

2. AMENDMENT/MODIFICATION NO. P00001	3. EFFECTIVE DATE See Block 16C	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
6. ISSUED BY HHS/HRSA/OO/OAMP Office of Acquisition Management and Policy 5600 Fishers Lane, Rm 14W26B Rockville MD 20857	CODE OAMP	7. ADMINISTERED BY (If other than Item 6) HHS/HRSA/OO/OAMP Office of Acquisition Management and Policy 5600 Fishers Lane, Room 14W26B Rockville MD 20857	CODE OAMP

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) UNITED HEALTHCARE SERVICES, INC. 148892 Attn: NANETTE SADUSKE UNITED HEALTHCARE SERVICES, INC. 9900 BREN RD E MN008 MINNETONKA MN 553439664	(x)	9A. AMENDMENT OF SOLICITATION NO.
		9B. DATED (SEE ITEM 11)
	x	10A. MODIFICATION OF CONTRACT/ORDER NO. 75R60220C00005
		10B. DATED (SEE ITEM 13) 04/16/2020
CODE 148892	FACILITY CODE	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended. is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

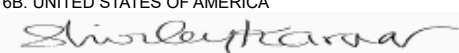
CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
Tax ID Number: 41-1289245
DUNS Number: 071778674
Title: Testing and Treatment COVID-19
Unique ID#: IOA181_C_3404

The purpose of this no cost modification is to change the Contracting Officer Representative (COR) from Robyn Ashton to Dina Passman.

Continued ...
Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) SHIRLEY KARVER
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED
	16B. UNITED STATES OF AMERICA  (Signature of Contracting Officer)
	16C. DATE SIGNED 01/12/2021

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00001

PAGE OF
2 2

NAME OF OFFEROR OR CONTRACTOR
UNITED HEALTHCARE SERVICES, INC. 148892

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Payment: FISCAL U.S. Department of Health and Human Program Support Center 7700 Wisconsin Ave; Suite 9000 BETHESDA MD 20814 Period of Performance: 04/16/2020 to 04/15/2021 Contracting Office Point of Contact: Russell Grabill Email: rgrabill@hrsa.gov Contracting Officer Representative (COR): Dina Passman Email: dpassman@hrsa.gov				

Performance Work Statement (PWS)
**COVID-19 Claims Reimbursement to Health
Care Providers
For Testing and Treating the Uninsured**
Dated: March 16, 2021

I. Background

In December 2019, a novel (new) coronavirus known as SARS-CoV-2-) was first detected in Wuhan, Hubei Province, People's Republic of China, causing outbreaks of the coronavirus disease COVID-19 that has now spread globally. The Secretary of U.S. Department of Health and Human Services (HHS) declared a public health emergency on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), in response to COVID-19. The Federal Government, along with State and local governments, has taken preventive and proactive measures to slow the spread of the virus and treat those affected, including by instituting Federal quarantines for individuals evacuated from foreign nations, issuing a declaration pursuant to section 319F-3 of the Public Health Service Act (42 U.S.C. 247d-6d), and releasing policies to accelerate the acquisition of personal protective equipment and streamline bringing new diagnostic capabilities to laboratories.

On March 11, 2020, the World Health Organization announced that the COVID-19 outbreak can be characterized as a pandemic, as the rates of infection continue to rise in many locations around the world and across the United States. On March 13, 2020, President Donald J. Trump announced and proclaimed that the COVID-19 outbreak in the United States constitutes a national emergency.

On March 18, 2020, the Families First Coronavirus Response Act (FFCRA) (P.L. 116 - 127) became law. The FFCRA responds to the coronavirus outbreak by providing paid sick leave and free coronavirus testing, expanding food assistance and unemployment benefits, and requiring employers to provide additional protections for health care workers, including \$1 billion dollars to be used for testing for the uninsured. On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (P.L. 116 – 136) became law and amended the FFCRA, specifying coverage of diagnostic COVID testing and treatment.

In addition, On April 24, 2020, the Paycheck Protection Program and Health Care Enhancement Act (PPPHCEA) was signed into law. This provides additional funding for COVID-19 testing and related expenses and specifies that up to \$1 billion dollars may be used to cover costs of testing for the uninsured.

In summary, “the COVID-19 Claims Reimbursement to Health Care Providers for Testing and Treating the Uninsured” Program is authorized and appropriated by the following:

- Families First Coronavirus Response Act or FFCRA (P.L. 116-127) and the Paycheck Protection Program and Health Care Enhancement Act or PPPHCEA (P.L. 116-139), which each appropriate \$1 billion to reimburse providers for conducting COVID-19 testing for the uninsured; and the Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136), which provides \$100 billion in relief funds, including to hospitals and other health care providers on the front lines of the COVID-19 response, and the PPPHCEA, which appropriated an additional \$75 billion in relief funds (Provider Relief Fund). Within the Provider Relief Fund, a portion of the funding will be used to support healthcare-related expenses attributable to the treatment of uninsured individuals with COVID-19.

As part of the FFCRA, PPPHCEA, and CARES Act, HHS, HRSA will award a contract to a vendor to provide end-to-end claims reimbursement directly to eligible health care providers, generally at Medicare rates, for testing uninsured individuals for COVID-19 and treating uninsured individuals with a COVID-19 diagnosis. Applicants will agree to accept

reimbursement from the COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured as payment in full and not subsequently balance bill patients. Applicants will attest/certify to eligibility, allowable costs, and availability of records. HRSA will reimburse claims under the COVID-19 Claims Reimbursement for Testing and Treatment to Health Care Providers Serving the Uninsured until all funds are expended.

Funding for claims reimbursement to health care providers will be limited to approximately \$10 Billion for Treatment related claims and \$2 Billion for Testing related claims.

II. Purpose / General Description

The purpose of this contract is to process and distribute claims reimbursement, provide customer service education and outreach, project and program management, compliance and dispute resolution support, provider outreach, and data support for the COVID-19 Claims Reimbursement to Health Care Providers for Testing and Treating the Uninsured Program.

A. The general scope of the contract includes:

1. Project Management
2. Provider Education and Outreach
 - a. Microsite
3. Eligibility and Provider Reimbursement Terms and Conditions Attestations
 - a. Provider Portal
 - b. Patient Eligibility Verification
4. Electronic Claims Intake
 - a. Electronic Data Interchange
5. Claim Adjudication
 - a. General Claims Processing
 - b. Back-End Processing
 - c. Remittance Advice
6. Financial Management and Claims Reimbursements
 - a. Reimbursement System
 - b. Approved Bank Account
 - c. Financial Management and Reporting
 - d. Payment Returns and Recovery
 - e. Remittance Support
7. Provider Call Support
 - a. Call Center
8. IT Services
 - a. Software Quality Control and Systems Development Management Plan

b. Secure Data Transfer

9. Support for Program Operations

- a. Compliance
- b. Research, and Data Support
- c. Records Management
- d. Training

10. Security Requirements

B. Assumptions :

1. The contract shall have the following technical assumptions when developing the Claims Processing Services for COVID-19 Testing and Treatment and Vaccine Administration related services for the Uninsured Patients.

- This is a National contract for providers to submit and receive payment on COVID-19 visits (Evaluation/Management codes-ICD-10 codes) and lab tests for the virus for the uninsured patients. Contractor will validate providers.
- Systems leveraged for this program are hosted by the contractor.
- The payment for the in vitro diagnostic product as well as lab processing cost related to the provision of any FDA approved coronavirus testing will be covered and paid at generally Medicare National Rates with no adjustments based on locality. Healthcare Common Procedure Coding System (HCPCS) shall be used to determine fee for covered services.
- The payment for testing costs related to COVID-19 will be covered and generally paid at Medicare National Rates using the following CMS codes:
 - Z03.818 – Encounter for observation for suspected exposure to other biological agents ruled out (possible exposure to COVID-19).
 - Z20.828 – Contact with and (suspected) exposure to other viral communicable (confirmed exposure to COVID-19).
 - Z11.59 – Encounter for screening for other viral diseases (asymptomatic).
- For antibody testing and testing-related services to be eligible for reimbursement, claims submitted for testing-related visits rendered in an office, urgent care or emergency room or via telehealth setting must include one of the following procedure codes:
 - 86318 – Immunoassay for infectious agent antibody, qualitative or semi-quantitative, single step method (e.g., reagent strip).
 - 86328 – Immunoassay for infectious agent antibody (ies), qualitative or semi-quantitative, single step method (e.g., reagent strip); severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) (coronavirus disease [COVID-19]).

