructions for electing a new PCP. The final workflows will be defined during Contract implementation. See Exhibit 6, "PCP Selection Tool and Maintenance" for high level overview of PCP synchronization requirements.

Confirm

Does Not Confirm

x. Vendor will customize ID cards with all data elements requested by the Plan, including, but not limited to, each of the following: (See Exhibit 7, "Sample ID Cards," for examples of the Plan's current ID card.)

i. Plan's logo.

ii. Plan's messaging.

- iii. Plan's network (if applicable).
- iv. Out-of-NC network.
- v. Member out-of-pockets.
- vi. Plan's Rx BIN and PBM information.
- vii. Group Name (e.g., Wake County Schools, University of North Carolina, Department of Transportation).
- viii. Member's unique ID number.
- ix. Member's selected PCP.

Confirm Does Not Confirm

- y. Vendor will meet all Plan, Federal, and State mandated Plan enrollment communication and/or reporting requirements such as, but not limited to, the production of Certificates of Creditable Coverage (CCC) and reporting needs under sections 6055 and 6056 of the IRS code.

Confirm Does Not Confirm

- z. Vendor will provide a custom claims data files to the Plan on a monthly basis, or more frequently, if requested by the Plan. The file requirements will be documented in a BRD during implementation and may be updated from time to time throughout the lifetime of the Contract, as requested by the Plan.

Confirm Does Not Confirm

- aa. Vendor will provide a custom provider data file(s) to the Plan on a bi-weekly basis. The file(s) requirements will be documented in a BRD during implementation and may be updated from time to time throughout the lifetime of the Contract, as requested by the Plan.

Confirm Does Not Confirm

- bb. Vendor will provide other, ad hoc data files, as requested by the Plan. The specifics of the data file requests will be outlined in an ADM and/or BRD.

Confirm Does Not Confirm

- cc. Vendor will implement a process with the Plan to respond to data quality (DQ) issues with any files provided to the Plan. The specifics of the DQ checks will be developed during implementation and may be amended throughout the lifetime of the Contract, as requested by the Plan.

Confirm Does Not Confirm

dd. Vendor will release data to the Plan as described in state and federal law.

Confirm Does Not Confirm

ee. Vendor will not place limitations on the Plan's use of data that are more restrictive than described in state and federal law.

Confirm Does Not Confirm

5.1.7 Customer Experience Minimum Requirements

a. Vendor will provide a dedicated customer call center with hours of operation from at least 8:00 a.m. to 5:00 p.m. ET, each State Business Day, to respond to Member inquiries.

Confirm Does Not Confirm

b. Vendor will have a dedicated toll-free number for Plan Members.

Confirm Does Not Confirm

c. Vendor will answer the phones with a greeting that identifies the call center as a representative for the Plan.

Confirm Does Not Confirm

d. Vendor will customize its interactive voice response (IVR) script with a Plan-specific greeting and prompts, and transfers to other Plan vendors.

Confirm Does Not Confirm

e. Vendor will make and receive warm and cold transfers to/from other Plan vendors who may be required to resolve the Members' issues.

Confirm Does Not Confirm

f. Vendor will record and track all Member calls including date of initial call, inquiry closed, representative who handled the call, call status, if and where the call was referred for handling, reason for call (issue), and what was communicated to the Member.

Confirm Does Not Confirm

g. Vendor will allow the Plan to include customized inserts or messaging in ID Cards and Explanation of Benefits (EOB) mailings as well as offer customization of the EOB and ID Cards as directed by the Plan. Refer to Exhibit 7, "Sample ID Cards" and Exhibit 8, "Sample EOB."

Confirm Does Not Confirm

h. Vendor will customize the content of any and all letters or other materials Vendor will send and/or display to Members.

Confirm Does Not Confirm

i. Vendor will co-brand letters or other materials Vendor sends to Members.

Confirm Does Not Confirm

j. Vendor will customize the portal with the Plan's branding (logo).

Confirm Does Not Confirm

k. Vendor will provide an employer portal to be utilized by Plan staff to view real-time individual Member enrollment and claim information.

Confirm Does Not Confirm

5.1.8 Claims Processing and Appeals Management Minimum Requirements

a. Vendor will comply with all requirements set forth in Article 29B of Chapter 90 of the North Carolina General Statutes. As required, Vendor will validate provider enrollment in North Carolina's Health Information Exchange (NC HealthConnex) prior to paying Plan Member claims. If prohibited by the Statewide Health Information Exchange Act, Vendor must deny any claims received from providers that are not in compliance on the date of service.

Confirm Does Not Confirm

b. Vendor will process all claims, including claims that are Medicare primary and Medicare secondary, from the same claims processing platform.

Confirm Does Not Confirm

c. Vendor will administer the appeals process required by Chapters 58 and 135 of the North Carolina General Statutes, including appeals for the Plan's PBM. Refer to Benefits Booklets and N.C.G.S. § 135-48.24.

Confirm Does Not Confirm

d. Vendor will customize any appeals letters, as requested by the Plan.

Confirm Does Not Confirm

e. Vendor will work with the Plan to resolve and respond to any inquiries from the North Carolina Department of Insurance's Smart NC Program.

Confirm Does Not Confirm

f. Vendor will support the Plan's methodology for coordinating with Medicare Members who have not elected Medicare Part A and/or B. As required by state law, the Plan coordinates claims for Members who do not elect Medicare Parts A and/or B as if they had elected them. (a.k.a. Phantom Processing) See Exhibit 9, "Claims Processing Phantom Plan - Medicare Part B."

