

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE
PAGE OF PAGES
1 18

2. AMENDMENT/MODIFICATION NO. P00002
3. EFFECTIVE DATE See Block 16C
4. REQUISITION/PURCHASE REQ. NO. HRS274459
5. PROJECT NO. (If applicable)

6. ISSUED BY CODE OAMP
HHS/HRSA/OO/OAMP
Office of Acquisition
Management and Policy
5600 Fishers Lane, Rm 14W26B
Rockville MD 20857
7. ADMINISTERED BY (If other than Item 6) CODE OAMP
HHS/HRSA/OO/OAMP
Office of Acquisition
Management and Policy
5600 Fishers Lane, Room 14W26B
Rockville MD 20857

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
9A. AMENDMENT OF SOLICITATION NO. (x)
9B. DATED (SEE ITEM 11)
10A. MODIFICATION OF CONTRACT/ORDER NO. x
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 Net Increase: \$11,900,000.00

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.
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(d).
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
D. OTHER (Specify type of modification and authority)
X 52.212-4(c) Changes

E. IMPORTANT: Contractor is not is required to sign this document and return 1 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#: OPS184 C 3392
Contract Type: Commercial FFP
The purpose of this modification is to definitize letter contract 75R60220C00005 by incorporating the final Performance Work Statement (PWS), Non-disclosure agreement, and the FAR and HHSAR clauses and additional terms relevant to the finalized contract.

Modification Details:

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)
Daniel Schumacher, President & COO, Optum
16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
SHIRLEY KARVER
15B. CONTRACTOR OFFICER
/s/
(Signature of person authorized to sign)
15C. DATE SIGNED
3/22/2021
16B. UNITED STATES OF AMERICA
/s/
(Signature of Contracting Officer)
16C. DATE SIGNED

Previous edition unusable

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>1. Letter contract 75R60220C00005 is hereby definitized as a Commercial Item Purchase Order for a total firm fixed price amount of \$15,000,000.00. The amount obligated is increased by \$11,900,000.00 from \$3,100,000.00 to \$15,000,000.00.</p> <p>2. The PWS is hereby revised. See attached PWS dated March 16, 2021.</p> <p>3. Non-disclosure agreement is hereby attached. See attached non-disclosure agreement.</p> <p>4. The FAR clauses, HHSAR clauses and additional terms applicable to this contract are as follows:</p> <p>FAR 52.212-4 Contract Terms and Conditions-Commercial Items (Oct 2018) (v) Incorporation by reference is tailored to add the following FAR, HHSAR and commercial terms:</p> <p>I. FAR Clauses:</p> <p>52.202-1 Definitions (Jun 2020) 52.203-5 Covenant Against Contingent Fees (MAY 2014). 52.203-7 Anti-Kickback Procedures (JUN 2020) 52.203-17 Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights (JUNE 2020) 52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation (JAN 2017) 52.204-9 Personal Identity Verification of Contractor Personnel (JAN 2011) 52.204-19 Incorporation by Reference of Representations and Certifications (DEC 2014) 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016) 52.204-22 Alternative Line Item Proposal (JAN 2017) 52.209-12 Certification Regarding Tax Matters (FEB 2016) 52.223-6 Drug-Free Workplace (MAY 2001) 52.224-1 Privacy Act Notification (APR 1984) 52.224-2 Privacy Act (APR 1984) 52.225-25 Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran Representation and Continued ...</p>				

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Certification (JUN 2020)</p> <p>52.232-1 Payments (APR 1984)</p> <p>52.232-9 Limitation on Withholding of Payments (APR 1984)</p> <p>52.232-39 Unenforceability of Unauthorized Obligations (JUN 2013)</p> <p>52.232-40 Providing Accelerated Payments to Small Business Subcontractors (DEC 2013)</p> <p>52.233-2 Service of Protest (SEPT 2006)</p> <p>52.237-3 Continuity of Services (JAN 1991)</p> <p>52.242-13 Bankruptcy (JUL 1995)</p> <p>52.244-5 Competition in Subcontracting (DEC 1996).</p> <p>52.244-6 Subcontracts for Commercial Items (AUG 2019)</p> <p>52.245-1 Government Property (JAN 2017).</p> <p>52.246-25 Limitation of Liability-Services (FEB 1997).</p> <p>52.252-6 Authorized Deviations in Clauses (APR 1984).</p> <p>52.253-1 Computer Generated Forms (JAN 1991).</p> <p>II. HHSAR Clauses:</p> <p>352.224-71 Confidential Information (December 18, 2015)</p> <p>(a) Confidential Information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.</p> <p>(b) Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this contract. The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.</p> <p>(c) Confidential Information or records shall not be disclosed by the Contractor until:</p> <p>(1) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.</p> <p>Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
4 18

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>(2) For information provided by or on behalf of the government,</p> <p>(i) The publication or dissemination of the following types of information are restricted under this contract: See 52.212-4 (v) III. (ii) Government Ownership and Control of All Contract-Related Data.</p> <p>(ii) The reason(s) for restricting the types of information identified in subparagraph (i) is/are: See 52.212-4 (v) III. (ii) Government Ownership and Control of All Contract-Related Data.</p> <p>(iii) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.</p> <p>(d) Whenever the Contractor is uncertain with regard to the confidentiality of or a property interest in information under this contract, the Contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication.</p> <p>The following HHSAR Clauses have been incorporated by reference:</p> <p>The full text of HHSAR provisions or clauses may be accessed electronically at: https://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/index.html</p> <p>HHSAR 352.203-70 Anti-Lobbying (DEC 2015). HHSAR 352.208-70 Printing and Duplication (DEC 2015). HHSAR 352.211-1 Public Accommodations and Commercial Facilities (DEC 2015). HHSAR 352.211-3 Paperwork Reduction Act (DEC 2015). HHSAR 352.224-70 Privacy Act (DEC 2015). HHSAR 352.227-70 Publications and Publicity (DEC 2015). HHSAR 352.231-70 Salary Rate Limitation (DEC 2015). Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
5 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>HHSAR 352.233-71 Litigation and Claims (DEC 2015). HHSAR 352.239-74 Electronic and Information Technology Accessibility (DEC 2015).</p> <p>III. Additional Terms:</p> <p>(i) Organizational Conflict of Interest.</p> <p>General: The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.</p> <p>Disclosure: The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contract or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.</p> <p>Resolution: In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.</p> <p>(ii) Government Ownership and Control of Contract-Related Data:</p> <p>All data furnished by the Government to the Contractor under this contract is deemed to be furnished to the Contractor under this contract by or on behalf of the Government under FAR 52.227-17, Rights in Data-Special Works, which is hereby incorporated by reference in this contract, solely with respect to such data.</p> <p>Except as otherwise provided in this Clause, the Contractor hereby assigns and conveys to the Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
6 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Government all of Contractor's interests (including without limitation all ownership and intellectual property rights interests), in and to Uninsured Provider Submission Data, which consists of data related to testing, treatment or vaccination services rendered by providers to patients that is submitted to Contractor by providers in order to receive payment of uninsured claims. (Collectively "Uninsured Provider Submission Data").</p> <p>For the avoidance of doubt, the Parties agree that all information previously held by the Contractor related to providers and all provider-related information that Contractor obtains outside of this contract, including through enrollment in the Optum Pay system, (collectively, "contractor's previously held information") may continue to be used by the Contractor in the normal course of its operations and that any data collected from providers that was not previously held by the Contractor or that was obtained outside of this contract shall be subject to the terms of the HRSA COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Website Privacy Policy, Terms of Use and the Optum Pay Enrollment Agreement (collectively "Terms") and may be used by the contractor as permitted by the Terms. (https://coviduninsuredclaim.linkhealth.com/).</p> <p>The contractor's previously held information is considered proprietary to the Contractor and will not be delivered to, used by or released to the Government under this contract.</p> <p>For the avoidance of doubt, the Parties further agree that none of Contractor's systems or processes, including its claim adjudication, claims payment and Optum Pay systems and processes, will be delivered to the Government during the performance of this Contract, and that the Government has no right, title or interest in or to such payment processing and adjudication systems and processes.</p> <p>Expectation of confidentiality on all submitted data. Except to the extent such information has already been publicly disclosed, the Government's Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
7 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>expectation is that all Uninsured Provider Submission Data in the possession of the Contractor that was submitted by providers as part of the HRSA COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Website will be kept confidential and not released to any third party unless required by a valid court order or otherwise required by law. Furthermore, upon completion of the contract, except as prohibited by law, the Contractor is to provide the Government all the Uninsured Provider Submission Data collected during the performance of the contract. For the avoidance of doubt, Uninsured Provider Submission Data does not include any of contractor's previously held information.</p> <p>Legal Process. With respect to any legal process from third-parties (including, but not limited to, subpoenas or discovery requests) seeking disclosure of any of contractor's previously held information the Contractor is solely responsible for responding to any such request, and the costs associated with any such response.</p> <p>With respect to any legal process from third-parties (including, but not limited to, subpoenas or discovery requests) seeking disclosure of the Uninsured Provider Submission Data, the Contractor will oppose such legal process seeking discovery on the ground that the U.S. government is the real party in interest and has the sole legal right to possess, control, release, disclose or utilize such Data. Should the United States be substituted as a party in interest, the United States will subsequently defend each such discovery request and legal action at no charge or expense to the Contractor. In each case, unless and until the United States Department of Justice successfully moves to substitute the United States Government as the real party in interest and is able to remove any such action that is in a state court to Federal Court, the Contractor will defend such legal action. Any responses to legal process by Contractor will be treated as within the scope of work under this contract, and such reasonable costs treated in accordance with FAR 31.205-47 Costs related to legal and other proceedings. Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
8 18