- 86769 – Antibody; severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) (coronavirus disease [COVID-19]).

2. Testing Codes Independent Labs. For testing to be eligible for reimbursement billed by an independent lab, claims submitted must include one of the following diagnosis codes:

- Z03.818 – Encounter for observation for suspected exposure to other biological agents ruled out (possible exposure to COVID-19).
- Z20.828 – Contact with and (suspected) exposure to other viral communicable (confirmed exposure to COVID-19).
- Z11.59 – Encounter for screening for other viral diseases (asymptomatic).

3. In addition, single line item claims for the following procedure codes with any diagnosis will also be eligible for reimbursement:

- COVID-19 tests: U0001, U0002, U0003, U0004, 87635.
- Antibody tests: 86318, 86328, 86769.
- Specimen collection: G2023, G2024.

4. For services related to treatment to be eligible for reimbursement, claims submitted must meet the following criteria:

- The COVID-19 diagnosis code must be the primary diagnosis code submitted. The only exception is for pregnancy (O98.5-), when the COVID-19 code may be listed as secondary.
- COVID-19 diagnosis code for dates of service or dates of discharge prior to April 1, 2020 (see recent guidance (<https://www.cms.gov/files/document/MM11764.pdf>) for additional information):
 - B97.29 – Other coronavirus as the cause of diseases classified elsewhere COVID-19 diagnosis codes.
 - COVID-19 diagnosis code for dates of service or dates of discharge on or after April 1, 2020:
 - U07.1 – 2019-nCoV acute respiratory disease.
- Additional codes may be added for reimbursement after discussion and approval by HRSA policy team. Contractor will not be validating that an order for or administration of an in vitro diagnostic product was made in order to process the claim for the health care provider office visit, urgent care center visit, or emergency room visit.
- For Office visits (in-person and telehealth), emergency room, urgent care visits, payments will be made to providers based on the Medicare Physician Fee Schedule National Medicare amount for Evaluation and Management Healthcare Common Procedure Coding System (HCPCS) codes, with no adjustments based on locality.

5. Once COVID 19 vaccines are authorized or licensed by the FDA, vaccine administration, for which codes have yet to be identified, will be covered by this program.

- There may be no numeric patient identifier submitted therefore, insurance status (uninsured) will not be validated or verified. But provider attestation will be required.
- An overpayment recovery process that will begin 1 year after the contract begins.
- Utilization thresholds shall be discussed with HRSA to identify potential outliers for the number of services per provider per day through a post-payment analytics.
- The website address may be <https://www.hrsa.gov/CovidUninsuredClaim> pending availability and registration with .gov.
- Patient Verification Assumptions for Claims.
- Required fields for electronic data interchange (EDI) and Paper claims (claims will be rejected/returned without these fields populated) – will be used for patient verification demographics.
- Required fields for electronic data interchange (EDI) and Paper claims (claims will be rejected/returned without these fields populated) – will be used for patient verification demographics.
- Temporary Member ID provided as a result of healthcare provider attestation,
 - Name (First & Last).
 - Date of Birth.
 - Gender.
 - Patient Account Number.
 - Date of Service.
- The providers shall also provide in the claims submission.
 - Last 4 digits of the patient's SSN if the provider has it.
 - Middle Initial/Name.
 - Address.
 - Patient date of birth.
- Provider Verification Assumptions Contact center will ask for the following to validate providers who call into the call center.
 - Name (First & Last).
 - NPI.
 - TIN.

- Contractor shall not make payments directly to patients.
- Contractor shall not be handling any special claims processing (e.g. adjustments, reconsiderations).
- Handwritten claims will not be accepted for processing.
- EDI files will only receive an Electronic Data Interchange 999 acknowledgement transaction, the Electronic Data Interchange 277CA (claims acknowledgment) shall be generated (Not required by HIPAA).
- One contract ID code will be used for uninsured COVID-19 claims.
- The Electronic Data Interchange 837 Professional transaction will be used to submit EDI claims.
- The Electronic Data Interchange 837 Professional transaction will be used to submit EDI claims.
- Leverage clearinghouses that contract may have existing relationships with to accept electronic data interchange claims, rather than requiring each individual provider to enroll in electronic data interchange directly with contractor.
- Contractor will use contractor bank as the banking entity.

III. Period of Performance / Place of Performance

The period of performance is a base period of 12 months from the effective date of the contract. The place of performance shall primarily be performed at the contractor's facilities, which includes work performed by contractor staff via telework.

IV. Tasks

Task 1 – Records Management

The contractor shall:

Manage and maintain Federal records, including electronic records, ensuing from this contract in accordance with all applicable records management laws and regulations, including but not limited to:

- The Federal Records Act (44 U.S.C. Chapters. 21, 29, 31, 33); 36 CFR,
- 1236.20 “What are appropriate recordkeeping systems for electronic records?”, and
- 1236.22 “What are the additional requirements for managing electronic mail records?”

(<http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36:3.0.10.2.25>);

- NARA Bulletin 2013-02, August 29, 2013, “Guidance on a New Approach to Managing Email Records”

(<https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html>); and
• NARA Bulletin 2010-05 September 08, 2010, “Guidance on Managing Records in Cloud Computing Environments”

(<http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html>).

Managing the records includes, maintaining records to retain functionality and integrity throughout the records’ full lifecycle including: (1) maintenance of links between records and metadata, and (2) categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

Task 2 – Records Management Training

The contractor (and/or subcontractor) shall ensure that all employees having access to (1) Federal information or a Federal information system, or (2) personally identifiable information (PII), complete the HRSA Records Management Training before performing work under this contract, and thereafter completing the annual refresher course during the life of the contract. The training can be requested by emailing the records management team at recordsmanagement3@hrsa.gov. The listing of completed training shall be included in the first progress report. Any revisions to this listing as a result of staffing changes shall be submitted with next required progress report.

Regardless of format, all digital content or communications materials produced as a deliverable under this contract must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities. The contractor is responsible for remediating all deliverables that do not comply with the applicable requirements as set forth below.

HHS guidance regarding accessibility of documents can be found at <http://www.hhs.gov/web/section-508/making-files-accessible/index.html>

Task 3 – Contract Administration

This task details the contractor’s responsibilities for managing the overall contract performance, personnel, project planning, and project scheduling.

Task 3.1 – Program and Project Management

The contractor shall:

- Be responsible for efficient and effective Uninsured Program and Project Management.

- Establish and maintain program and project objectives and priorities consistent with overall program guidance and direction provided by HRSA. Responsibility for overall direction and administrative support for execution of HRSA program guidance for program project work will fall under the direction of the contractor’s Project Manager.

- Establish and maintain the process for the claims reimbursement workflow with an end-to-end process.

- Program Management activities include:
- Management of personnel.
- Establishment of processes and procedures for effective operations and contract management.
- Management of subcontractors as appropriate.
- Establishment of effective communications and reporting procedures with HRSA.
- Financial management of the contract.
- Overall scheduling and resource management to minimize the risk of scheduling conflicts.
- Management of system testing.
- Risk management; document control.
- Other project management tasks necessary to successfully meet or exceed the requirements of this contract.

Task 3.2 – Single Point of Contact

The Contractor shall:

- Provide a single point of contact for the management of all aspects of this contract to the Contracting Officer Representative (COR). The point of contact shall be responsible for ensuring that the services and deliverables required by HHS/HRSA are provided in accordance with the contract.

Task 3.3 – Kickoff Meeting

The Contractor shall:

- Meet with the COR and other HHS/HRSA representatives within two (2) business days of the effective date of the contract (EDOC) to discuss all current activities and the scope of work. One (1) day prior to the kickoff meeting, the contractor shall provide an agenda for the meeting. At the kickoff meeting, the contractor shall discuss project timeline, review scope and assumptions, projects guiding principles, contact information of key personnel, and proposed communication schedule/plan.

- Submit detailed minutes of the meeting to the COR within one (1) week.

- The objectives of the kickoff meeting are to:

1. Initiate the communication process between HHS/HRSA and the contractor.
2. Review scope and assumptions as outlined in the proposal to ensure alignment on the work, deliverables, and outcomes and ensure the contractor understands the expectations of key stakeholders regarding the scope of work and the effort.
3. Review communication approach and ground rules.

Task 3.4 – Update Meetings

The Contractor shall:

- Chair semi-weekly conference calls with the COR and HHS/HRSA representatives,
- Communicate project updates at these semi-weekly conference call meetings, and as requested by the COR. One Ad hoc meeting per month will be scheduled as necessary.