Confirm Does Not Confirm

g. Vendor will reimburse the Plan on a weekly basis for any prompt pay penalties included in the weekly claims disbursement for that week as the Plan will pay no prompt-pay penalties for claims that are paid outside of the prompt-pay guidelines as a result of Vendor's action, inaction, or system failure.

Confirm Does Not Confirm

h. Vendor will customize EOBs with the Plan's logo and if applicable, custom network and other information as illustrated in Exhibit 8, "Sample EOB."

Confirm Does Not Confirm

5.1.9 Claims Audit, Recovery, and Investigation Minimum Requirements

a. Vendor will support ongoing quarterly claims accuracy audits, or Standard Audits, performed on a statistically valid random claims sample selected by the Plan's audit vendor which will be used to measure claims accuracy for Performance Guarantees on a quarterly basis. Vendor will share provider contracts and system pricing with the Plan's auditors for review and audit. The audit will also include a targeted sample selected from a comprehensive analysis of all claims by the Plan's audit vendor.

An audit plan will be provided prior to the initial quarterly audit that will define the ongoing Standard Audit timelines. Both the random claims sample and the targeted sample will be used to identify overpayments owed to the Plan. For purposes of Standard Audits, claims accuracy will be measured based on the following criteria:

- i. Financial Accuracy: Total dollar amount processed accurately divided by the total dollar amount processed in the audit sample. The total dollar amount processed accurately is calculated by subtracting the absolute values of the dollars processed in error from the total dollars processed. Underpayments and overpayments are not offset by one another.
- ii. Payment Accuracy: The number of claims with the correct benefit dollars paid divided by the total number of claims paid in the audit sample.

iii. Processing Accuracy: The number of claims processed with no procedural errors divided by the total number of claims processed.

For purposes of the above definitions, if Vendor has identified and recovered an overpayment or processed an underpayment prior to the audit, it is not an error. If Vendor has identified but not recovered the overpayment or processed the underpayment, it is an error.

Confirm Does Not Confirm

b. Vendor will, in addition to supporting ongoing quarterly claims accuracy audits, support Focus Audits, such as, but not limited to, coordination of benefits (COB) audits, duplicate claims audits, eligibility audits, and comprehensive electronic audits conducted by the Plan's auditor vendor on an as needed basis. All the rules outlined in Section 5.1.9.a above will apply to these audits.

Confirm Does Not Confirm

c. Vendor's recovery processes will follow all deposit and financial reporting requirements outlined in Section 5.2.2, Finance and Banking.

Confirm Does Not Confirm

d. Vendor will recover any overpayments to Providers by offsetting future payments or by demand without any limitation as to time since the Plan as a government payor is not subject to the two-year limitation established in N.C.G.S. § 58-3-225(h).

Confirm Does Not Confirm

e. Vendor will support the Plan's participation in the North Carolina Debt Setoff Program (North Carolina General Statutes, Chapter 105A, Article 1), the Retirement/Disability Offset Program (N.C.G.S. §§ 135-9(b), 128-31, 120-4.29), Wage Garnishment (N.C.G.S. § 135-48.37A), and Credit Card Intercepts (N.C.G.S. § 1- 359) and implement an accounts receivable collection process as outlined under the North Carolina Office of State Controller, Statewide Accounts Receivable Program. Refer to Exhibit 10, "State Health Plan Recovery Workflows."

Confirm Does Not Confirm

f. Vendor will ensure the Plan's compliance with all federal and state regulations not otherwise stated previously (i.e., prompt pay, mental health parity, disclosures, reporting, etc.).

Confirm Does Not Confirm

g. Vendor has an investigation or similar unit to investigate possible fraud and abuse and will share details about specific investigations that impact the Plan, including the names of the providers involved.

Confirm Does Not Confirm

5.1.10 Initial Implementation and Ongoing Testing Minimum Requirements

a. Vendor will have a fully assembled implementation team that includes the appropriate subject matter experts, ready to begin work within two (2) weeks of contract award. The team shall include an overall implementation manager and separate implementation resources for, at a minimum, each of the following work streams:

- i. Group Set-Up & Enrollment
- ii. Plan Vendor Integration & EDI, which includes:
 - 1) EES vendor Integration. (EDI, PCP Tool, SSOs, Audits)
 - 2) PBM vendor Integration. (Data files, SSOs, Accumulators)
 - 3) Billing vendor Integration. (Claims hold, Audits)
 - 4) Plan Data Warehouse Integration. (Data files)
- iii. Network Evaluation

Other workstreams will kick-off throughout 2023.

Confirm Does Not Confirm

b. Vendor will have the depository bank account(s) setup and tested at least 45 days prior to January 1, 2025.

Confirm Does Not Confirm

c. If applicable, Vendor will have the disbursement account(s) setup and tested at least 30 days prior to January 1, 2025.

Confirm Does Not Confirm

d. Vendor will have all services, including custom programs, operational by January 1, 2025.

Confirm Does Not Confirm

e. Vendor will work with the Plan to document in an ADM all custom processes developed to meet the Plan's unique requirements. The Plan's Contract Administrator for day-to-day activities is authorized to sign ADMs for the Plan.

Confirm Does Not Confirm

f. Vendor will work with the Plan to finalize Vendor Audit Schedule for 2025 and subsequent years. This Audit Schedule will be updated via ADM. The Plan's Contract Administrator for day-to-day activities is authorized to sign ADMs for the Plan.