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>FAR clause FAR 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders - Commercial Items (MAR 2020) [DEVIATION APR 2020] is hereby revised as follows:</p> <p>52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders - Commercial Items (MAR 2020) [DEVIATION APR 2020]</p> <p>(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:</p> <p>(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).</p> <p>(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).</p> <p>(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a) (1) (A) of Pub. L. 115-232).</p> <p>(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).</p> <p>(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).</p> <p>(6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805note)).</p> <p>(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:</p> <p>XX (1) 52.203-6, Restrictions on Subcontractor Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
9 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).</p> <p>XX (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509)).</p> <p>___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)</p> <p>XX (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).</p> <p>___ (5) [Reserved].</p> <p>XX (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).</p> <p>___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).</p> <p>XX (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Oct 2015) (31 U.S.C. 6101note).</p> <p>XX (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).</p> <p>___ (10) [Reserved].</p> <p>___ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Mar 2020) (15 U.S.C.657a).</p> <p>___ (ii) Alternate I (Mar 2020) of 52.219-3.</p> <p>___ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).</p> <p>___ (ii) Alternate I (Mar 2020) of 52.219-4.</p> <p>___ (13) [Reserved]</p> <p>___ (14) (i) 52.219-6, Notice of Total Small Business Set-Aside (Mar 2020) (15 U.S.C.644).</p> <p>___ (ii) Alternate I (Mar 2020).</p> <p>___ (iii) Alternate II (Nov 2011).</p> <p>___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Mar 2020) (15 U.S.C. 644).</p> <p>___ (ii) Alternate I (Mar 2020) of 52.219-7.</p> <p>___ (iii) Alternate II (Mar 2004) of 52.219-7.</p> <p>XX (16) 52.219-8, Utilization of Small Business Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
10 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Concerns (Oct 2018) (15 U.S.C. 637(d) (2) and (3)).</p> <p>XX (17) (i) 52.219-9, Small Business Subcontracting Plan (Mar 2020) (15 U.S.C. 637(d) (4)).</p> <p>___ (ii) Alternate I (Nov 2016) of 52.219-9.</p> <p>___ (iii) Alternate II (Nov 2016) of 52.219-9.</p> <p>___ (iv) Alternate III (Mar 2020) of 52.219-9.</p> <p>___ (v) Alternate IV (Aug 2018) of 52.219-9.</p> <p>___ (18) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).</p> <p>___ (19) 52.219-14, Limitations on Subcontracting (Mar 2020) (15 U.S.C.637 (a) (14)).</p> <p>XX (20) 52.219-16, Liquidated Damages-Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d) (4) (F) (i)).</p> <p>___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Mar 2020) (15 U.S.C. 657f).</p> <p>XX (22) (i) 52.219-28, Post Award Small Business Program Representation (Mar 2020) (15 U.S.C. 632(a) (2)).</p> <p>___ (ii) Alternate I (MAR 2020) of 52.219-28.</p> <p>___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (15 U.S.C. 637(m)).</p> <p>___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Mar 2020) (15 U.S.C. 637(m)).</p> <p>___ (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).</p> <p>___ (26) 52.219-33, No manufacturer Rule (Mar 2020) (15 U.S.C. 637(a) (17)).</p> <p>XX (27) 52.222-3, Convict Labor (June 2003) (E.O.11755).</p> <p>___ (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2020) (E.O.13126).</p> <p>XX (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).</p> <p>XX (30) (i) 52.222-26, Equal Opportunity (Sept 2016) (E.O.11246).</p> <p>___ (ii) Alternate I (Feb 1999) of 52.222-26.</p> <p>XX (31) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).</p> <p>___ (ii) Alternate I (July 2014) of 52.222-35.</p> <p>XX (32) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29</p> <p>Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
11 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>U.S.C.793).</p> <p>___ (ii) Alternate I (July 2014) of 52.222-36. XX (33) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).</p> <p>XX (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).</p> <p>XX (35) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).</p> <p>___ (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter78 and E.O. 13627).</p> <p>XX (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)</p> <p>___ (37) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c) (3) (A) (ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)</p> <p>___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i) (2) (C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)</p> <p>___ (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).</p> <p>___ (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).</p> <p>___ (40) (i) 52.223-13, Acquisition of EPEAT-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).</p> <p>___ (ii) Alternate I (Oct 2015) of 52.223-13.</p> <p>___ (41) (i) 52.223-14, Acquisition of EPEAT-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).</p> <p>___ (ii) Alternate I (Jun 2014) of 52.223-14.</p> <p>___ (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).</p> <p>___ (43) (i) 52.223-16, Acquisition of EPEAT-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).</p> <p>___ (ii) Alternate I (Jun 2014) of 52.223-16.</p> <p>XX (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
12 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	2011) (E.O. 13513). ___ (45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693). ___ (46) 52.223-21, Foams (Jun 2016) (E.O. 13693). XX (47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a). ___ (ii) Alternate I (Jan 2017) of 52.224-3. ___ (48) 52.225-1, Buy American-Supplies (May 2014) (41 U.S.C. chapter 83). ___ (49) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43). ___ (ii) Alternate I (May 2014) of 52.225-3. ___ (iii) Alternate II (May 2014) of 52.225-3. ___ (iv) Alternate III (May 2014) of 52.225-3. ___ (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note). XX (51) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury). ___ (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; (10 U.S.C. 2302 Note)). ___ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150). ___ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150). ___ (55) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C.4505, 10 U.S.C.2307 (f)). ___ (56) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C.4505, 10 U.S.C.2307 (f)). XX (57) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) (31 U.S.C. 3332). ___ (58) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C.3332). ___ (59) 52.232-36, Payment by Third Party (May Continued ...				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
13 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>2014) (31 U.S.C.3332). XX (60) [52.232-40, Providing Accelerated Payments to Small Business Subcontractors (DEC 2013) (DEVIATION APR 2020) (31 U.S.C. 3903 and 10 U.S.C. 2307). XX (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a). XX (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d) (13)). ___ (63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). ___ (ii) Alternate I (Apr 2003) of 52.247-64. ___ (iii) Alternate II (Feb 2006) of 52.247-64.</p> <p>(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:</p> <p>___ (1) 52.222-17, No displacement of Qualified Workers (May 2014) (E.O. 13495). ___ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67). ___ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67). ___ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67). ___ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67). ___ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67). ___ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67). ___ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015). ___ (9) 52.222-62, Paid Sick Leave Under Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
14 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Executive Order 13706 (Jan 2017) (E.O. 13706). ____ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792).</p> <p>(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records-Negotiation.</p> <p>(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.</p> <p>(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.</p> <p>(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.</p> <p>(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
15 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>flow down any FAR clause, other than those in this paragraph (e) (1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-</p> <p>(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).</p> <p>(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).</p> <p>(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).</p> <p>(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a) (1) (A) of Pub. L. 115-232).</p> <p>(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C.637 (d) (2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.</p> <p>(vi) 52.222-17, No displacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.</p> <p>(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).</p> <p>(viii) 52.222-26, Equal Opportunity (Sept 2015) (E.O.11246).</p> <p>Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
16 18