Task 3.5 – Reports

This section identifies the reports the contractor shall provide to meet the performance requirements. The report formats will be agreed upon between the contractor and the COR.

Task 3.5.2 – Weekly Data Files

The Contractor shall:

- Provide a weekly report to the COR due on each Wednesday by 6 PM (Eastern Time). The Weekly Data File Report shall be cumulative and contain key data, such as customer service summary statistics, and reimbursement and return details.

Identified Weekly Data Files:

- Frequency and dollar amount of Testing, Treatment, and Vaccine Administration Found on Claims-Weekly File rolling up Treatment, Testing, and Vaccine Administration by Codes found on Claims.
- Member Rollup-Provider, Member, Treatment, Testing, and Vaccine Administration totals by week.
- Provider Demographic Data-Weekly file for providers, by specialty type) who have submitted claims that week showing their demographics as defined by HRSA.
- Public File Report-Cumulative Report showing all data for Billing Provider at Treatment, Testing, and Vaccine Administration Total.
- White House Report-Cumulative Provider, Member, Treatment, Testing, Vaccine Administration and claim roll- up, to ensure the performance of the Uninsured Program.
- Report on types of visits (for example, hospital, inpatient, etc.) broken down by treatment and testing.
- Report on Coverage types. This shall include carriers and be cumulative.
- A Histogram depicting the number of claims submitted. This shall be cumulative.
- Report on uninsured patient demographics, including different age bands, states and gender.

Task 3.5.3 – Daily Reports

The Contractor shall:

- Provide daily status reports to the COR and Uninsured on claims reimbursement as determined by the COR and outlined in the schedule of deliverables.

Identified Daily Reports:

- Daily Executive Email. This shall provide cumulative daily metrics showing:
 - 1) The status and health of the program.
 - 2) Projected and actual reimbursements for testing, treatment, and vaccination of the uninsured.
 - 3) The number of claims rejected.
 - 4) The number and dollar amount of payment errors.
 - 5) Payment returns.
 - 6) Possible testing, treatment, and vaccine administration requests in the pipeline (10-14 days out).
 - 7) Number of Distinct members (patients) served.
 - 8) Number of distinct providers with claims.
 - 9) Number of validated TINS.

- 10) Number of completed ACH enrollments.
 - 11) Number of submissions without member IDs.
 - 12) Number of members with existing coverage.
 - 13) Heat maps showing Providers paid by city, state, and zip code.
 - 14) Heat maps showing claims reimbursed by Provider state.
 - 15) Heat maps showing uninsured patients' submitted/state population.
 - 16) Heat map showing uninsured patients submitted.
- Heat map showing claims for vaccine reimbursed by Provider state
Heat map showing uninsured vaccinated patients submitted/state population
Heat map showing uninsured vaccinated patients submitted

• Daily Financial Report. This shall provide a daily payment reconciliation report to the Contract COR and the Chief, Budget Execution and Management Branch that includes cumulative reimbursements to providers for “testing” and “treatment” to facilitate the ability of HHS/HRSA to maintain financial control and stay within funding limitations for this program.

Task 3.5.4 – Ad hoc Reports

The Contractor shall:

- Provide one Ad hoc report each month as requested by the COR for the period of performance, that includes one follow-up request, to ensure the performance of the Uninsured Testing and Treatment Program.

Task 3.5.5 – Final Reports

The Contractor shall:

- Submit a final report to the COR 30 days prior to the end of the period of performance memorializing the contractor's scope, role, duties, key challenges, risks, decisions, and solutions, and timeline of events. The timeline of events shall be written as a narrative. This report may be a compendium of other deliverables. Submit a final claims reimbursement reconciliation report to the COR.

Task 3.6 – Communication and Correspondence

The Contractor shall:

- Include the COR on all correspondence with the Government.
- Send all reports and deliverables to the COR and/or CO and designee.
- Include the COR in all teleconferences/meetings with the Government.
- Send any and all requests for changes, such as modifications to the COR and/or CO.

Task 3.7 – Documents

The Contractor shall:

- Develop and submit the following project management documents to the COR:
 - Visual business workflows for the overall process.
 - Claims reimbursement methodology.
 - Provider support (call center) plan.
 - Systems security and privacy artifacts.

Task 4 – Provider and Consumer Outreach and Education (POE)

Task 4.1 – Provider Outreach and Education

The Contractor shall:

- Deliver education to groups or individuals through the most appropriate media channel such as website materials, emails, teleconferences, etc. All communications materials shall be reviewed and approved by the COR and the HRSA Office of Communications (OC). Materials shall display HHS and HRSA branding. Contractor logo may not be included on these materials.
- Leverage HRSA's existing social media channels: Facebook, Instagram, LinkedIn and Twitter. Videos developed by the contractor shall be provided to HRSA to be placed on existing channels. The contractor shall coordinate with HRSA COR and OC on information and education that may need to be disseminated nationally through channels other than the contractor's website. Teleconference or webinars shall be made available on the contractor's website, or conducted using the contractor's available technology or in collaboration with HRSA Office of Information Technology. Source files for video and graphic shall be provided to HRSA at the end of the contract.

Update content on the educational microsite once per week to stay current with changes and updates to the program, including FAQs updates based on feedback being provided by the participants in the program.

- To expedite development and implementation, the contractor may leverage its existing processes and technologies and the contractor's brands may be visible (e.g. bottom of the webpage, contained within webinar technology, visible in email communications). Contractor will take measures to ensure HRSA and HHS logos are prominent and replace contractor's branding with the HRSA/HHS logos when possible.
- Coordinate with staff within the contractor's other business areas (Electronic Data Interchange and the contact center) to promote internal communication and development of provider education needs, including preventing common billing errors.
- Partner with HRSA on how to respond to inquiries received outside of the contact center.

Task 4.4 – Stakeholder Communications

The Contractor shall:

- Coordinate external communications related to the work contained in this PWS with Federal stakeholders and professional associations, which may include targeted email messages.
- Create social media plans and content to address eligible provider concerns in coordination with HHS and subject to HHS approval.
- Develop and maintain social media outreach plan with accompanying graphic images and messages to help inform eligible providers about the program in coordination with the COR and subject to HRSA OC and HHS ASPA approval.

Task 4.4.1 – Respond to Data Requests from Within Federal Government

The Contractor shall:

- Provide data reports (through the designated POC and the COR) to components within Federal Government.
- Notify through the designated POC and the COR if: (1) the data are not collected and/or available; (2) release of the data violates the Privacy Act or applicable laws; (3) the use of the data is not sufficiently valuable to warrant a large scale expenditure of time and effort; or (4) the data and information are otherwise exempted from disclosure under the FOIA, when applicable.
- Data requests from within the Federal government shall be given the highest priority of all data requests.
- Track the number of routine and complex data requests from inside the Government and report this information in the quarterly progress report.

Task 5 – Eligibility and Provider Reimbursement Terms and Conditions Attestations

Task 5.1 – Provider Portal

The Contractor shall:

- Per HRSA guidance and direction, develop, implement and maintain a portal based on program requirements to allow healthcare providers to confirm and/or submit data required for ACH transactions, attest to the terms and conditions of the uninsured testing and treatment program and submit provider and patient rosters for validation to program guidelines.
- Configure the portal so that it can be closed, once funding thresholds are met.
- Maintain the integrity of the original provider records.
- Establish and maintain the process for providers not currently enrolled with contractor to register on the contractor's program portal.
- Establish and maintain process for providers to set up a bank account with contractor's designated bank for electronic reimbursement of claims submissions.

Task 5.2 – Patient Eligibility Verification

The Contractor shall:

- Review Provider Attestation Documents to determine whether the provider submitted the required information. NOTE: The parties agree that the provider and not the contractor is responsible for the accuracy of the information provided.
- Perform prepayment verifications of patients' insurance status.
- For individual(s) (patient(s)) where eligibility is determined, issue temporary member ids for the use of claims submissions and processing.

- Establish and manage a process for reconsideration of eligibility for providers who have received a denial of eligibility based on insurance coverage found for submitted individual(s) (patient(s)).