Confirm Does Not Confirm

- g. For all technical components of the initial implementation as well as any implementations throughout the lifetime of the Contract, Vendor will develop functional requirements documents, Implementation Plans, Test Plans, Deployment Plans, and Close-Out Documentation derived from the Plan's Business Requirements. These documents must be mutually agreed upon by Vendor, the Plan, and any impacted Plan vendor. The Plan's Contract Administrator for day-to-day activities is authorized to sign these documents for the Plan.

Confirm

Does Not Confirm

- h. Vendor will support both Unit Testing and End-to-End Testing prior to Go-Live of any initiative. To support testing, Vendor must not only have the resources, but also the test environments, necessary to support multiple work streams at one time. As mentioned above, the Test Plan will be mutually agreed upon by Vendor, the Plan, and impacted Plan vendors. The Plan's Contract Administrator for day-to-day activities is authorized to sign these documents for the Plan.

Confirm

Does Not Confirm

- i. Vendor will support the 2025 Open Enrollment, which is currently scheduled for October 2024 but may be rescheduled to a different time at the Plan's sole discretion. Vendor must have the group set-up complete, the call center open, any required SSOs in place, the PCP selection tool integrated with the Plan's EES vendor and be able to accept EDI from Plan vendors during the month Open Enrollment occurs.

Confirm

Does Not Confirm

5.1.11 Reporting Minimum Requirement

- a. Vendor will agree to delivering the Standard Reports as described in Section 5.2.11.2.b.viii.2) – xvii.3), and based on the delivery schedule in Exhibit 11, "Standard Reports."

Confirm

Does Not Confirm

ATTACHMENT C: NORTH CAROLINA GENERAL CONTRACT TERMS & CONDITIONS

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.

- | | |
|---|--|
| a. Accenture - Philippines, India | e. EXL Service Holdings - India, Philippines, Columbia |
| b. Cognizant - India | f. HGS Healthcare - India, Philippines |
| c. Concentrix - India | g. Infosys - India |
| d. Conduent - Philippines, India, Fiji, Guatemala | h. Optum Insights - India, Philippines |

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

- | | |
|---|--|
| a. Accenture - data entry | e. EXL Service Holdings - overpayment recovery |
| b. Cognizant - claims | f. HGS Healthcare - claims |
| c. Concentrix - provider calls, claims services | g. Infosys - transactional billing and eligibility processes |
| d. Conduent - claims | h. Optum Insights - overpayment recovery |

None of the locations and services listed above are for member facing services.

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

- 4050 Piedmont Parkway, High Point, NC 27265
- 5000 CentreGreen Way, Suite 350, Cary, NC 27513
- 151 Farmington Avenue, Hartford, CT 06156
- 261 N University Dr, Plantation, FL 33324
- Home-based employees located throughout United States

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. Confirmed.
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. Confirmed.
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. Confirmed.

ATTACHMENT E: CERTIFICATION OF FINANCIAL CONDITION

Name of Vendor: Aetna Life Insurance Company

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: 02/09/2022 (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.

Aetna Life Insurance Company (ALIC) and its subsidiaries/affiliates are routinely involved in non-material litigation regarding the administration of health and dental plans. Most of this litigation involves a single claim for benefits or payment for provider services.

ALIC is a wholly-owned subsidiary of Aetna Inc. (Aetna). On November 28, 2018, Aetna Inc. and each of its subsidiaries, including ALIC became a wholly-owned subsidiary of CVS Health Corporation. All material litigation was reported in Aetna's public filings.



Signature

Date

9/20/22

Tami Polsonetti

Assistant Vice President

Printed Name

Title

[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 Aetna Life Insurance Company (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: _____

Aetna Life Insurance Company

By: Tami Polsonetti

Signature: 

Title: Assistant Vice President

Date: 9/20/22

Attachment A: Department of State Treasurer HIPAA Privacy Officer (“HPO”)

Chris Almberg, Esq.
HIPAA Privacy Officer
3200 Atlantic Avenue
Raleigh, NC 27604
(919) 814-4428
Chris.Almberg@nctreasurer.com

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: Aetna Life Insurance Company

Address (city, state, and zip code): 151 Farmington Avenue, Hartford, CT 06156

Website URL: Aetna.com

ATTACHMENT H: HIPAA QUESTIONNAIRE

Name of person completing form, and role: Tami Polsonetti, Executive Director, Sales Support

Email address: PolsonettiT@aetna.com

Phone number: 860-273-3396

Fax number: 860-636-7795

HIPAA compliance person's name, title, phone number, and email address, if different than person completing form: Anna Shimanek, Chief Privacy Officer, 401-374-2466, Anna.Shimanek@cvshealth.com

Date you are completing this form: 9/20/2022

*** 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: Anna Shimanek

Title: Chief Privacy Officer

Address: 151 Farmington Avenue, Hartford, CT 06156

Phone number: 401-374-2466

E-mail address: Anna.Shimanek@cvshealth.com

Certification designation (e.g., CHC, CISSP, CIPP, CHP, CHPSE, etc.): None

Date certified: None

ATTACHMENT H: HIPAA QUESTIONNAIRE

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.).
-

Our Chief Privacy Officer is an attorney knowledgeable of state and federal privacy laws. Anna leads our Information Governance and Privacy Office and is responsible for ensuring we have a robust privacy compliance program, advising on incident response and providing legal and privacy advice on best practices for our innovative products and services. She also oversees our information governance program, including our enterprise information firewall program. She was named the Chief Privacy Officer for CVS Health in June 2021.