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

ITEM NO. (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>(ix) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C.4212).</p> <p>(x) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C.793).</p> <p>(xi) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C.4212).</p> <p>(xii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.</p> <p>(xiii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).</p> <p>(xiv) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O 13627).</p> <p>(B) Alternate I (Mar 2015) of 52.222-50(22 U.S.C. chapter 78and E.O 13627).</p> <p>(xv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).</p> <p>(xvi) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).</p> <p>(xvii) 52.222-54, Employment Eligibility Verification (Oct 2015) (E.O. 12989).</p> <p>(xviii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).</p> <p>(xix) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).</p> <p>(xx) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).</p> <p>(B) Alternate I (Jan 2017) of 52.224-3.</p> <p>(xxi) 52.225-26, Contractors Performing Private Continued ...</p>				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
17 18

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).</p> <p>(xxii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.</p> <p>(xxiii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx.1241(b) and 10 U.S.C.2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.</p> <p>(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.</p> <p>Attachments:</p> <p>Attachment A - PWS Attachment B - Non-disclosure Agreement</p> <p>Payment:</p> <p>FISCAL U.S. Department of Health and Human Program Support Center 7700 Wisconsin Ave; Suite 9000 BETHESDA MD 20814</p> <p>Period of Performance: 04/16/2020 to 04/15/2021</p>				
3	<p>Claims Reimbursement for Testing and Treatment to Health Care Providers Serving the Uninsured. Obligated Amount: \$5,950,000.00</p> <p>Accounting Info: 2021.370CO4A.25235 Appr. Yr.: 2021 CAN: 370CO4A Object Class: 25235 Funded: \$5,950,000.00</p>				5,950,000.00
4	<p>Claims Reimbursement for Testing and Treatment to Health Care Providers Serving the Uninsured. Obligated Amount: \$5,950,000.00</p> <p>Continued ...</p>				5,950,000.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
75R60220C00005/P00002

PAGE OF
18 18

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

ITEM NO (A)	SUPPL ES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: 2021.370COVE.25235 Appr. Yr.: 2021 CAN: 370COVE Object Class: 25235 Funded: \$5,950,000.00 Contracting Office Point of Contact: Russell Grabill Email: rgrabill@hrsa.gov Contracting Officer Representative (COR): Dina Passman Email: dpassman@hrsa.gov				

PERFORMANCE WORK STATEMENT

Claims Processing Services for Provider Relief and Protection Fund

April 7, 2020

1. 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 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 27, 2020, the Coronavirus Aid, Relief and Economic Security (CARES) Act (P.L. 116 - 136) became law. The CARES Act provides economic and financial support for individuals and business impacted by the coronavirus outbreak. To provide relief, Congress appropriated funding from the Public Health and Social Services Emergency Fund to reimburse eligible health care providers for health care related expenses or lost revenues that are attributable to coronavirus.

The CARES Act specifies that eligible health care providers are to be reimbursed for health care related expenses or lost revenues that are attributable to coronavirus that have to been reimbursed from other sources or that other sources are obligated to reimburse. Eligible health care providers are public entities, Medicare or Medicaid enrolled suppliers and providers, and other entities the Secretary may specify, that provide diagnoses, testing, or care for individuals with possible or actual cases of COVID-19. The CARES funds can be used to reimburse eligible providers for lost revenues and costs related to the coronavirus outbreak including building or construction of temporary structures, leasing of properties, medical supplies and equipment including personal protective equipment and testing supplies, increased workforce and trainings, emergency operation centers, retrofitting facilities, and surge capacity.

2. PURPOSE/GENERAL DESCRIPTION

HHS will be issuing a contract to process and pay claims from eligible health care providers for reimbursement of health care related expenses or lost revenues that are attributable to coronavirus. The scope of this activity may include:

1. Project Management
 2. Intake Electronic and Paper Claims
-

- a. Electronic Data Interchange
- b. Paper Claim Intake, Scanning, and Optical Character Recognition
3. Claim Adjudication
 - a. Paper Remittance Advice
 - b. General Claims Processing
 - c. Back-End Processing
 - d. Remittance Advice and Explanation of Benefits
4. Provider Customer Service Program
 - a. Education and Outreach
 - b. Call Center
5. Provider Payment and Integrity
6. Security

3. PROBLEM STATEMENT

HHS is establishing a Provider Relief and Protection Fund (PRF). How will providers be reimbursed for health care related expenses or lost revenues that are attributable to coronavirus?

4. PERIOD OF PERFORMANCE/PLACE OF PERFORMANCE

4.1 Period of Performance

Base Period: 12 months from date of award

4.2 Place of Performance

The Contractor shall perform the work under this contract off-site, primarily at the contractor's facilities.

5. Assumptions

Contractor shall consider the following technical assumptions when developing the claims processing services for the PRF Performance Work Statement.

1.1. Assumptions

- This is a National contract for all eligible providers to submit and receive payment on health care related expenses or lost revenues that are attributable to coronavirus.
 - DESCRIBE the DATA that you will use to validate the provider.
- All systems leveraged for this program are hosted XXXXXXXX WHERE DO YOU PLAN TO HOST.
- The PRF will be divided into tranches including a General, Targeted and Reserve Distribution.

- Each distribution method will follow separate eligibility and methodology requirements.
- Under the General Distribution, the contractor will immediately disperse a pre-defined payment amount to Medicare enrolled providers based on a list provided by HHS.
- Contractor will utilize a website to process applications for payment requests from eligible providers not included on the list supplied by HHS who will attest to the terms and conditions for receiving payment from the PRF.
- The website address will be pending availability and registration with .gov.
- Contractor will collect information from providers and perform any necessary validation checks to ensure their eligibility for funds.
- Contractor will receive requests for payment and disperse payment under the Targeted Distribution based on criteria provided by HHS.
- HHS may require an independent Authority to Operate for this system which will not be feasible to execute fully in order to meet the timelines being proposed.
- A provisional ATO may be required in the interim and Contractor will work to address any gaps between existing ATO's and any required for this program
- Contractor will collect among other elements for each eligible provider seeking payment: Provider Name, Address, Tax Identification Number (TIN), Name and location of Financial Institution, Bank Routing Number, and Bank Account Number.
- Contractor will establish a specific call center to technical support and service and payment support for providers.
- Contractor will develop and retain data collection and reporting on specific factors to be determined by HHS including application volume and payment disbursement.
- Comprehensive, daily financial accounting in HHS preferred format.
- Contractor will not be responsible for 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

6. TASKS

The contractor shall perform the following tasks:

Task 1 Project Management

1.1 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's Representative (COR). The point of contact shall be responsible for ensuring that the services and deliverables required by HHS are provided in accordance with the contract.

1.2 Kickoff Meeting

The contractor shall meet with the COR and other HHS 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 provide a draft project management plan and timeline, updated roster of key personnel, a roster of all personnel and roles, signed Non-Disclosure Agreements, and proposed communication schedule/plan. The contractor shall submit detailed minutes of the meeting to the COR within one week.

The objectives of the kickoff meeting are to:

1. Initiate the communication process between HHS and the contractor by introducing key project participants and identifying their roles.
2. Ensure the contractor understands the expectations of key stakeholders regarding the scope of work and the effort described in this contract, including task requirements and objectives.
3. Discuss critical aspects of the Project Management Plan (PMP) and deliverables.
4. Review communication ground rules.
5. Define a roadmap to a successful project.
6. Provide a live demonstration of the system

1.3 Conference Calls

The contractor shall chair weekly/bi-weekly conference calls with the COR and HHS representatives, providing an agenda by 5:00 pm Eastern Time the day prior, and update the agenda with action items and any corrections within 24 hours of the meeting. The contractor shall also provide project updates and ad hoc reports as requested by the COR. Ad hoc meetings will be scheduled as necessary.

1.4 Monthly Status Report

The contractor shall submit monthly progress reports by the 15th of each month to the COR.

1.5 Final Report

The contractor shall submit a final report 30 days prior to the end of the period of performance that includes all project accomplishments and recommendations.

The contractor shall submit a final payment reconciliation report, return unobligated funds to HHS, and close out the bank account.