Task 6 – Electronic Claims Intake and Data Interchange

The Contractor shall:

- Set up an electronic system for eligible providers to submit COVID-19 837 claims for testing and treating uninsured individuals.
- Implement a system of edits at the EDI gateway or where applicable to identify claims not meeting program eligibility or reimbursement guidelines resulting in rejection of non-compliant claims.
- Be able to mask the data extract file to avoid PII intake.
- Establish a reimbursement management system.
- Establish and control reimbursement requests, chain of custody, and money transfer workflow.
- Implement controls to ensure reimbursement transfer accuracy.
- Recommend and establish processes to ensure reimbursement integrity and improve efficiencies.
- Provide a reimbursement system that manages financial transactions, such as:
 - Interface with the bank.
 - Accept wire transfers.
 - Return any returned funds to.
- Disburse claims reimbursements daily, Monday through Friday, with the exception of any Federal Reserve Bank holidays.

Task 7 – Claim Processing

Task 7.1 – Claim Adjudication

The Contractor shall:

- Send provider (including billing agents or clearing houses, acting on behalf of the provider) claims to a collection point that houses preprocessing functionality before entry into the adjudication systems.
- Accept claims that meet eligibility requirements (are for covered services, during established dates of service submitted by eligible provider(s) contain patients that have been submitted via the attestation process and are not reimbursable by other insurance).
- Perform an eligibility verification to ensure that the patient on the claim is not eligible for other insurance.

Task 7.2 – General Claims Processing

The Contractor shall:

- Establish and maintain written process that will be shared with the COR that outlines the contractors claims verification process to ensure that claims are accurate and meet all eligibility requirements as indicated in HHS policies and regulations. To include verification of the following:
 - Appropriate Diagnosis/Code (a COVID-19 diagnosis).
 - Provider Eligibility.
 - Verify the Providers status using the following lists (and other identified sources):
 - Office of Inspector General's List of Excluded Individuals/Entities (LEIE).
 - CMS Preclusion List.
 - Do Not Pay.
 - Notify the COR and appropriate HRSA Team in writing immediately, in the event that a provider that is on either of the above lists has been reimbursed.
 - Submit monthly report to COR that includes providers with claims held due to OIG concerns.
 - Establish and maintain a written retroactive claim verification process that will be used to validate the above information.
 - Patient Eligibility.
 - Verification of Patients Insurance Status.

Task 7.3 – Back-End Processing

The Contractor shall:

- Perform a back-end processing to close out and verify claims payments.

Task 7.4 – Remittance Advice

The Contractor shall:

- Generate timely and accurate payment and delivery of 835 Electronic Remittance Advices (ERAs) and make 835 ERAs available to providers

Task 8 – Financial Management and Claims Reimbursements

Task 8.1 – Claims Reimbursement

The Contractor shall:

- Distribute claim reimbursements to eligible providers based on verified and adjudicated testing and treatment claims submitted through contractor's EDI gateway.
- The reimbursements shall be based on required diagnoses, coding, dates of service, provider and patient information

Providers are required to enable an ACH Account (Optum Pay) part of the Uninsured project to facilitate payment.

- The contractor's Bank shall use this information to make ACH payments to providers who have performed COVID-19 testing or treatment on behalf of uninsured patients.
- Use the approved Wire Transfer Instructions and execute the Wire Transfer Instructions using an FDIC-protected Bank Account ("Bank Account") as described in the TriPartite Agreement among the parties dated April 27, 2020.
- Validate that the funds have been received in the contractor's bank account.

Task 8.2 – Reimbursement System

The Contractor shall:

- Establish and maintain a reimbursement system that shall distribute reimbursements to Healthcare Providers serving the uninsured using its existing systems.
- Send a funding request to the COR and the HRSA Office of Budget and Finance for approval and funds certification daily. The funding requests shall be for the total funds required for claim reimbursement payments pending distribution to providers.
- After receiving confirmation from HRSA's Administrator, HRSA Office of Budget and Finance will review and approve the funding request. HRSA Office of Budget and Finance will process the funding request through UFMS to the Treasury.
- The Treasury will deposit the funds into the bank account per the payment date on the HHS calendar.
- Funding requests shall include the gross payment total for the program, the contractor's legal business name, and the date of the request.
- Identify the reimbursements as "testing" versus "treatment" within 24 business hours of the request so that those specific funds, CANs, and appropriations will be tracked and expended.
- After reimbursements are sent via electronic funds transfer to Healthcare Providers, process any rejections, failed transactions and payment errors arising from the reimbursements and provide this data to the COR within 72 hours, or as soon as possible given the nature of the rejection.
- As determined by the COR or designee, the contractor's Provider Services team shall contact providers to obtain corrected ACH information.

Task 8.3 –Return Payments

The Contractor shall:

- Establish and maintain a process for return of over-payment and other forms of non- acceptance or return by the Providers and submit this process to the COR.

- Implement the agreed upon process.
- Return overpayments returned by healthcare providers to HRSA per Treasury instructions.
- Manage, maintain and report reimbursement over-payments and status of returns through file submission to Uninsured Program Team and COR. Review with Uninsured Program team twice monthly.
- Maintain an auditable system of records for all claims reimbursements.
- Maintain auditable funds control and management of all deposits and transactions.
- Have payment integrity capabilities and use Contractor defined processes to ensure reimbursements are processed accurately and without duplication.

Task 8.4 – Approved Bank Account

The Contractor shall:

- Maintain a bank account capable of processing and managing all financial transactions in accordance with the Tripartite Agreement.
- Establish and Maintain bank account for the Testing and Treatment for the Uninsured Program (the “Bank Account”) with accounting and reporting to reflect the actual testing vs treatment reimbursements.
- Return any and all interest gained on net balances in the account to HRSA via wire transfer on a monthly basis.
- Provide account safeguards, monitoring and access controls to Unrelated Testing and Treatment related financial transactions.
- Use the Bank Account to process and make claims payments.
- Submit a monthly utilization report to the COR to validate the total monthly utilization for the account.
- Coordinate with contractor affiliates to maintain a lockbox to receive payments from providers, if needed.
- Complete, sign, and send a form to HRSA’s Office of Budget and Finance (OBF) and HHS’s Program Support Center (PSC) to establish and maintain a vendor account (also known as supplier site) in the UFMS system that identifies contractor’s bank account. Treasury shall deposit funds into the bank account during each payment cycle.

- Ensure that the bank account maintains a near zero balance unless otherwise approved by the COR and the HRSA Office of Budget and Finance. Non-zero balances may be necessary for managing obligated funds to cover electronic funds payments in process.
- Return surplus funds received from providers to HHS. Returned funds shall include the principal, interest, total amount, total count and allowance.
- Submit a final claims reimbursement reconciliation report to the COR within 2 weeks of the contract close out and return any unobligated funds

Task 8.5 – Financial Management and Reporting

The Contractor shall:

- Provide documentation annually to the HRSA PRF Program Integrity Team for A-123 assessment demonstrating that adequate internal control policies and procedures have been established by the contractor for all financial transactions conducted under this contract.
- Have the required accounting, logical partitions, firewalls, and funds control capabilities to ensure that all Treasury deposits and financial transactions are managed, maintained, and reported separately in a bank account.
- Establish and maintain payment integrity plan that ensures internal contractor controls comply with the A-123 assessment to implement appropriate cost-effective management controls for results-oriented management; assess the adequacy of management controls; identify deficiencies; take corresponding corrective action, and report on management of those controls.

Task 8.5.1 – Financial Accounting System

The Contractor shall:

- Host the financial accounting systems responsible for processing and reimbursing claims.
- Secure routine execution of claims reimbursement files.
- Secure processing and storage of millions of claims reimbursement records.
- Secure reporting and file transfer capabilities.
- Secure interface with other HHS/HRSA internal systems and external systems such as US Treasury.
- Ensure disaster recovery capabilities.
- Operate and maintain the financial accounting system.
- Secure routine execution of claims reimbursement files.
- Secure processing and storage of payment records per HHS/HRSA records retention requirements.

- Secure reporting and file transfer capabilities.
- Secure interface with other internal systems and external systems such as US Treasury; and Disaster recovery capabilities.
- Provide HRSA's Director, Division of Financial Policy and analysis and contract COR with a daily extract of financial data from contractor's financial accounting system.
- Provide a scheduled banking data file(s) as necessary from the financial accounting system that provides details of all financial transactions, commitments, obligations, returns, and originated ACH, re-issued, flagged for stop payment, cashed, etc. with the fields and columns determined by HRSA financial oversight designee.
- Provide a secure file transfer process.
- Coordinate with and provide the approved file structure, data elements, data dictionary, etc. to the HRSA financial oversight designee.
- Reconcile the reimbursement files with the actual reimbursements made for testing and for treatment to ensure the reimbursements can be tied back to the initial funding request and the appropriate Legislation and accounting CANS.