Anna has more than 20 years of experience as an attorney and most recently led the CVS Health Information Governance and Transformation legal team, working closely with enterprise transformation consumer products, our digital organization, IT operations, and interoperability solutions. She has been at CVS Health five+ years. Previously, Anna held roles as the HIPAA Privacy Officer other large corporations.

Employee HIPAA Training

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

All of our employees are required to complete a number of compliance training courses upon hire and annually thereafter, and completion is tracked. The training courses include:

- Firewall Training
- Privacy Training for CVS Health Colleagues
- CVS-Aetna Health Code of Conduct
- Information Security Awareness

ATTACHMENT H: HIPAA QUESTIONNAIRE

We conduct the training online through our secure intranet. Our compliance organization electronically monitors the training through a training tracker tool, which follows up with each employee until we reach 100 percent completion.

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
-

Yes.

- 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?
-

CVS-Aetna Health's Code of Conduct, which includes HIPAA training, is reviewed annually for potential updates. It was reviewed in May 2022 and will be reviewed again in May 2023.

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

Yes.

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

Please refer to our Privacy Program Overview under Tab S-9 in the Supplemental Items section of our response.

ATTACHMENT H: HIPAA QUESTIONNAIRE

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

Our privacy policies were reviewed in May of 2022 and will be reviewed again in May of 2023.

8. Are employees trained on the privacy policies and procedures? Yes No

Yes.

9. Are employees required to sign an agreement stating they have read and understand the privacy policies and procedures? Yes No

Yes.

10. Are there internal HIPAA security policies and procedures in place which govern the security practices of the organization and its employees? Yes No

Yes.

11. Attach a copy of all internal/employee-facing security policies and procedures.

See refer to our CVSH Control Standards document included under Tab S-10 in the Supplemental Items section of our response. Specifically, please refer to the following sections within that document:

- ACS-1104 – Software Security Education
- ATCS-017 – Information Security Training
- ATCS-599 – Training Evaluation

ATTACHMENT H: HIPAA QUESTIONNAIRE

Employees who support Aetna's information security activities are encouraged to maintain technical proficiency. EIS proactively participates in the industry groups and forums, including Financial Services Information Sharing and Analysis Center (FS-ISAC), National Health Information Sharing and Analysis Center (NH-ISAC), System Administration, Network and Security (SANS), and the Cloud Security Alliance. Personnel with security responsibilities must complete Aetna's Security Compliance Technology Based Training (TBT) to increase awareness and knowledge of Aetna's information security policies, standards, and procedures, which must be followed when granting access to Aetna's information resources.

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

Our security policies were reviewed in August of 2022 and will be reviewed again in August of 2023.

12. Are employees trained on the security policies and procedures? Yes No
-

Yes.

13. Are employees required to sign an agreement stating they have read and understand the security policies and procedures? Yes No
-

Yes.

14. Can you provide documentation that all employees have completed training? Yes No
-

Yes.

ATTACHMENT H: HIPAA QUESTIONNAIRE

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.)
-

Yes. We are fully compliant with all HIPAA requirements that have been issued to date. We use all HIPAA EDI mandated code sets.

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.
-

An audit of our HIPAA compliance was completed in August of 2022. We have provided a copy of the audit findings under Tab S-11 in the Supplemental Items section of our response.

Data Security

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

Aetna personnel follow the Aetna Proper Disposal of Confidential Information Exhibit and the Aetna Physical and Electronic Safeguards for Protected Health Information (PHI).

Servers containing ePHI that need to be returned at the end of a lease go through a multi-step cleaning and sanitization process performed by approved vendors and Aetna. All parties keep a chain-of-custody log.

All sensitive media is disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Aetna colleagues adhere to the Proper Disposal of Confidential Information Exhibit to determine the appropriate method for disposal.

ATTACHMENT H: HIPAA QUESTIONNAIRE

Per ATCS-052, Restricted, Confidential, and/or Proprietary information in hard copy form must be disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Papers, slides, microfilm, microfiche, diskettes, and photographs containing sensitive information should be disposed of by cross-shredding or burning. Magnetic tape must be degaussed prior to being reused and/or if it is being physically destroyed. If removable storage media or hardware cannot be sanitized it is destroyed. All Confidential or Restricted information is purged through overwrites prior to any hardware being released for off-site maintenance.

The use of third-party collection and disposal services for disposal of information in hard copy is authorized, however emphasis is placed on selecting suitable contractors that exercise adequate security controls and have requisite experience. Aetna has media destruction agreements with vendors who periodically remove and sanitize media. Vendors are National Institute of Standards and Technology (NIST) certified. All data is encrypted or otherwise unreadable when waiting for destruction. Specific destruction policies and procedures have been created for each type of Aetna media asset.

For any other details on the security control standards please refer to the CVSH Control Standards document included under Tab S-10 in the Supplemental Items section of our response.

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.
-

Our policies, procedures and technologies are in place to protect sensitive information against use and disclosure that is inappropriate and not authorized. Examples include:

- Written privacy and security policies
- Annual privacy and security awareness training for all employees
- Integrity and access controls
- Message authentication and/or encryption
- Firewall and proxy server technologies

ATTACHMENT H: HIPAA QUESTIONNAIRE

We restrict access to protected health information (PHI) to employees who need it to provide products or services to our members through “role-based access control” (RBAC). We maintain physical, electronic and procedural safeguards to protect PHI against access and use we didn’t authorize. We limit access to our facilities to personnel we authorize. We protect electronic information through a variety of technical tools.