1.6 Documents

The contractor shall develop and submit the following project management documents to the Contracting Officer's Representative (COR):

- Integrated Project Management Project Management Plan, which include payments and reconciliation activities
- Business requirements documents with visual business workflows for the overall process
- Payment Methodology
- Systems Plan and
- Systems Security and Privacy Artifacts

1.7 Performance and Quality Metrics

The contractor shall work with the COR to develop and implement contractor performance and quality metrics. The COR will evaluate the contractor using these metrics on a quarterly basis. HHS will require frequent updates on total workload volumes and provider payments to ensure that the COVID-19 Testing for Uninsured Reimbursement Program stays within statutory funding limits.

1.8 Requirements

The contractor shall facilitate multiple requirements workshops to

- Provide multiple detailed demonstrations of the Claims processing process with an end to end process.
- Document HRSA requirements for the PRF claims processing
- Discuss and document technical requirements to integrate HRSA's IRMS with EDI, XXX Cost Point
- Demonstrate the System's reporting capabilities and document Reporting and analytics requirements for HRSA w.r.t. claims processing.

Task 2 Intake Electronic and Paper Claims

The Contractor shall:

2.1 Electronic Data Interchange

- Accept COVID-19 837 professional claims for the uninsured from EDI clearinghouses who have an existing Trading Partner ID with the contractor to minimize the number of paper claims to process.
- Establish a new contractor ID which will be used to identify and route claims from clearinghouses to the contractors EDI front-end.
- Upon receipt of the EDI claim file, the trading partner shall be sent an EDI 999

acknowledgment transaction. The 277CA (claims acknowledgment transaction) responses will not be sent.

- Traditional EDI editing, including Common Edit Module edits, will be bypassed.
- Clearinghouses not enrolled with Contractor will be handled by a manual enrollment process as we expect this volume to be very low.

Task 4 Provider Customer Service Program (PCSP)

The contractor shall:

- Establish a Customer Service Program:
Customer service addresses the ability to provide quality services effectively and to increase the overall level of customer service and satisfaction. In support of customer service, the Contractor shall do the following:
 - a) Respond to provider telephone inquiries promptly, clearly, and accurately.
 - b) Provide effective provider education to promote accurate request for payment.
 - c) Maintain a high level of provider service and satisfaction through good communication and relationships with providers.

4.1 Provider Outreach and Education (POE)

- Educate providers about the PRF. POE may be delivered to groups, to individuals and through various media channels at the complete discretion of the Contractor.

4.1.1 Website

- Establish a provider educational website hosted on HTML5 site on the NGS LINUX servers. Initially the site will consist of 3 content items including payment request form requirements, contractor contact information, and FAQs including general information around reimbursement. Contractor shall develop additional FAQs based on inquiries received in the Call Center.
- The primary audience of the website will be the provider community impacted by the coronavirus outbreak. The site shall provide up-to-date information on provider reimbursement under the PRF including links to the CDC and other responsible sources for public health updates. Site content shall follow [Federal plain language guidelines](#).

4.2 Provider Contact Center (PCC)

- Establish and maintain a PCC to support Provider Inquiries regarding the requests for payment processing lost revenues and costs related to the coronavirus outbreak. The PCC shall respond to Provide Inquiries within 48 hours.
- Choose and implement contact center technology that demonstrates innovation and efficiency in providing excellent customer service. The PCC serves as the coordinating centerpiece for developing and managing the relationship with the providers.

4.2.1 Telephone Inquiries

- Respond to provider telephone inquiries in an accurate and consistent manner, from 8:00 a.m. to 8:00 p.m. Eastern Time. All calls shall be answered within XX minutes.
- Report on standard call center metrics such as average handle time, average hold time and average call length.
- Provider contact centers shall monitor a minimum of five (5) calls per Customer Service Representative (CSR) per month for Quality Call Monitoring (QCM) purposes.
- The contractor shall be held accountable to performance standards and quality monitoring for all PCC telephone inquiries.
- Divide telephone inquiry staff into at least two levels of CSRs. First level CSRs shall answer a wide range of basic questions. Second-level CSRs will answer more complex questions.

Task 5 Provider Payment and Integrity

The Contractor shall:

5.1 Payment System

- Provide payment system that manages all financial transactions.

The payment system shall:

- 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;
- Manage, maintain and report check payments;
- Be an auditable system of records for all financial transactions;
- Be capable of auditable funds control and management of all deposits and transactions;
- Have quality assurance and payment integrity capabilities to ensure payments are processed accurately and without duplication;
- Have separate interfaces for transferring files with HHS, the bank, and the Treasury/IRS to process payments, receivables, FPLP, 1099s, and remittance advices; *and*
- Have full and ad hoc reporting capability for all financial transactions and audits, and shall comply with all HHS security requirements.

5.2 Approved Bank Account

- Maintain a bank account capable of processing and managing all financial transactions.
- Sign a Tripartite Agreement with the bank and HHS/HRSA
- Fill out Direct deposit form,
- Create a new supplier account
- Coordinate a monthly banking services utilization report with the bank that details all transactions conducted through the account.
 - The contractor shall use the monthly utilization report to validate the total monthly utilization for the account. The bank shall submit a monthly invoice to HHS/HRSA for

- the total cost of the bank account.
- The bank account shall be non-interest bearing and be restricted to receiving Treasury deposits, accounts payable and accounts receivable, and related financial transactions.
- The contractor shall maintain a lockbox with the bank to receive payments from providers.
- Complete and sign a form that shall be sent to HHS/HRSA to establish a vendor account (also known as supplier site) in the UMFS system that identifies contractor's bank account. The Treasury shall deposit funds into the bank account during each payment cycle; using these funds, the contractor shall disburse payments.
- Ensure that the bank account maintains a near zero balance unless otherwise approved by the COR and the HRSA Office of Budget and Finance.
- Return surplus funds received from providers due to voluntary returns to HHS on a monthly basis. Refunds shall include the principal, interest, total amount, total count and allowance.

5.3 Financial Management and Reporting

- Provide the COR and the HRSA Office of Budget and Finance with financial reports and monthly bank statements.
- Provide documentation to the COR and the HRSA Office of Budget and Finance demonstrating that adequate internal control policies and procedures have been established by the contractor for all financial transactions conducted under this contract.
 - The contractor's internal controls shall comply with the A-123 assessment. As part of the revised Office of Management and Budget (*OMB Circular A-123 Management's Responsibility for Enterprise Risk Management and Internal Controls*), HRSA must take systematic and proactive measures to 1) develop and implement appropriate, cost-effective management controls for results-oriented management; 2) assess the adequacy of management controls in Federal programs and operations; 3) identify deficiencies; 4) take corresponding corrective action, and 5) report annually on management controls.

Given the emergent need and significance of the COVID-19 Program, HRSA will perform testing of internal controls and assess risks to provide management with reasonable assurance of performance and payment integrity.

5.4 Deltek Cost point Database

- Host the Deltek Costpoint system responsible for making payments.
 - Secure routine and ad hoc 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; and
 - Ensure disaster recovery capabilities.
- Operate and maintain the Deltek Costpoint Database.

- Secure routine and ad hoc 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 internal systems and external systems such as US Treasury; and
 - Disaster recovery capabilities.
- The contractor shall participate in workgroup sessions facilitated by HRSA and collaborate with IRMS vendor to document the technical and business requirements for the IRMS system's connectivity with Deltek Costpoint.
 - Provide a daily incremental extract file from the Deltek database that provides details of all financial commitments, obligations, etc., posted to the General Ledger -
 - Either a direct database link from HRSA Integrated Resource Management System (IRMS) to Deltek Costpoint; or through a trusted and secure scheduled extract file process
 - HRSA's IRMS system will connect to the Deltek via database link one time per day on a daily basis in order to query the Deltek
 - Specifics of the file structure, data elements, data dictionary, etc., to be provided after initial kickoff meeting with contractor
 - Ensure compliance with all necessary FISMA security requirements such as Interconnection Security Agreements, Authority to Operate, etc.

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.