Task 8.5.2 – Accounting System Database

The Contractor shall:

- Manage and operate an accounting system responsible for making payments.
- Secure routine execution of payment files.
- Secure processing and storage of millions of payment records.
- Secure reporting and file transfer capabilities.
- Secure interface with other HHS internal systems and external systems such as US Treasury.
- Ensure disaster recovery capabilities.
- Operate and maintain accounting system.
- Secure routine execution of payment files.
- Secure processing and storage of payment records per HHS records retention requirements.
- Secure reporting and file transfer capabilities.
- Secure interface with other CMS internal systems and external systems such as US Treasury.
- Disaster recovery capabilities.
- Participate in workgroup sessions facilitated by HRSA and collaborate with Integrated Resources Management System (IRMS) vendor to document the technical and business requirements for the IRMS system's connectivity with contractor accounting system.
- Provide a daily incremental extract file from the banking system to HRSA's Director, Division of Financial Policy and Analysis that provides details of all financial reimbursement transactions, including payment date, amount, TIN, customer name, testing amount, treatment amount, and total amount.

- Establish and maintain a trusted and secure file exchange process between UHG and HRSA's IRMS.
- Specifics of the file structure, data elements, data dictionary, etc., to be provided to COR and financial oversight designee after initial kickoff meeting with contractor.

Note: IRMS is financial data warehouse managed by HRSA to collect and store financial commitments, obligations and disbursements, and is used by Agency staff to verify the status and availability of funds, support internal controls testing, and other enterprise risk management activities.

Task 8.5.3 – Claims Reimbursement Files

The Contractor shall:

- Work with COR and HRSA project staff to establish and maintain a standardized reimbursement file format.
- Ensure each claims reimbursement file has an ACH as necessary.
- Track each claims reimbursement file distribution amount, ACH addenda record.
- Review the claims reimbursement file for quality controls.
- Ensure each provider payment has a TIN.

Task 8.5.4 – Reimbursement Requests

The Contractor shall:

- Send a reimbursement request to the COR for approval and funds certification prior to the initiation of a transfer to the contractor's Bank Account.
- The reimbursement requests shall provide the total funds requested. Funds are to initiate transfers to contractor's HRSA Uninsured Testing and Treatment Fund Bank Account. Upon receipt, contractor's bank will release the corresponding ACH reimbursements to health care providers serving the uninsured for COVID-19 claims for testing and treatment services.
- The reimbursement request shall include, the contract number associated with the program, the contractor's legal business name, and the date of the request. Additional documentation to support the claims reimbursement may be requested by the COR

Task 8.5.5 – Patient Verification

The Contractor shall:

- Implement retrospective verification of patients' insurance status 90 days after claim payment to confirm eligibility at the time of claims submission.

Task 8.6 – Payment Returns and Recovery

The Contractor shall:

- Develop and maintain a process to handle funds returned by providers. The contractor will receive the returned funds from the provider, reconcile the funds returned between the treatment and testing funds, and allocate funds back to the testing or treatment account, as appropriate.
- Develop and maintain a process to identify an overpayment to a provider, offset the overpayment against a future claim by the provider of the overpayment, reconcile the recovered overpayment against the treatment and testing funding, and allocate funds back to the treatment or test funding, as appropriate. Submit this process to the COR.
- If testing or treatment funds are exhausted, contractor will identify and send a report of all open overpayment inventory to the COR. HRSA will direct contractor to pursue collection of the overpayment from the eligible provider and return recovered overpayments to HRSA.
- Assist HHS/HRSA in recovering funds from identified providers via offset against future program payments.
- Include an adjustment flag within the daily incremental extract file that identifies the provider, TIN, amount, etc., for all return transactions,

Task 8.7 – FPLP Withholding to Payments

The Contractor shall:

- Ensure that all payments are subjected to FPLP or non-tax debt withholding in accordance with Treasury policy and procedure.
- Construct an extract file of the reimbursement information file including legal business name and TIN.
- Send the extract file to the Treasury to match against the debt database.
- Receive a match file from to the Treasury for any payee with outstanding tax or non-tax debt.
- Offset payment to the payee in accordance with the Treasury withholding requirements and send offset file to the Treasury with the debt amounts withheld.
- Receive an acknowledgement file from the Treasury.
- Forward all FPLP withholdings to the Treasury within 10 business days.
- Ensure that the payment remittance advice is designated with the appropriate reason code for the FPLP withholding.

Task 8.8 – IRS 1099s to Payees

The Contractor shall:

- Prepare and send IRS 1099-MISC, in accordance with IRS regulations (<https://www.irs.gov/newsroom/frequently-asked-questions-about-taxation-of-provider-relief->

payments, no later than January 31st to all payees that received payments during the prior calendar year.

- Send the electronic 1099 file with this information to the IRS in accordance with the IRS reporting deadline.

Task 9 – Provider Call Support

Task 9.1 – Customer Service

The Contractor shall:

- Establish a Customer Service Program to respond to provider inquiries and educate providers about the COVID-19 Claims Reimbursement for Testing and Treatment to Health Care Providers Serving the Uninsured. The contractor's Customer Service Center serves as the primary point of contact with the providers needing Uninsured program support on a day to day basis.
- Provide customer service:
 - Provide Call Center Services from 8:00am to 8:00pm EST to respond to provider telephone inquiries.
 - Establish the infrastructure to adequately support call volume.
 - Respond to provider telephone and email (for off hour inquiries) inquiries promptly, clearly, and accurately.
 - Coordinate HHS/HRSA on response plans for external correspondence.
 - Maintain a high level of provider service and satisfaction through good communication and relationships with providers.
 - Train and prepare call center staff to receive and respond to calls from health care providers regarding testing and treating the uninsured.
- Define FAQ scripts using the available information including talking points and manager talking points, Q&A, train call center staff, and develop a plan to train to interface with the Providers.
- Monitor provider contact centers as needed to ensure satisfactory quality and performance standards are met for all PCC telephone inquiries.
- Provide Federal Telecommunications Services (FTS) lines for toll-free access to the customer support service.
- Meet the requirements for the Americans with Disabilities Act (ADA).
- Develop and update efficient protocols, SOPs, and training manuals for referring, tracking and monitoring user requests. Protocols, SOPs, and training manuals shall be made available to the COR anytime upon request.
- Support eligible provider inquiries related to technical issues, such as Attestation and accessing microsite/portal.
- Establish and maintain a defined internal escalation and issue tracking process with input from HRSA to review and respond to questions and to transfer escalated issue to HRSA to support resolution. Submit this defined process to the COR within 30 days of EDOC.

Task 10 – IT Services

Task 10.1 – Software

The Contractor shall:

- Manage contractor provided software resources and for coordinating with other program systems (e.g. JIRA, etc.) to perform the activities of the COVID-19 Uninsured Program.
- Provide resources to support operations and corrective maintenance of supporting software.
- Provide both emergency and routine system support as needed.
- Ensure all contractor owned contractor operated (COCO) and commercial off the shelf software (COTS) software is maintained, patched, and updated to maintain the security baseline.

Task 10.2 – Software Quality Control and Systems Development Management Plan

The Contractor shall:

- Use its existing systems and processes regarding maintenance and changes to its Software and Systems including processes consistent with FDIC regulations and HITRUST certification.

Task 10.3 – Secure Data Transfer

The Contractor shall:

- Provide a secure method to send and receive sensitive data files, the point of contact for sending and receiving all sensitive files is the COR or COR designee.

Task 11 – Support for Program Operations

Task 11.1 – Compliance

The Contractor shall:

- Adhere to the contractor's code of conduct, as a guide to principles of ethics and integrity, directing acceptable and appropriate business conduct by the company's employees and contractors. The code of conduct establishes expectations of organizational culture that encourages ethical conduct and a commitment to compliance. The code of conduct also establishes the importance for all employees to understand their role in achieving compliance; all employees are accountable to understand the laws, regulations, contractual obligations, and company policies that apply to their specific area.

All contractor employees are required to report suspected or known non-compliance in accordance with company policies and procedures. Contractor employees are required to attest to the code of conduct upon hire and annually thereafter.

- Establish and maintain strategies to ensure that healthcare providers receiving reimbursements submit all required information and complete all attestation actions as required by law and policy per HRSA guidance and direction.
- Provide user and technical support services related to attestation compliance.
- Obtain additional information, as necessary, from appropriate providers to assist in resolving compliance, policy, and program integrity issues.