We have multiple data processing controls to ensure data confidentiality. Application integrity controls demonstrate that data has not changed between checkpoints. Process-integrity controls are safeguards and measures taken to ensure that the underlying business logic and practices are properly embedded into the logic of the application. Data quality is the process of ensuring the accuracy and integrity of data used by an application; this process involves edit and validation controls that verify the accuracy and integrity of the information being input into the application.

Our Privacy Office includes privacy and security advisors. We assign advisors to our business units to serve as the initial point of contact. They are responsible for day-to-day enforcement of our privacy and security policies and the procedures that support them.

Our privacy and security policies and procedures are subject to ongoing monitoring. For example:

- Our Internal Audit department and Corporate Compliance Assessment Teams periodically perform assessments on the company’s privacy policies and procedures and issue compliance review reports. We develop corrective action plans as needed to address the findings of the reviews.
- Key business areas (e.g., member services) incorporate review of employee adherence to privacy policies in ongoing quality management efforts.
- We review our corporate privacy policies annually and update as needed. We conduct an annual review of our security program to make sure the necessary controls are in place to meet HIPAA Security requirements and the program continues to address evolving security threats. Our subject matter experts review each HIPAA requirement to confirm compliance. We require they provide supporting evidence of compliance. We completed our most recent security reviews in August 2022.

ATTACHMENT H: HIPAA QUESTIONNAIRE

Aetna has implemented technical security measures, including the use of strong encryption algorithms and secure networks protocols, to guard against unauthorized access to ePHI that is being transmitted over the network. ACS-710 details specific encryption, hashing, and cryptographic requirements. Approved encryption is required when confidential or restricted data, including PII and ePHI, is transmitted over a public network or a WAN connection.

In all scenarios, encryption is applied in the event of contractual, line of business, legal, or regulatory requirements mandating encryption. ACS-905 also outlines SSL/TLS configuration requirements for data transmission. All applications must utilize TLS 1.2 or greater.

Protocols with known vulnerabilities, including SSLv2, SSLv3, TLS 1.0, and TLS 1.1 should be disabled on all communication end points. SSL/TLS end points use Internet Engineering Task Force (IETF) X.509 certificates in accordance with ATCS-252.

Aetna utilizes Symantec DLP which monitors data that is being downloaded, copied, or transmitted to or from laptops and desktops. DLP is implemented to monitor data leaving the network through SMTP, HTTP, certain HTTPS sites, and approved FTP transfers. DLP control health and effectiveness is primarily measured through KPIs, which are reported to senior management at least monthly. Additionally, Mimecast Email Security is utilized for inbound and outbound email hygiene to ensure information contained within emails is protected. Mimecast performs filtering scans for malware, viruses, malicious URLs, suspicious attachments, phishing attempts, spam, and is also used to encrypt outbound emails after they have been scanned by the DLP tools.

For any other details on the security control standards please refer to the CVSH Control Standards document included under Tab S-10 in the Supplemental Items section of our response.

-
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. We consider the security and integrity of customer data to be our highest priority. We consider how we identify data security breaches proprietary. Upon learning of an incident, designated Aetna experts assess all facts known about the incident and determine all known and potential impacts.

ATTACHMENT H: HIPAA QUESTIONNAIRE

To prevent inappropriate use or disclosure of member health information, we have adopted extensive information privacy and security policies and use rigorous quality assurance and audit procedures to assure these policies are followed.

Even with these strict safeguards in place, there may be instances where a member's health information may be disclosed due to unintentional errors that occur while handling a very high claim volume. We have a comprehensive incident response plan to handle any potential data security breach.

Our investigators and individuals in specific business areas take the lead on reported incidents. They determine if there is an unapproved disclosure of data and the required notification.

We investigate any suspected breach of member privacy. Parties involved in the investigation include:

- Privacy Office
- Contacts for the business area that experienced the incident
- The business area's assigned business area privacy and security manager, who works closely with the Privacy Office on all privacy/security-related matters
- Representatives from other departments such as IT Security, Human Resources, Corporate Security and Investigative Services, as appropriate

Our investigators execute the Privacy Office Incident Response Plan for any potential privacy breaches. The Privacy Office works with Global Security on security incidents.

Our rapid response team handles breaches. The team includes information security, physical security, investigative services, business continuity, legal, compliance, business subject matter experts, and customer-facing representatives.

Regardless of who handles a breach, we follow a rigorous process to immediately halt any ongoing breach and to mitigate the impact of the event to our customers. We also notify members, customers, regulators, and/or the media, as appropriate.

ATTACHMENT H: HIPAA QUESTIONNAIRE

We identify the root cause of the breach to strengthen controls. And, where necessary, we develop a corrective action plan, which may include employee training, to prevent such breaches in the future.

20. Has the company conducted a risk assessment and gap analysis to address any findings? Yes No
-

If yes: Date: August 2022 Performed by: Lunarline, Inc.

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

Yes. We have included our most recent SOC2 report under Tabs S-1, S-2, and S-3 in the Supplemental Items section of our response. Our current report covers October 1, 2020 through June 30, 2021. The next report (through 6/30/2022) is anticipated to be available sometime in October. We have also included a Bridge Letter which covers June 30, 2021, through June 20, 2022.

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).
-

In 2020, Aetna entered into a Resolution Agreement with the Office for Civil Rights (OCR) related to three breaches suffered by Aetna in 2017.