5.5 Software Quality Control and Systems Development Management Plan

- Establish a culture and infrastructure that supports the practices needed to produce systems and services that meet requirements and satisfy HHS needs. The contractor's quality improvement program shall include:
 - Procedures and standards for creating quality products from the beginning of the lifecycle process including elements such as:
 - ◆ Clear identification of quality roles, responsibilities and authorities within the organization;
 - ◆ A set of objective (both technical performance and business performance, as well as business impact) criteria to define the overall health of the systems;
 - ◆ Standard activities to review planning, analysis, and design deliverables that define a system; and

- ◆ Practices and tools to verify and validate software release before delivery to HHS.
- Quality control to ensure that project teams follow the standards.
- Ongoing work to improve software quality
 - ◆ Evaluate progress against the defined metrics;
 - ◆ Track and manage the source code quality;
 - ◆ Track functional defects (e.g., defect density) and execute strategies for efficient defect resolution. Recommend improvements for efficiency and effectiveness of the defect resolution process; and
 - ◆ Provide oversight and compliance reporting management for HHS systems under this contract development environment and to manage the process for code promotion.
- Develop a System Development Management Plan (SDMP) that describes its approach to software quality control and managing the software development lifecycle. This is a one-time deliverable that describes the contractor’s approach to software development to include:
 - The contractor’s quality control program (standards, roles, etc.);
 - Requirements management process;
 - Design and architecture process;
 - Source code management (environnements, builds, etc.);
 - Change and configuration management;
 - Verification and validation of sprints and releases before delivery to COR; and
 - Templates for deliverables, including requirements documents and test plans.

5.6 Payment File Format

- Work with HHS/HRSA and designated project staff to develop a standardized payment file format. At a minimum, the file format shall include these payee identifiers, legal business name, Employer Identification Number (EIN)/ Tax Identification Number (TIN), Project ID, date, and amount; additional identifiers may include NPI, CCN, and business address as required by HHS.
- HRSA for review then
- PSC for funding/treasury
- PSC sends stuff to treasury every day, will include in normal transactions each day to treasury

5.7 Payment Files

- Provide HHS with a payment file for each payment cycle that includes the payees, identifiers, and payment amounts for at least five (5) business days prior to the payment submit date on the payment calendar. (file process: To HRSA for review then, PSC for funding/treasury; PSC sends information to treasury every day, will include in normal transactions each day to treasury)
- Submit an expectations report to HHS for all returned payments.
- Scrub payment files against the Do Not Pay list to ensure payments are not deposited into these accounts.
- Notify the COR and HRSA Office of Budget and Finance when payees on the Do Not Pay list are identified on the payment file and these findings shall also be included in the exceptions report.

5.8 Payment Request for Each Payment Cycle

- Send a payment request to the HRSA Office of Budget and Finance for approval and funds certification five (5) business days prior to the submit date during a payment cycle.
 - a. The payment requests shall provide the total funds requested.
 - b. After reviewing and approving the payment request, HRSA Office of Budget and Finance will process the payment request through UFMS to the Treasury. The Treasury will deposit the funds into the bank account per the payment date on the HHS calendar. The payment request from the contractor shall include the gross payment totals for the project, the contractor EIN associated with the project bank account, the contractor's legal business name, and the date of the request. Additional documentation to support the payment may be requested by HHS.
 - c. Due to the potential for unanticipated changes in enrollment such as late entry by participants, incomplete banking information, and other circumstances, HHS shall require the contractor to be capable of completing payment cycles as requested by the contractor.

5.9 FPLP Withholding to Payments

- 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 payment 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.

5.12 IRS 1099s to Payees

- Prepare and send IRS 1099-MISC, in accordance with IRS regulations, 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.

5.13 IRS Backup Withholding

- The contractor shall apply backup withholding to affected payments in compliance with IRS and Treasury laws and regulations.

5.14 Authority to Operate (ATO) and Annual Adaptive Capabilities Testing (ACT)

- Obtain “Application” ATO for the Deltek Costpoint payment system and all contract-related payment and data management systems. HHS will work with the contractor and the HHS Certified Information System Security Officer (CISSO) to establish a schedule for the ATO that meets the program needs.
- Be required to participate in all facets of security testing, prepare security documents, answer questions, and implement recommendations as required by the CISSO to obtain ATO for the payment system application.
- Maintain an ATO by successfully completing all annual HHS security testing requirements needed to process payments. This shall be done in a 3-year cycle, with one-third of the system reviewed annually.

5.16 Overpayment Recovery

- Coordinate with HRSA to development an overpayment program, including: overpayment identification, issuing demand letters, and collections.
- Comply with Federal overpayment rules and regulations.
- Report monthly on overpayments identified and collections.

Task 6 Security Requirements

The contractor shall:

A. Baseline Security Requirements

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

- b. **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.
- 2) **Safeguarding Information and Information Systems.** In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:
- a. Protect government information and information systems in order to ensure:
- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - **Availability**, which means ensuring timely and reliable access to and use of information.
- b. 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. 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.
- c. Adopt and implement the policies, procedures, controls, and standards required by 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.
- d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.
- 3) **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, 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:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Integrity:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> High
Availability:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Overall Risk Level:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> 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

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

- 4) **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: “...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:
- a. marked appropriately;
 - b. disclosed to authorized personnel on a Need-To-Know basis;
 - c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and*

Organizations if handled by internal Contractor system; and

d. 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*.

- 5) **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 OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

See the HHS Standard for the Definition of Sensitive Information, for additional information in defining and protecting sensitive information.

- 6) **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 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 employee or subcontractor 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 HHS and *HRSA* policies. Unauthorized disclosure of information will be subject to the HHS/*HRSA* policies and/or governed by the following laws and regulations:

- a. 18 U.S.C. Section 641 (Criminal Code: Public Money, Property or Records); and
- b. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

- 7) **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
- 8) **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). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not

required, but it is highly recommended.

9) **Contract Documentation.** The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

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

- a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
- b. 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.) with FIPS 140-2 validated encryption solution.
- c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OpDiv-specific encryption standard requirements. 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).
- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR *within thirty days of contract award*.
- e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys <http://csrc.nist.gov/publications/>. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11) **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 OpDiv non-disclosure agreement 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.

12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the OpDiv 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.

- a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the OpDiv SOP or designee with completing a PIA for the system or information within *4-6 weeks or prior to system implementation* 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*.

- b. The Contractor shall assist the OpDiv 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.

B. 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/OpDiv Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete *OS/OASH* 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. A copy of the training records shall be provided to the CO and/or COR within **30 days** after contract award and **annually** thereafter or upon request.

C. 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*.
- 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 OpDiv Information Security Awareness
- 3) Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

D. Incident Response

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) and OASH IRT teams **within 24 hours**, whether the response is positive or negative.

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.

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”.

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

- 1) 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 with FIPS 140-2 validated encryption.

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 *OS/OASH* approved notifications to affected individuals.

- 2) Report all suspected and confirmed information security and privacy incidents and breaches to the OpDiv Incident Response Team (IRT) at 1-866-646-751, csirc@hhs.gov, COR, CO, HHS/OCIO 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 OpDiv 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:

- a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
- b. not include any sensitive information in the subject or body of any reporting e-mail; and
- c. encrypt sensitive information in attachments to email, media, etc.

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

- 3) 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. This may also involve physical access to contractor facilities during a breach/incident investigation.

E. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR).

F. 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*.

For additional information, see HSPD-12 policy at: <https://www.dhs.gov/homeland-security-presidential-directive-12>

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 and/or CO within one week of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within *1 week* 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.

G. Contract Initiation and Expiration

- 1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC framework and methodology in accordance with the HHS

Contract Closeout Guide (2012).

HHS EA requirements may be located here:
<https://www.hhs.gov/ocio/ea/documents/proplans.html>

- 2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
- 3) **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 the 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*.
- 4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within *one week* before an employee stops working under this contract.
- 5) **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 *OS/OASH* policies.
- 6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the *OS/OASH* Contractor Employee Separation Checklist when an employee terminates work under this contract within *14* days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. Records Management and Retention

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/OASH policies and shall not dispose of any records unless authorized by HHS/OASH.

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/OASH policies.

A. Privacy Act

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.

The System of Records Notice (SORN) that is applicable to this contract is: *A SORN will be developed.*

The disposition to be made of the Privacy Act records upon completion of contract performance.

B. Security Requirements for GOCO and COCO Resources

- 1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
- 2) **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 within the specified timeline(s). 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).

For an existing ATO, OpDiv must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such.

OS/OASH 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 *a format/timeline/process as outlined in the project plan* to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package
 - **System Security Plan (SSP)** –The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable

baseline requirements, and other applicable NIST guidance as well as HHS and *OS/OASH* policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least **annually** thereafter.