Task 11.2 – Research and Data Support

The Contractor shall:

- Maintain and improve the integrity and accuracy of the data reported to the Uninsured program. The contractor shall use a secure method to send and receive data.

- Coordinate all reporting, research, data support and data requests through the contractor single point of contact and COR.

- Assist with agreed upon specific projects related to preparation of data files, statistical analysis of research data, and other projects related to research efforts. Assist with agreed upon specific projects related to ad-hoc data requests, data integrity efforts, data extracts, and other data-related projects that support the Uninsured Program.

- Maintain a log of all reports and Ad hoc data requests. The log shall include the requestor, report purpose, request date, delivery date, and any relevant comments/notes. Provide this log electronically to the COR once per month.

- Retain records and documentation of all authorized changes to the data including the HHS/HRSA official who authorized the change, the dates and the details of the data before and after the changes were made for each payment file.

- Identify and reduce duplicate reports and improper report types (e.g., corrections vs. revisions).
- Identify and consolidate multiple reports for the same action.

Task 12 – Baseline Security Requirements

A. Applicability. The requirements herein apply whether the entire contract or order (hereafter “contract”), or portion thereof, includes either or both of the following:

1. Access (Physical or Logical) to Government Information: A contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.

2. Operate a Federal System Containing Information: A contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of “information technology” (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

3. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location per FAR clause 52.239-1, Privacy or Security Safeguards. In addition, if new or unanticipated threats or

hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, within one (1) hour or less, bring the situation to the attention of the other party.

4. Adhere to UnitedHealth Group's policies, procedures, controls, and standards in support of the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

5. Comply with the Privacy Act requirements and tailor FAR clauses as needed.

B. Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, at <https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final> and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality: Low Moderate High

Integrity: Low Moderate High

Availability: Low Moderate High

Overall Risk Level: Low Moderate High

Based on information provided by the ISSO, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

No PII Yes PII

C. Personally Identifiable Information (PII). Per the Office of Management and Budget (OMB) Circular A-130, "PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother's maiden name, biometric records, etc.

PII Confidentiality Impact Level has been determined to be:

Low Moderate High

D. Controlled Unclassified Information (CUI). CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR, part 2002) when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "handling" refers to "any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

1. Marked appropriately;
2. Disclosed to authorized personnel on a Need-To-Know basis;
3. Protected in accordance with HITRUST Certification
4. Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

E. Protection of Sensitive Information. For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with HITRUST Certification.

F. Confidentiality and Nondisclosure of Information. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor officer or employee or any of its subcontractors to whom any HHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information shall be protected in accordance with UnitedHealth Group policies. Unauthorized disclosure of information will be subject to sanction policies and/or governed by the following laws and regulations:

1. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
2. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
3. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

H. Government Websites. All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS).

I. Contract Documentation. The Contractor shall use HRSA-provided templates, forms and other documents to comply with contract deliverables as appropriate.

J. Standard for Encryption. The Contractor (and/or any subcontractor) shall:

1. Comply with the UnitedHealth Group Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.

2. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) in accordance with UnitedHealth Group Standards.

3. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information in accordance with UnitedHealth Group Standards Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

K. Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the HRSA non-disclosure agreement (Attachment C), as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

L. Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) – The Contractor shall assist the HRSA Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

1. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the HRSA SOP or designee with completing a PIA for the system or information within 60 days after completion of the PTA and in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

2. The Contractor shall assist the HRSA SOP or designee in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

M. Training.

1. Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/HRSA Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete HHS/HRSA Information Security Awareness, Privacy, and Records Management training at least annually, during the life of this contract. All provided training shall be compliant with HHS training policies.

2. Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training annually commensurate with their role and responsibilities in accordance with HHS

policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.

3. Training Records. The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS policy. The training records shall be provided to the CO and/or COR within 30 days after contract award and annually thereafter or upon request.

N. Rules of Behavior

1. The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the HHS Information Technology General Rules of Behavior, the HRSA Information Technology Rules of Behavior (included in the HRSA Information Security and Privacy Awareness Training), and any applicable system-level rules of behavior.

2. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least annually thereafter, which may be done as part of annual HRSA Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable.

O. Incident Response

1. FISMA defines an incident as “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

2. A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as “a suspected or confirmed incident involving PII”.

3. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor), the Contractor (and/or any subcontractor) shall:

a. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident

b. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send notifications to affected individuals following specific instructions from the HHS Privacy Incident Response Team (PIRT).

c. Report all suspected and confirmed information security and privacy incidents and breaches to the HRSA Security Operations Center (SOC), COR, CO, HRSA SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than one (1) hour, and consistent with the applicable HRSA and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

- i. Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
- ii. Not include any sensitive information in the subject or body of any reporting e-mail; and
- iii. Encrypt sensitive information in attachments to email, media, etc.

4. Comply with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, HHS, and HRSA incident response policies when handling PII breaches.

5. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

P. Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, Part 1 §1.2.

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR within 14 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 14 days of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

Q. Contract Initiation and Expiration

1. General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements in accordance with UnitedHealth Group Standards to ensure information is appropriately protected from initiation to expiration of the contract.

2. Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

3. Notification. The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within two weeks before an employee stops working under this contract.

4. Contractor Responsibilities. Upon Physical Completion of the Contract. The Contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or HRSA policies.

5. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the HRSA Clearance Form for Separating Employees and Contractors (Form-419) when an employee terminates work under this contract within two weeks days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

R. Contractor Owned Contractor Operated System Security Requirements.

1. Security Assessment and Authorization (SA&A). A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO 30 days prior to the EPLC Operational Readiness Review (ORR). The Contractor shall conduct the SA&A requirements in accordance with HHS IS2P, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (latest revision).

HRSA's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

a. SA&A Package Deliverables - The Contractor (and/or any subcontractor) shall provide an SA&A package within 30 days prior to the ORR to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package:

HITRUST Certification – An active HITRUST Certification to be provided to meet System Security Plan (SSP) and Security Assessment Plan/Report (SAP/SAR) Requirements. • Plan of Action and Milestones (POA&M) – due within 7 days after the Security Control Assessment Report is delivered. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and HRSA policies. All high-risk weaknesses must be mitigated within 30 days and all moderate weaknesses must be mitigated within 180 days from the date weaknesses are formally identified, and documented. HRSA will determine the risk rating of vulnerabilities.

- Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, HRSA may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least quarterly.

- Contingency Plan – due within 120 days prior to the Operational Readiness Review. The Contingency Plan must be developed in accordance with NIST SP 800-34, latest revision, and be consistent with HHS and HRSA policies. The Contractor shall review/update the Contingency Plan at least annually thereafter.

- Contingency Plan Test – due within 60 days of acceptance of the Contingency Plan by the System Owner. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. The Contractor shall conduct a Contingency Plan Test at least annually thereafter.

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with HITRUST. The following are the minimum requirements for ISCM:

- Annual Assessment/Review - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by the agreed upon Authorization to Operate (ATO) date.

- Configuration Management - Use industry standard automated tools, per, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and

process government information. Compliance will be measured using IT assets and configuration baselines prior to the EPLC Operational Readiness Review.

- Vulnerability Management - Use industry standard automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with UnitedHealth Group policy.
- Patching and Vulnerability Remediation - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes:
 - 30 days for Critical and High risk vulnerabilities
 - Critical and High vulnerabilities identified by an application scan are required to be remediated prior to the EPLC ORR.
 - 90 days for Moderate risk vulnerabilities.
 - 180 days for Low risk vulnerabilities.
- Secure Coding - Follow secure coding best practice requirements, the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

3. Government Access for Security Assessment. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:

a. The Government includes the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information,

and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request.

c. Cooperate with inspections, audits, investigations, and reviews.

4. End of Life Compliance. The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO). The contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS End-of-Life Operating Systems, Software, and Applications Policy.

5. Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor. The Contractor (and/or any subcontractor) shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

a. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with UnitedHealth Group standards.

b. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and HHS Minimum Security Configuration Standards;

c. Maintain the latest operating system patch release and anti-virus software definitions;

d. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

S. HHS Privacy and Security Requirements

The Contractor (and/or any subcontractor) shall be responsible for the following privacy and security requirements:

1. HITRUST Compliant ATO. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid HITRUST Certification

a. A security control assessment must be conducted by an approved assessing organization in accordance with HITRUST Requirements

2. Data Jurisdiction. The contractor shall store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS) if so required.

3. Service Level Agreements. The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with HRSA to develop and maintain an SLA.