Aetna Life Insurance Company and the affiliated covered entity (Aetna) has agreed to pay \$1,000,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle

ATTACHMENT H: HIPAA QUESTIONNAIRE

potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Aetna is an American managed health care company that sells traditional and consumer-directed health insurance and related services.

In June 2017, Aetna submitted a breach report to OCR stating that on April 27, 2017, Aetna discovered that two web services used to display plan-related documents to health plan members allowed documents to be accessible without login credentials and subsequently indexed by various internet search engines. Aetna reported that 5,002 individuals were affected by this breach, and the protected health information (PHI) disclosed included names, insurance identification numbers, claim payment amounts, procedures service codes, and dates of service.

In August 2017, Aetna submitted a breach report to OCR stating that on July 28, 2017, benefit notices were mailed to members using window envelopes. Shortly after the mailing, Aetna received complaints from members that the words "HIV medication" could be seen through the envelope's window below the member's name and address. Aetna reported that 11,887 individuals were affected by this impermissible disclosure.

In November 2017, Aetna submitted a breach report to OCR stating that on September 25, 2017, a research study mailing sent to Aetna plan members contained the name and logo of the atrial fibrillation (irregular heartbeat) research study in which they were participating, on the envelope. Aetna reported that 1,600 individuals were affected by this impermissible disclosure.

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.

Our CVSH Control Standards document is included under Tab S-10 in the Supplemental Items section of our response. Specifically, please refer to the following sections within that document:

ATTACHMENT H: HIPAA QUESTIONNAIRE

- ATCS-045 – Disposing of Information in Electronic Form
- ATCS-052 – Disposing of Information in Hard Copy Form
- ATCS-113 – Removing Data from Storage Media Prior to Disposal

Aetna has media destruction agreements with vendors who periodically remove and sanitize media. Vendors are National Institute of Standards and Technology (NIST) certified. All data is encrypted or otherwise unreadable when waiting for destruction. Specific destruction policies and procedures have been created for each type of Aetna media asset. We keep our Certificates of Recycling and Destruction from Lifespan that certify the destruction of Aetna equipment in accordance with NIST 800-88 standards.

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. The following table identifies our Tier 1 subcontractors, who are a subset of our suppliers/vendors. Tier 1 subcontractors provide member constituent services directly related to the administration of a customer contract and for whom a portion of the services provided may include direct member contact or significant access to member identifiable data.

Subcontractor	Scope of Services	Contact Information
1.Accenture LLP	Correspondence processing, accounts receivable, contract drafting, enrollment data entry	Patty Campbell (267) 216-1336
2.Cognizant Worldwide Limited	Clinical Claim review prep and related services	Jeffrey Taylor (972) 806-0844

ATTACHMENT H: HIPAA QUESTIONNAIRE

3. Conduent	Intake services: mailroom, imaging, data entry, X-ray handling, encounters, referrals, CATS and correspondence. Overpayment recovery for hospital credit balance review, HMO claims, call center services - SRC, ETech/SSHL, recertification. Print fulfillment.	Jeannie Hargis(844) 663-2638
4. Cotiviti	Overpayment Recovery for Data Mining, Duplicate Payments, Provider Credit Balance	Melissa Christensen (770) 379-2800
5. End-Game Strategy, Inc.	Overpayment recovery - data mining	Patrick Parker (860) 829-2200
6. Optum Insights LLC	Overpayment recovery - retro termination, contract compliance, out-of-network review, duplicate payment.	Barbara-Raye Stegner (888) 687-8555
7. Change Healthcare	Overpayment recovery - high cost drug audits, implant audits, medical bill audit (hospital bill audit, DRG audit and inpatient contract compliance audit)	Rick Meeske (866) 371-9066
8. EXL Service Holdings, Inc.	Clinical services including precertification scope/ steerage, Healthy Lifestyle Coaching/ Aetna Maternity Program, Pre-determination of services, clinical claim review, HEDIS abstraction for NCQA accreditation. Overpayment recovery and validation.	Michael Sefransky (518) 210-8974
9. HGS Healthcare	Claim adjudication, claim and correspondence processing, quality auditing, overpayment recovery, balancing and reconciliation, individual bill calls, repricing and audit, data entry.	Russ Uhlmann, JR (770) 635-8768
10. Iron Mountain, Inc.	Records archiving, retrieving, transportation, and destruction services	Jerry Harward (801) 381-0982
11. Navigate Well	Configurable wellbeing engagement platform; incentive tracking; real-time data reporting, integration with client vendors, wellbeing resources and digital and telephonic chronic condition coaching	Megan Smith (515) 325-1671

ATTACHMENT H: HIPAA QUESTIONNAIRE

12. Quest Diagnostics	Determine individual health risk factors resulting in a personal summary report or personalized health action plan. Quest Diagnostics Blueprint for Wellness Fasting Venipuncture Heart & Glucose Panel; blood testing; metabolic syndrome testing - will draw blood and measure other metabolic tests - includes data processing and calculating of data and communication to employee and benefits administration vendor or pass/fail for earning incentives.	Jason Moczul (248) 207-1169
13. Rawlings Company, LLC	Overpayment recovery for coordination of benefits and subrogation; medical	Camille Mills (502) 587-1279
14. Centrix	Provider calls, claim adjudication, claim and correspondence processing, overpayment recovery, quality audits, repricing, provider coding and reimbursement.	Philip Hadden (615) 596-8779
15. Infosys	Transactional billing and eligibility processes	Parayarikkal Renjith (510) 402-3778
16. Teladoc	Teladoc offers technology solutions to facilitate patient access to a network of physicians who can diagnose, treat and prescribe medication for common medical issues. Teladoc is a subcontractor in connection with its technology solutions while medical care is rendered through Teladoc's physician network (which is not a subcontractor of Aetna).	Kathleen Brand (412) 576-8319

1. 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. Please find the Business Associate Agreements under Tab S-12 in the Supplemental Items section of our response.