- **Security Assessment Plan/Report (SAP/SAR)** –The security assessment shall be conducted by *HHS/OCIO* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with ***OS/OASH*** shall *assist* in the assessment of the security controls and update the SAR at least **annually**.

- **Independent Assessment** - The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all “*high*” deficiencies. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).
- **POA&M** – The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. All high-risk weaknesses must be mitigated within *OS/OASH timeframes as agreed and documented within the project management plan* and all medium weaknesses must be mitigated within *OS/OASH timeframes as agreed and documented within the project management plan* from the date the weaknesses are formally identified and documented. *OS/OASH* 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, ***OS/OASH*** may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least **quarterly**.

- **Contingency Plan and Contingency Plan Test** –The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and OpDiv policies. 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. Thereafter, the Contractor shall update and test the Contingency Plan at least **annually**.

- **E-Authentication Questionnaire** – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

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 FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/Pen Test** - 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 (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates.
- **Asset Management** - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least *quarterly by the CSP*. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
- **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, 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 standard HHS and government configuration baselines at least *at least quarterly*. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

- **Vulnerability Management** - Use SCAP-compliant 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 HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least *quarterly*.
 - **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.
 - **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
- 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. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and

portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to 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, but is not limited to, 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. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
 - c. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
 - d. 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 HHS and FIPS 140-2 encryption 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
- e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
 - Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a *monthly* basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

7. OPTIONAL TASKS – Not funded unless is exercised

Optional Task 1 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 (for a 120 day transition). The plan must support phases to allow collaboration with the outgoing contractor. The contractor must also submit a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees. The contractor(s) must also work with any future contractor(s) and HHS to facilitate complete operational transition, and this must be addressed in the transition plan.

- a. The plan shall ensure transition of all providers documenting eligible reimbursement claims to the new contractor responsible for the next phase of the contract with minimal disruption. The plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including, devices, equipment, databases and systems. 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.

7. DELIVERABLES

The contractor shall ensure all products and services delivered under this contract are compliant with HHS Section 508 requirements 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/) (<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) (<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) (<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 HHS 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 identified in the HHS Section 508 checklists

*Performance Work Statement
Claims Processing Services for Provider Relief and Protection Fund*

1.	Develop Payment File Format	4 weeks prior to payment	COR
2.	Develop Control File	4 weeks prior to payment	COR
3.	Conduct File Scrubbing	Each Payment Cycle	COR
4.	Develop Payment Files	Each Payment Cycle	COR
5.	Prepare Payment Request	5 business days prior to submit date	COR
6.	FPLP Offsets Withholding	Each Payment Cycle	COR
7.	Check Files to Bank	Each Payment Cycle	COR
8.	Payment History Report	Monthly	COR
9.	Payment Exception Report	3 business days after payment	COR
10.	Notification of Payment Report	3 business days after payment	COR
11.	Customer Service Help Desk Report	Monthly	COR
12.	IRS 1099s	Annually by January 31st	COR
13.	IRS Backup Withholding	As required	COR
14.	Authority to Operate (ATO)	As required	COR
15.	Quality Assurance Surveillance Plan	A draft is due 2 weeks after award with quarterly updates Updates due by the 5 th day of each quarter.	COR

*Performance Work Statement
Claims Processing Services for Provider Relief and Protection Fund*

		QASP Metrics should be delivered to HRSA along with the monthly contract status report.	
--	--	---	--

*Performance Work Statement
Claims Processing Services for Provider Relief and Protection Fund*

ATTACHMENT A –SAMPLE QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)				
Task Area	Evaluation Measure	Performance Standard/Acceptable Quality Level (AQL)	Method Used	Frequency
All Tasks	Status reporting	Timely information on project status AQL: Submitted timely 97% of time	Inspection	Monthly
	Claims filing and processing	Claims filing and processing time AQL: Reduce by 40%	Inspection	Monthly
	Clean-claim rate	Clean-claim rate AQL: Increase by 9%	Inspection	Annually
	Documentation deliverable	Secure and confidential patient information AQL: 100% patient information is secured and confidential	Inspection	Monthly
	A/R Days	Correct and resubmit claims online AQL: Reduce by 50%	Inspection	Monthly
	Claims	Status of claims AQL: Processed within 30 days of receipt	Report	Monthly
	Duplicate Claims	Detect duplicate claims AQL: Corrected within 30 days	Report	Monthly
	Compliance Issues	Compliance issues AQL: Reduce by 80%	Report	Annually
	Adjudication rates	Increase adjudication rates AQL:	Inspection	Monthly
	Calls Received	Calls answered within 30 seconds AQL: 90%	Report	Monthly
	Emails or Web Inquiries Received	Responded to emails and web inquiries within 24 hours AQL: 90%	Report	Monthly

*Performance Work Statement
Claims Processing Services for Provider Relief and Protection Fund*

	Voicemails Received	Respond to voicemails within 24 hours AQL: 100%	Report	Monthly
	Abandon Call Rate	Number of received calls abandoned AQL: Less Than 3%	Report	Monthly
	Average Customer Satisfaction (As Measured by Post-Call Survey)	Average Customer Satisfaction AQL: Greater Than 90%	Report	Monthly

NOTE: This a sample. QASP submitted with proposal shall be commensurate to Final Performance Work Statement (PWS).

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 its slide deck proposal submitted April 10, 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. Engel
HRSA, Administrator

PERFORMANCE WORK STATEMENT

**COVID-19 Claims Reimbursement for Testing and Treatment to
Health Care Providers Serving the Uninsured**

April 16, 2020

1. 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 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, have taken preventive and proactive measures to slow the spread of the virus and treat those affected, including 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 (FFCR) (P.L. 116 - 127) became law. The FFCR 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. The FFCR provided HHS with \$1 billion from the Public Health and Social Services Emergency Fund (PHSSEF) to allow provider reimbursements for COVID-19 testing-related activities for uninsured patients.

On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116 – 136) became law and amended the Families First Coronavirus Response Act, specifying coverage and pricing of diagnostic coronavirus testing. The CARES Act also provided HHS with \$100 billion under the PHSSEF, to administer a "Provider Relief and Protection Fund" (PRF) to reimburse eligible health care providers for health care related expenses or lost revenues that are attributable to coronavirus. On behalf of HHS, HRSA is administering reimbursement activities for both the COVID-19 testing for the uninsured and PRF resources.

HRSA will coordinate and align COVID-19 testing-related funding and a portion of PRF funding to support provider reimbursement to cover coronavirus-related testing and treatment for the uninsured. HRSA will award a contract to a vendor who will make payments directly to eligible providers beginning in May. Payments will be made on a rolling basis directly to eligible providers for claims that are attributable to testing and treatment of the COVID-19 for uninsured individuals. Applicants will agree to accept reimbursement as payment in full and not subsequently balance bill patients. Applicants will attest/certify to eligibility, allowable costs, and availability of records. HRSA will disburse funds allocated to the "COVID-19 Claims Reimbursement for Testing and Treatment to Health Care Providers Serving the Uninsured" until all funds are expended.

The services covered are as follows:

- *In vitro* diagnostic products (as defined in section 809.3(a) of title 21, Code of Federal Regulations) for the detection of SARS-CoV-2 or the diagnosis of the virus that causes COVID-19 that are approved, cleared, or authorized under section 510(k), 513, 515 or 564 of the Federal Food, Drug, and Cosmetic Act, and the administration of such *in vitro* diagnostic products.
- Items and services furnished to an individual during health care provider office visits (which term in this paragraph includes in-person visits and telehealth visits), urgent care center visits, and emergency room visits that result in an order for or administration of an *in vitro* diagnostic product described in paragraph (1), but only to the extent such items and services relate to the furnishing or administration of such product or to the evaluation of such individual for purposes of determining the need of such individual for such product and to the provision of the test results to the patient if a test was administered.
- Treatment of uninsured individuals for possible or actual cases of COVID-19.

2. PURPOSE/GENERAL DESCRIPTION

HRSA will be issuing a contract to process and pay claims for health care provider office visits and point of care testing, urgent care center visits and point of care testing, emergency room visits and point of care testing, labs, and treatment and any health care entity covered under the Families First Coronavirus Response Act that provides COVID-19 testing, as amended by the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116 – 136), and related medical visits to uninsured patients. In addition, the contract will cover claims reimbursement for treatment for the uninsured, who either have or are presumed to have coronavirus, through the PRF as established in the CARES Act.