4. Interconnection Agreement / Memorandum of Agreements. The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements / Understanding in accordance with HHS / HRSA policies.

T. Protection of Information in a Cloud Environment

1. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/HRSA policies.

2. HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS within one (1) business day from request date or within the timeframe specified otherwise. In addition, the data shall be provided at no additional cost to HHS.

3. The Contractor (and/or any subcontractor) shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

4. The disposition of all HHS data shall be at the written direction of HHS/HRSA. This may include documents returned to HHS control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

5. If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements. It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records on individuals.

U. Security Assessment and Authorization (SA&A) Process

1. The Contractor (and/or any subcontractor) shall comply with HITRUST Certification requirements

a. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with UnitedHealth Group policies in support of HHS/HRSA

2. HHS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS exercises this right, the Contractor (and/or any subcontractor) shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but

are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

3. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, all gaps shall be documented and tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the contractor's expense, before HHS issues an ATO.

4. The Contractor (and/or any subcontractor) shall mitigate security risks for which they are responsible, including those identified during SA&A, and continuous monitoring activities. All high risk vulnerabilities must be remediated no later than thirty (30) days from discovery. All moderate risk vulnerabilities must be remediated no later than ninety (90) days from discovery. All low risk vulnerabilities must be remediated no later than one hundred and eighty (180) days from discovery.

5. Revocation of a Cloud Service. HHS/HRSA have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or HRSA may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

V. Reporting and Continuous Monitoring

1. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

2. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis:

- a. Operating system, database, Web application, and network vulnerability scan results.
- b. Updated POA&Ms.

c. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the HRSA System Owner or AO.

d. Any configuration changes to the system and/or system components or CSP's cloud environment that may impact HHS/HRSA's security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

W. Configuration Baseline

1. The contractor shall certify that applications are fully functional and operate correctly as intended on systems using UnitedHealth Group Configuration Standards

The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved configuration baseline.

2. The contractor shall use industry standard validated tools with configuration baseline scanner capability to certify their products operate correctly with UnitedHealth Group Configuration Standards and do not alter these settings.

X. Media Transport

1. The Contractor and its employees shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

2. All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

Y. Boundary Protection, Trusted Internet Connections (TIC)

1. The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes.

2. The contractor shall route all external connections through a TIC.

Task 13 – Transition Out Plan

The Contractor shall:

- Develop and implement a 120-day transition-out plan. The plan shall include:
 - Methodologies and procedures for minimizing disruption of service to qualified eligible providers and major milestones at 30, 60, 90, and 120 days post contract end date (for a 120 day transition).
 - Support phases to allow collaboration with the outgoing contractor.

- Develop a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees.
- Work with any future contractor(s) and HHS/HRSA to facilitate complete operational transition, and this must be addressed in the transition plan.
- Data captured during the performance of the base and optional periods will be transferred to the government at contract conclusion; the format to deliver the data shall be decided during the performance period. However, the transition materials will not include UHG proprietary or competitively sensitive information regarding its information, data, systems and processes used to execute this contract.
 - This transition plan is predicated on the incoming contractor being available on day one to shadow UHG staff, be available for all knowledge transfer meetings, and ensure that their staffing is complete at the end of the transition period. UHG is not responsible for the incoming contractor's performance during transition.

V. Schedule of Deliverables

The contractor shall ensure all products and services delivered under this contract are compliant with Section 508 in accordance with the Health and Human Services Acquisition Regulation (HHSAR). These Section 508 Standards were issued by the United States Access Board (<https://www.access-board.gov/>) and published in the Federal Register, on January 18, 2017, as the final rule (<https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule>). The final rule updates the Section 508 Standards along with accessibility guidelines for telecommunication products and equipment covered by section 255 of the Communications Act.

The Section 508 Standards applicable to this contract are:

Section 508 Standards and Guidelines (<https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>).

- Web Content Accessibility Guidelines (WCAG) 2.0.
- Success Criteria, Level A and AA.
- Chapter 3: Functional Performance Criteria (FPC).
- Chapter 4: Hardware (If Applicable).
- Chapter 5: Software.
- Chapter 6: Support Documentation and Services.

Regardless of format, all digital content or communications materials produced as a deliverable under this contract must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities. The contractor is responsible for remediating all deliverables that do not comply with the applicable requirements as set forth below.

HHS guidance regarding accessibility of documents can be found at <http://www.hhs.gov/web/section-508/making-files-accessible/index.html>.
ICT vs. EIT

Procurement documentation from HHS or other agencies may contain references to "EIT" (Electronic and Information Technology) and "ICT" (Information and Communications Technology). HHS considers these terms to be interchangeable, and "EIT" should always be interpreted to be "ICT" in any HHS procurement.

Item	Description	Quantity	Due Date	Format	Submit To
4	Claims Reimbursement Workflow.	1	Prior to Contract Kickoff Meeting	Electronic Format	Email to COR
6	Kickoff Meeting Agenda.	1	One (1) Day Prior To Kickoff Meeting.	Electronic Format	Email to COR.
7	Kickoff Meeting Minutes.	1	One (1) Week After Kickoff Meeting.	Electronic Format	Email to COR.
8	Semi-weekly Meeting Agendas.	104	Two (2) Times A Week	Electronic Format	Email to COR
11	Weekly Reports.	52	Each Wednesday by 6PM EST,	Electronic Format	Email to COR
12	Daily Executive Email.	262	Daily (weekdays)	Electronic Format	Email to COR
13	Daily Financial Report.	262	Daily (weekdays)	Electronic Format	Email to COR and the Chief, Budget Execution and Management Branch
14	Ad hoc Reports.	12	As Requested	Electronic Format	Email to COR
15	Final Report.	1	Thirty (30) Days Prior to the End of the	Electronic Format	Email to COR
17	Website Content.	Within Fifteen (15) days After Award of Contract and as Requested		Electronic Format	COR
19	Social Media Plan.	1 Within Thirty (30) Days After Award of Contract.		Electronic Format	Email to COR
26	Claims Verification Process.	1 Within 5 Days of After Award of Contract		Electronic Format	Email to COR
27	Claims Held Report	1 Monthly 2		Electronic format	Email to COR

29	Reimbursement Submissions	2 Daily (weekdays) 6 2	Electronic Format	Email to COR and HRSA Office of Budget and Finance
30	Reimbursement Return Payments - Process Report.	1 Prior to Contract term	Electronic Format	Email to COR
31	Approved Bank Account Monthly Utilization Reports.	1 Monthly 2	Electronic Format	Email to COR
32	HHS/HRSA Form to Establish A Vendor Account.	1 Within Five (5) Days After Award of Contract	Electronic Format	Email to HRSA's OBF and PSC
33	Submit a final claims reimbursement reconciliation report and return any unobligated funds.	1 Within Two (2) Weeks of Contract Closeout	Electronic Format	Email to COR
34	Financial Management and Reporting Documentation.	1 Annually	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
35	Daily Extract of Financial Data Report.	2 Daily (weekdays) 6 2	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis

36	Daily Incremental Extract File.	2 6 2	Daily (weekdays)	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
37	Specifics of the file structure, data elements, data dictionary.	1	Within 90 days of contract kickoff	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
38	Claims Reimbursement File formats.	1	Within 90 days of contract kickoff	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
39	Claims Reimbursement Files, returned funds. Reports.	1			COR and Director, Division of Financial Policy and Analysis
41	Process to identify and offset an overpayment to a provider.	1	prior to contract term	Electronic Format	Email to COR
42	Funds Exhausted Submissions.		When Funding is Exhausted	Electronic Format	Email to COR
43	FPLP Withholding to Payments Submissions.	1	Annually	Electronic Format	Email to Treasury
46	Contractor Non-Disclosure Agreements.	1	Prior To Contractor Performance	Electronic Format	Email to COR

47	Incident Response.	As Required	Electronic Format	Email to HRSA Security Operations (SOC), CO, COR, HRSA SOP (or His or Her Designee) and Other Stakeholders
52	Transition Out Plan.	1 30 Days Prior to the End of Contract Performance	Electronic Format	Email to COR

With the exception of daily reports and data files, which are accepted upon delivery, the Government will have 5 days to accept or reject the deliverable submitted. To the extent that the Government rejects a deliverable it should specify with particularity the basis for the rejection. The Contractor shall have 3 days to correct and retender rejected deliverables, which will then be deemed final and accepted.