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

We require subcontractors to successfully complete and meet the standards stated in our privacy and security assessment as part of the initial contracting process.

ATTACHMENT H: HIPAA QUESTIONNAIRE

They must continue to meet the security standards. Subcontractors must comply with a series of requirements designed to protect constituents' information and keep it safe from theft, loss or inadvertent disclosure. We include the security requirements into our master agreement with the subcontractor. We make subcontractor adherence to the security standards a contractual requirement.

We require annual recertification of subcontractor compliance with the security requirements. This requirement applies to all subcontractors who have access to member health information and those who provide member constituent services directly related to the administration of the customer contract. We reserve the right to perform onsite audits of all such subcontractors.

In addition, our subcontractor contracts include confidentiality requirements and comply with the federal Hf PAA Privacy and Security Rules via a signed Business Associate agreement with each subcontractor who has access to member health information.

Violations

We consider the security and integrity of customer data to be among our highest priorities. We require subcontractors to notify us of any breach of confidential information when it occurs and to immediately take steps to halt and mitigate the breach.

Subcontractors not in compliance with our privacy and security requirements must complete a mutually agreed upon remediation plan to bring themselves into compliance or provide acceptable mitigating controls. We closely monitor progress of remediation plans to ensure completion. We reserve the right to suspend subcontractors that do not meet our requirements until they comply or we terminate them.

In addition to conducting security risk assessments, we have a formal continuous monitoring program to monitor the overall security posture of our third parties. The monitoring assessment period is based on the risk level of a third party. High-risk third parties go through annual risk assessment to monitor compliance with security obligations.

We use information received from a variety of sources, including daily Security Scorecard reports, threat and vulnerability analysis reports and incident information to gauge the risk level associated with our third parties. A significant drop in a

ATTACHMENT H: HIPAA QUESTIONNAIRE

Security Scorecard score, a privacy breach or a security incident will trigger a follow up risk assessment or other remediation activities.

We assume the responsibility for the performance of our subcontractors. In addition, we remain liable for contracted services performed by our company, including those services subcontracted by our company to another organization. Our third-party contracts confidentiality agreements that preclude us from sharing and risk assessment results.

We provide specifics to impacted customers. We also report such information to applicable government websites.

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

Yes. We have a documented vendor management process in place for the selection, oversight and risk assessment of our third parties.

The CVS Health Third Party Risk Governance (TRPG) team is responsible for the security assessment and risk management of our third parties. The risk governance program is designed to help ensure the privacy and security of our data and assets. Taking an innovative approach to third-party assessments using a risk-based methodology, we collaborate with our third parties and evolve with the ever-changing cybersecurity threat landscape. TRPG assesses the effectiveness of a third party's controls and works with them to increase the security maturity of their risk management techniques. Third Parties are subject to pre-contract and periodic follow up assessments to ensure their controls continue to meet our standards.

Risk assessment

The TPRG risk assessment is comprised of multiple steps that begin with creating a third party service portfolio that is used to evaluate and categorize risk. The risk category is used to determine the artifacts needed so that the appropriate assessment can be assigned. Risk categorization is based on several factors, including service type, data elements required, data storage location, and level of access, among others.

ATTACHMENT H: HIPAA QUESTIONNAIRE

A risk assessment can take up to 90 days to complete, depending on the type of assessment assigned and the number of findings identified. We will assign a risk manager to work with the third party for the duration of the assessment. The third party has thirty (30) days to submit their initial responses and artifacts. The risk manager is responsible for assisting the third party with navigating the process, reviewing the artifacts and working with the third party to develop mutually acceptable remediation plans for any findings that have been identified.

Onsite Assessment Report

Third parties that pose the highest risk to CVS Health are required to provide us with an independent onsite security assessment report as verification that effective security controls are in place and functioning as described in their questionnaire responses. Reports that we generally accept are SOC 2 Type II, HITRUST, ISO-27001, E-HNAC, or the Standardized Control Assessment (SCA) from Shared Assessments. Other reports may be accepted on an individual case basis.

Evidence Collection

As part of the security risk assessment, the third party may be required to provide artifacts for our review, as evidence of security control effectiveness. Artifacts requested may include but are not limited to:

- Data flow diagrams,
- Internal and external system, application, and network vulnerability scan results,
- Results of network and application layer penetration tests,
- List of their third parties that may have access to confidential CVS Health data

SecurityScorecard™

Using the third party's web address, TPRG will run a Security Scorecard report, which provides an overall scoring of the external risks and vulnerabilities associated with the third party. This report identifies potential vulnerabilities based on information gathered from the public internet, enabling us to evaluate a third party's overall health from an outsider's perspective. This is not a network penetration report. The data included in the report is gathered from publicly accessible external data sources. The third party is required to address any high or medium risk vulnerabilities identified in the Security Scorecard report.