The scope of this activity may include:

1. Project Management
2. Intake Electronic and Paper Claims
 - a. Electronic Data Interchange
 - b. Paper Claim Intake, Scanning, and Optical Character Recognition
3. Claim Adjudication
 - a. Paper Remittance Advice
 - b. General Claims Processing
 - c. Back-End Processing
 - d. Remittance Advice and Explanation of Benefits
4. Provider Customer Service Program
 - a. Education and Outreach
 - b. Call Center
5. Provider Payment and Integrity
6. Security

PROBLEM STATEMENT

How will providers be reimbursed for provider office visits and point of care testing, urgent care center visits and point of care testing, emergency room visits and point of care testing, laboratory tests and treatments covered under the Families First Coronavirus Response Act for COVID-19 services for uninsured patients?

How will providers be reimbursed for health care expenses related to the treatment of uninsured patients who either have or are presumed to have coronavirus, as covered under the CARES Act?

3. PERIOD OF PERFORMANCE/PLACE OF PERFORMANCE

3.1 Period of Performance

Base Period: 12 months from date of award

3.2 Place of Performance

The Contractor shall perform the work under this contract off-site, primarily at the contractor's facilities.

4. Assumptions

Contract shall have the following technical assumptions when developing the Claims Processing Services for COVID-19 Testing and treatment related medical visits for the Uninsured Patients.

1.1. Assumptions

- This is a National contract for all 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.
 - DESCRIBE the DATA that you will use to validate the provider.
- All systems leveraged for this program are hosted **XXXXXXXXX WHERE DO YOU PLAN TO HOST.**
- 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 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 treatment costs related to COVID-19 will be covered and paid at Medicare National Rates with no adjustments based on locality using **CMS codes XXX- Codes will need to be added after discussion with 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.*
- HHS may require an independent ATO for this system which will not be feasible to execute fully in order to meet the timelines being proposed.
 - A provisional ATO may be required in the interim and Contractor will work to address any gaps between existing ATO's and any required for 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 post-payment analytics and review
 - The website address may be UninsuredCovidClaims.HRSA.gov 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
 - Health care provider attestation
 - Name (First & Last)
 - Date of Birth
 - Gender
 - Patient Account Number
 - Date of Service
 - Contractor will review patient information against deceased records as a pre-payment activity.
 - 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 ensure that there is benefit coordination before payment.
 - 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
- 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 Optum Bank as the banking entity.

5. TASKS

The contractor shall perform the following tasks:

Task 1 Project Management

1.1 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's Representative (COR). The point of contact shall be responsible for ensuring that the services and deliverables required by HHS are provided in accordance with the contract.

1.2 Kickoff Meeting

The contractor shall meet with the COR and other HHS 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 provide a draft project management plan and timeline, updated roster of key personnel, a roster of all personnel and roles, signed Non-Disclosure Agreements, and proposed communication schedule/plan. The contractor shall submit detailed minutes of the meeting to the COR within one week.

The objectives of the kickoff meeting are to:

1. Initiate the communication process between HHS and the contractor by introducing key project participants and identifying their roles.
2. Ensure the contractor understands the expectations of key stakeholders regarding the scope of work and the effort described in this contract, including task requirements and objectives.
3. Discuss critical aspects of the Project Management Plan (PMP) and deliverables.
4. Review communication ground rules.
5. Define a roadmap to a successful project.
6. Provide a live demonstration of the system

1.3 Conference Calls

The contractor shall chair weekly/bi-weekly conference calls with the COR and HHS representatives, providing an agenda by 5:00 pm Eastern Time the day prior, and update the agenda with action items and any corrections within 24 hours of the meeting. The contractor

shall also provide project updates and ad hoc reports as requested by the COR. Ad hoc meetings will be scheduled as necessary.

1.4 Monthly Status Report

The contractor shall submit monthly progress reports by the 15th of each month to the COR.

1.5 Final Report

The contractor shall submit a final report 30 days prior to the end of the period of performance that includes all project accomplishments and recommendations.

The contractor shall submit a final payment reconciliation report, return unobligated funds to HHS, and close out the bank account.

1.6 Documents

The contractor shall develop and submit the following project management documents to the Contracting Officer's Representative (COR):

- Integrated Project Management Plan, which include payments and reconciliation activities
- Business requirements documents with visual business workflows for the overall process
- Payment Methodology
- Systems Plan
- Systems Security and Privacy Artifacts

1.7 Performance and Quality Metrics

The contractor shall work with the COR to develop and implement contractor performance and quality metrics. The COR will evaluate the contractor using these metrics on a quarterly basis. The contractor will provide HHS frequent updates on the types, quantities, and amount of procedure codes and total provider payments to ensure that the COVID-19 services for the uninsured reimbursement program aligns with appropriated funding streams and stays within the respective statutory funding limits.

1.8 Requirements

The contractor shall facilitate multiple requirements workshops to

- Provide multiple detailed demonstrations of the Claims processing process and contractor system with an end to end process.
- Document HRSA requirements for the COVID-19 claims processing
- Discuss and document technical requirements to establish a daily extract-transform-load (ETL) process from the contractor's accounting system and claims intake system to HRSA's Integrated Resource Management System (IRMS) Demonstrate the contractor system's reporting capabilities and document Reporting and analytics requirements for HRSA w.r.t. claims processing.

Task 2 Intake Electronic and Paper Claims

The Contractor shall:

2.1 Electronic Data Interchange

- Accept COVID-19 837 professional claims for the uninsured from EDI clearinghouses who have an existing Trading Partner ID with the contractor to minimize the number of paper claims to process.
- Establish a new contractor ID which will be used to identify and route claims from clearinghouses to the contractor's EDI front-end.
- Upon receipt of the EDI claim file, the trading partner shall be sent an EDI 999 acknowledgment transaction. The 277CA (claims acknowledgment transaction) responses will not be sent.
- Traditional EDI editing, including Common Edit Module edits, will be bypassed.
- Clearinghouses not enrolled with Contractor will be handled by a manual enrollment process as we expect this volume to be very low.

2.2 Paper Claim Intake, Scanning, and Optical Character Recognition

The contractor shall perform the following:

- Establish a dedicated P.O. Box and dedicated courier delivery to the contractor's Mail and Distribution location.
- Any paper claim received on an incorrect claim form or without the minimum patient information shall be rejected.
- Accepted claims shall be scanned and sent to the contractor's optical character recognition software. Scanned claims shall be reviewed and validated to ensure scanning accuracy and shall be shredded 30 days after validation.

2.3 Claims Intake Data Exchange

The contractor shall:

- Provide claims intake data extract file through EDI to HRSA's Integrated Resource Management System (IRMS) on a daily basis to allow HRSA to capture incoming claims data (including unique patients, unique providers, location of providers, individual claims, and CPT codes). This will allow HRSA to monitor frequency and volume of services rendered to meet anticipated reporting requirements.
- Be able to mask the data extract file to avoid PII intake.
- Create all required reports in contractor system for Claims monitoring, including COVID-19 testing and treatment related visits by service dates, provider, and location, and provide access to authorized HRSA staff.

Task 3 Claim Adjudication

The Contractor shall perform the following:

- Providers (or billing agents and clearinghouses on their behalf) send claims to a collection point that houses preprocessing functionality before entry into the adjudication systems.
- The adjudication system begins processing: claims edits for completeness, and check for duplicative services (benefit coordination).
- The claims that do not fail any edits are then approved for payment.
- Provide a capability in contractor system for HRSA to review the approved Claims
OR
Send the encrypted email version of the approved claims file for HRSA' review and approval.

3.1 General Claims Processing

The contractor shall perform the following:

- Most claims are processed automatically through the adjudication system and are usually resolved without requiring manual intervention on the part of the Contractor.
- Handwritten claims will not be accepted for processing.
- Provide the claims adjudication system to process payment with the exception of special circumstances, such as information on actual or potential duplicate billing.
- However, there will be instances where a claim that is submitted requires manual intervention on the part of the Contractor.
- Process a claim to the point of payment, denial, accurately, usually by operating adjudication system.
- Use optical character recognition (OCR) technology to enter legible paper claim forms unless the quantity of these forms drops to a level where OCR entry is no longer cost effective.
- Manual entry of claims should only be done on an exception basis.