VI. Payment Schedule

This is a Firm Fixed Price contract. Payment for services shall be made after submission of a proper invoice.

The payment schedule will be entered at award.

CLIN	DESCRIPTION	UNIT	QAUNTITY	REMAINING COST	TOTAL ESTIMATED PRICE
001	Claims Reimbursement to Health Care Providers for Testing and Treating the Uninsured Initiative Service Fee	Per Lot	1	\$11,900,000	\$15,000,000

Attachment B – PWS Assumptions

The Assumptions below are applicable to the PWS Articles and Tasks set forth in the heading above each assumption.

1. Section II. B. Assumptions:

The situation around COVID-19 is highly dynamic, evolving rapidly, and has been subject to significant uncertainty. The Government acknowledges that the Contractor executed the services it provided on expedited timelines to meet urgent and compelling Government needs. The Government is responsible to review and approve or concur with Contractor's work, including providing the methodologies and approaches for the Contractor to carry out the services provided and/or contemplated. In order to complete the services requested, the Contractor will rely on the Government's timely cooperation, including the Government making available relevant data, information and personnel; performing any tasks or responsibilities assigned to the Government; and notifying the Contractor of any issues or concerns that the Government may have relating to the services provided.

The parties acknowledge and agree that the Government is responsible for the cost of payments that Contractor makes to health care providers under the Contract.

2. Section II. B. 5. Once COVID 19 vaccines are authorized or licensed by the FDA, vaccine administration, for which codes have yet to be identified, will be covered by this program.

In accordance with the Authority to Operate (ATO) issued by HHS under this Contract, the Contractor assumes that its use of its Risk Management Framework and operating scope, including the use of the Contractor's incident response system and required notices to the HHS CSIRC to support the work required under this Contract meet any ATO requirements.

3. Section IV. Tasks.

The situation around COVID-19 is highly dynamic, evolving rapidly, and has been subject to significant uncertainty. The Government acknowledges that the Contractor executed the services it provided on expedited timelines to meet urgent and compelling Government needs. The Government is responsible to review and approve or concur with Contractor's work, including providing the methodologies and approaches for the Contractor to carry out the services provided and/or contemplated. In order to complete the services requested, the Contractor will rely on the Government's timely cooperation, including the Government making available relevant data, information and personnel; performing any tasks or responsibilities assigned to the Government; and notifying the Contractor of any issues or concerns that the Government may have relating to the services provided.

The parties acknowledge and agree that the Government is responsible for the cost of payments that Contractor makes to health care providers under the Contract.

4. Section IV. Tasks. Task 1. Records Management.

In order to meet the highly dynamic, rapidly evolving circumstances, and significant uncertainty, the Contractor relied on its existing record keeping, records management and related training programs in the execution of this Contract on the Government's behalf. The Government acknowledges that the Contractor executed the services it provided on expedited timelines to meet urgent and compelling Government needs. Accordingly, Contractor assumes UHG Records Management processes satisfies this task.

5. Section IV. Tasks. Task 2. Records Management Training

In order to meet the highly dynamic, rapidly evolving circumstances, and significant uncertainty, the

Contractor relied on its existing record keeping, records management and related training programs in the distribution of Provider Relief Funding on the Government's behalf. The Government acknowledges that the Contractor executed the services it provided on expedited timelines to meet urgent and compelling Government needs. Accordingly, Contractor assumes existing training satisfies this requirement. In addition, Contractor leads will complete the HHS Records Management training prior to conclusion of the contract and train their teams appropriately.

6. Section IV. Tasks. Task 3.1. Program Management

The Government assumes complete responsibility for the accuracy and sufficiency of the information and data provided to Contractor.

7. Section IV. Tasks. Task 4.4.1. Respond to Data Requests from Within Federal Government

Contractor will provide a monthly OIG Data Extract to the Government (Deliverable 53) that will allow the Government to respond to its' own data requests. Contractor assumes that providing the monthly OIG Data Extract satisfies that requirements of this task.

8. Section IV. Tasks. Task 11.1. Compliance

Contractor assumes that its standard training program for employees, which includes Compliance Training and Code of Conduct Attestation, as well as its HITRUST Certification, satisfies the requirements of this Task.

9. Section IV. Tasks. Task 12. Baseline Security Requirements

In order to meet the highly dynamic, rapidly evolving circumstances, and significant uncertainty, the Contractor relied on its existing systems and security protocols, and training programs to distribute support this Contract on the Government's behalf. The Government acknowledges that the Contractor executed the services it provided on expedited timelines to meet urgent and compelling Government needs. Accordingly, the Government accepts Contractor's systems, record keeping systems and training programs "AS IS" with the understanding that its systems are generally consistent with NIST security protocols except in the area of encryption.

In accordance with the Authority to Operation (ATO) issued by HHS under this Contract, the Contractor assumes that its use of its Risk Management Framework and operating scope, including the use of the Contractor's incident response system and required notices to the HHS CSIRC to support the work required under this Contract meets the Requirements of this Task. Contractor will provide its HITRUST certification to HHS under this Contract.

10. Section IV. Tasks. Task 12.E. Protection of Sensitive Information.

Consistent with its assumption applicable to this Task, the Contractor understands the Government requires encryption that is validated according to FIPS 140-2. Contractor's encryption covers – federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.). Contractor assumes that its security and encryption practices, as documented in its HITRUST and Risk Management Framework is sufficient to meet this requirement.

11. Section IV. Tasks. Task 12.J. Standard for Encryption.

For items 1-3, consistent with its assumption applicable to this Task, the Contractor understands the Government requires encryption that is validated according to FIPS 140-2. Contractor's encryption covers – federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.). Contractor assumes that its security and encryption practices, as documented in its

HITRUST and Risk Management Framework is sufficient to meet this requirement.

12. Section IV. Tasks. Task 12.M. Training.

Consistent with the assumption applicable to all items in this Task, Contractor assumes that its standard training program for employees which includes Compliance Training and Code of Conduct Attestation, as well as its HITRUST Certification, satisfies the requirements of this Task.

13. Section IV. Tasks. Task 12.N. Rules of Behavior.

Consistent with the assumption applicable to all items in this Task, Contractor assumes that its standard training program for employees which includes Compliance Training and Code of Conduct Attestation, as well as its HITRUST Certification, satisfies the requirements of this Task.

14. Section IV. Tasks. Task 12.T. Protection of Information in a Cloud Environment.

Consistent with the assumption applicable to all items in this Task, Contractor assumes that the government accepts Contractor's systems "AS IS" with the understanding that its systems are generally consistent with NIST security protocols except in the area of encryption. In accordance with the Authority to Operation (ATO) issued by HHS under this Contract, the Contractor assumes that its use of its Risk Management Framework and operating scope, including the use of the Contractor's incident response system and required notices to the HHS CSIRC to support the work required under this Contract meet this requirement.

NON-DISCLOSURE AGREEMENT

WHEREAS, the United States Department of Health and Human Services, Health Services and Resources Administration (HRSA) entered into a Contract, dated April 16, 2020, with United HealthCare Services, Inc., on behalf of itself and its affiliates (UHC);

WHEREAS, in advance of the Contract, UHC submitted technical approaches to the solution sought under the Contract.

NOW, THEREFORE, in consideration of UHC's promise to enter into the Contract, UHC agrees not to disclose outside the Government of the United States any information that UHC may learn by viewing or accessing the data file, except as may be required by law and as may be required to perform its duties under the Contract, except UHC will not release any information to any entity not a party to this Agreement unless required by law; and

The parties agree that any information UHC provides in connection with the Contract is considered by UHC to be competitively sensitive, confidential and proprietary business information subject to the protection of the Procurement Integrity Act and exempt from disclosure under the Freedom of Information Act. The information provided by UHC covers documents and discussions exchanged between the parties between April 10, 2020 and April 16, 2020, including its slide deck proposals submitted between April 10, 2020 and April 15, 2020.

This Non-Disclosure Agreement sets forth all of the promises, agreements, conditions, understandings, warranties, and representations between the parties hereto with respect to the subject matter hereof, and there are no promises, agreements, conditions, understandings, warranties, or representations, oral or written, express or implied, between them other than as set forth herein with regard to such subject matter.

This agreement shall be governed by the laws of the United States.

Signed for and on behalf of
United HealthCare Services, Inc.

By



Payman Pezhman
Secretary and Authorized Signatory

Signed for and on behalf of
HRSA

By



Thomas J. Engels
HRSA, Administrator