ATTACHMENT H: HIPAA QUESTIONNAIRE**Continuous Monitoring**

In addition to conducting security risk assessments, we have a formal continuous monitoring program to monitor the overall security posture of our third parties. The monitoring assessment period is based on the risk level of a third party. High-risk third parties go through annual risk assessment to monitor compliance with security obligations. We use information received from a variety of sources, including daily SecurityScorecard reports, threat and vulnerability analysis reports and incident information to gauge the risk level associated with our third parties. A significant drop in a Security Scorecard score, a privacy breach or a security incident will trigger a follow up risk assessment or other remediation activities.

SOC 1 Reports

We currently require a SSAE 18 SOC 1 (formerly SAS 70) report from key subcontractors. We review new subcontractor relationships and evaluate their services/functions to determine if a SSAE 18 SOC 1 report should be a contractual requirement. If a SSAE 18 SOC 1 report is required, we obtain the report upon its completion for our review. We also review subcontractor relationships to determine if a SSAE 18 SOC 2 report for systems integrity issues should be a contractual requirement.

We affirm that we are responsible for the performance of the outsourced operations provided by subservice organizations including ensuring that subservice organizations operate in accordance with both our standards and in accordance with the applicable governing master agreement. We annually review the quality of the outsourced operations by various methods including review of subservice organizations' Service Organization Control (SOC) reports, independent auditing and monitoring, and regular meetings to discuss performance. Although we cannot share the specific details of these efforts, the assigned Relationship Manager (RM) for each subservice organization is responsible for reviewing their subservice organization's SOC 1 reports to ensure the services provided are adequately covered by the SOC 1 report. In the event there are exceptions identified in the SOC 1 report, the RMs assess both the exceptions to determine any impacts to the contracted services and the need for additional controls to mitigate any risks identified. In addition, the RMs follow-up with the subservice organizations on a regular cadence to ensure mitigation efforts to address the exceptions are in process and implemented. We have included a copy of our SOC2 report in our submission.

ATTACHMENT H: HIPAA QUESTIONNAIRE**Emergency/Contingency Plans**

4. 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).
-

The Recovery Management Plan (RMP) is the high-level plan for the recovery of data centers and their critical components. The plan is derived from detailed IT infrastructure plans which are maintained by each critical support area. The plan contains processes and procedures to recover all functions, services, and equipment which are needed to continue operations at each facility.

Application Disaster Recovery plans document:

- Technical and management contacts
- Application recovery specifics
- Application dependencies
- Integrated system synchronization
- Validation procedures

We maintain the plans routinely and use automated recovery processes to insure appropriate data resilience. These Disaster Recovery Plans are validated annually.

All Disaster Recovery plans are centrally maintained by our disaster recovery group, stored offsite and updated annual or as needed by the respective infrastructure areas.

Escalation and notification procedures are contained within these Disaster Recovery plans to ensure recovery team members, affected partners and business unit owners are activated in a timely manner.

- 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.
-

There have been no incidents that have occurred within the last two years that has required activating the disaster recovery plan.

ATTACHMENT H: HIPAA QUESTIONNAIRE

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

Keeping with our commitment to providing the highest quality of service to our customers, we have developed a comprehensive Business Continuity Management (BCM) Program to manage business disruptions.

The mission and purpose of the BCM Program is to:

- Improve our resiliency against any disruption of services
- Ensure we can deliver services to our customers during events that negatively impact operations
- Provide a defined framework to identify critical operations, associated risks and impacts and develop appropriate recovery strategies
- Validate plan strategies and capabilities through testing and maintenance

The BCM Program is responsible for:

- Determining the company's objectives and statutory duties based on the organization's operating environment with regards to business continuity
- Identifying activities, assets and resources, and their respective criticality to the business that may comprise business operations
- Setting and documenting the business continuity responsibilities of the organization, based on Management directives
- Maintaining the Business Continuity Policy, standards, and technical controls for the organization, including the review of policy and standards on a regular basis
- Determining and supporting proper methodologies and processes for business continuity

ATTACHMENT H: HIPAA QUESTIONNAIRE

- Communicating business continuity responsibilities including a formal training and awareness program in accordance with the applicable program requirements and maintaining the records
 - Maintaining the Business Continuity Management (BCM) program including regular program reviews, updates to documentation and associated procedures
 - Implementing a program to exercise and test business continuity procedures and crisis management plans on a regular basis
 - Implementing performance objectives depending up on the results of the hazard identification, risk assessment, and business impact analysis to address both short-term and long-term needs defined by the organization
-

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

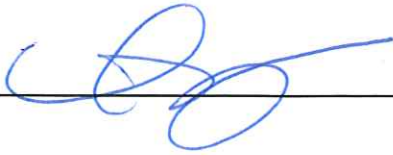
The plan was activated on February 2, 2021, due to Winter Storm Orlena causing power outages and office closures in the Northeast. The department was able to utilize cross trained staff to reprioritize and transfer work to unaffected colleagues. Due to colleagues being cross trained and geographically dispersed, the teams were able to mitigate risks to the business, colleagues, assets, and member service.

ATTACHMENT H: HIPAA QUESTIONNAIRE

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

Tami Polsonetti

Name (Type)



Signature

9/20/22

Date

ATTACHMENT I: NONDISCLOSURE AGREEMENT

By signing and returning this document, Vendor (*insert company name* Aetna Life Insurance Company), 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 SHPContracting@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.

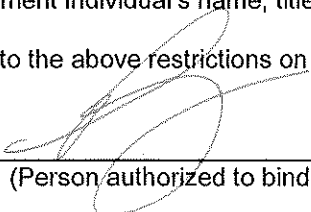
Name: Craig Baker

Title: Proposal Consultant

Email: bakerc5@aetna.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)