3.2 Back-End Processing

- The contractor shall perform a back-end processing closes out the claim by sending notices to providers, hard copy checks, bank notices and financial data.

3.3 Remittance Advice

The contractor shall perform the following:

- Timely and accurately generate payment and deliver Electronic Remittance Advices (ERAs) to providers or their clearinghouses, billing agents, or other third party agents as directed by providers, and mail paper remittances via the USPS to those providers unable to accept or process ERAs.

Task 4 Provider Customer Service Program (PCSP)

The contractor shall:

- Establish a Customer Service Program:

Customer service addresses the ability to provide quality services effectively and to increase the overall level of customer service and satisfaction. In support of customer service, the Contractor shall do the following:

- a) Respond to provider telephone inquiries promptly, clearly, and accurately.
- b) Provide effective provider education to promote accurate billing.
- c) Maintain a high level of provider service and satisfaction through good communication and relationships with providers.

4.1 Provider Outreach and Education (POE)

- The contractor shall educate providers about the COVID-19 Uninsured Payment Program. POE may be delivered to groups, to individuals and through various media channels at the complete discretion of the Contractor.

4.1.1 Website

- The contractor shall establish a provider educational website, UninsuredCovidClaims.HRSA.gov. Initially the site will consist of 3 content items including claim form requirements, contractor contact information, and FAQs including general information around billing and reimbursement. Contractor shall develop additional FAQs based on inquiries received in the Call Center.
- The primary audience of the website will be the provider community serving the uninsured across the country. The site shall provide up-to-date information on provider billing for COVID-19 related claims for the uninsured and include links to the CDC and other responsible sources for public health updates. Site content shall follow [Federal plain language guidelines](#).

4.1.2 Provider Education

The contractor shall perform the following:

- Education may be delivered to groups or to individuals through the most appropriate media channel such as website materials, 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 may not include their logo on these materials.
- The Contractor shall leverage HRSA's existing social media channels: Facebook, Instagram, LinkedIn and Twitter. Videos developed by the contractor shall be captioned and posted on HRSA's YouTube channel. 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.
- Coordinate with appropriate 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.

4.2 Provider Contact Center (PCC)

The contractor shall:

- Establish and maintain a PCC to support Provider Inquiries regarding the claims or payment processing for COVID-19 Tests, Office Visits and treatment. The PCC shall respond to Provide Inquiries within 48 hours.
- Choose and implement contact center technology that demonstrates innovation and efficiency in providing excellent customer service. The PCC serves as the coordinating centerpiece for developing and managing the relationship with the providers.

4.2.1 Telephone Inquiries

The contractor shall:

- Respond to provider telephone inquiries in an accurate and consistent manner, from 08:00 a.m. to 08:00 p.m. Eastern Time. All calls shall be answered within XX minutes.
- Report on standard call center metrics such as average handle time, average hold time and average call length.
- Monitor provider contact centers to monitor a minimum of five (5) calls per Customer Service Representative (CSR) per month for Quality Call Monitoring (QCM) purposes.
- Be held accountable to performance standards and quality monitoring for all PCC telephone inquiries.
- Divide telephone inquiry staff into at least two levels of CSRs. First level CSRs shall answer a wide range of basic questions. Second-level CSRs will answer more complex questions.

Task 5 Provider Payment and Integrity

5.1 Payment System

The contractor shall:

- Provide payment system that manages all financial transactions.

The payment system shall:

- 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;
- Manage, maintain and report check payments;
- Be an auditable system of records for all financial transactions;
- Be capable of auditable funds control and management of all deposits and transactions;
- Have quality assurance and payment integrity capabilities to ensure payments are processed accurately and without duplication;
- Have separate interfaces for transferring files with HHS, the bank, and the Treasury/IRS to process payments, receivables, FPLP, 1099s, and remittance advices; *and*
- Have full and ad hoc reporting capability for all financial transactions and audits, and shall comply with all HHS security requirements.

5.2 Approved Bank Account

The contractor shall:

- Maintain a bank account capable of processing and managing all financial transactions and paper check payments.
- Sign a Tripartite Agreement with the bank and HHS/HRSA
- Fill out Direct deposit form,
- Create a new supplier account
- Coordinate a monthly banking services utilization report with the bank that details all transactions conducted through the account.
 - The contractor shall use the monthly utilization report to validate the total monthly utilization for the account. The bank shall submit a monthly invoice to HHS/HRSA for the total cost of the bank account.
 - The bank account shall be non-interest bearing and be restricted to receiving Treasury deposits, accounts payable and accounts receivable, and related financial transactions.
 - The contractor shall maintain a lockbox with the bank to receive payments from providers.
- Complete and sign a form that shall be sent to HHS/HRSA to establish a vendor account (also known as supplier site) in the UMFS system that identifies contractor's bank account. The Treasury will deposit funds into. The Treasury shall deposit funds into the bank account during each payment cycle; using these funds, the contractor shall disburse paper check payments.
- 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 outstanding checks.
- Return surplus funds received from providers due to voluntary returns to HHS on a monthly basis. Refunds shall include the principal, interest, total amount, total count and allowance.
 - To issue a refund, the contractor shall submit a new payment request in accordance with Task 5.11-Payment Request for Each Payment Cycle.

5.3 Financial Management and Reporting

The contractor shall:

- Provide the COR and the HRSA Office of Budget and Finance with financial reports and monthly bank statements.
- Provide documentation to the COR and the HRSA Office of Budget and Finance demonstrating that adequate internal control policies and procedures have been established by the contractor for all financial transactions conducted under this contract.
 - The contractor's internal controls shall comply with the A-123 assessment. As part of the revised Office of Management and Budget (*OMB Circular A-123 Management's Responsibility for Enterprise Risk Management and Internal Controls*), HRSA must take systematic and proactive measures to 1) develop and implement appropriate, cost-effective management controls for results-oriented management; 2) assess the adequacy of management controls in Federal programs and operations; 3) identify deficiencies; 4) take corresponding corrective action, and 5) report annually on management controls.

Given the emergent need and significance of the COVID-19 Uninsured Program, HRSA will perform testing of internal controls and assess risks to provide management with reasonable assurance of performance and payment integrity.

5.4 Accounting System Database

The contractor shall:

- Manage and operate an accounting system responsible for making payments.
 - Secure routine and ad hoc 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; and
 - Ensure disaster recovery capabilities.
- Operate and maintain accounting system.
 - Secure routine and ad hoc 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; and
 - Disaster recovery capabilities.
- Participate in workgroup sessions facilitated by HRSA and collaborate with 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 accounting system that provides details of all financial commitments, obligations, etc., posted to the General Ledger -
 - Either a direct database link from HRSA Integrated Resource Management System (IRMS) to the contractor's accounting system; or through a trusted and secure scheduled extract file process
 - HRSA's IRMS system will connect to the accounting system via database link one time per day on a daily basis in order to query the details of financial management activities
 - Specifics of the file structure, data elements, data dictionary, etc., to be provided after initial kickoff meeting with contractor
 - Ensure compliance with all necessary FISMA security requirements such as Interconnection Security Agreements, Authority to Operate, etc.

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.

5.5 Software Quality Control and Systems Development Management Plan

The contractor shall:

- Establish a culture and infrastructure that supports the practices needed to produce systems and services that meet requirements and satisfy HHS needs. The contractor's quality improvement program shall include:
 - Procedures and standards for creating quality products from the beginning of the lifecycle process including elements such as:
 - ◆ Clear identification of quality roles, responsibilities and authorities within the organization;
 - ◆ A set of objective (both technical performance and business performance, as well as business impact) criteria to define the overall health of the systems;
 - ◆ Standard activities to review planning, analysis, and design deliverables that define a system; and
 - ◆ Practices and tools to verify and validate software release before delivery to HHS.
 - Ensure the project teams follow the standards of quality control that.
 - Ongoing work to improve software quality
 - ◆ Evaluate progress against the defined metrics;
 - ◆ Track and manage the source code quality;
 - ◆ Track functional defects (e.g., defect density) and execute strategies for efficient defect resolution. Recommend improvements for efficiency and effectiveness of the defect resolution process; and
 - ◆ Provide oversight and compliance reporting management for HHS systems under this contract development environment and to manage the process for code promotion.
- Develop a System Development Management Plan (SDMP) that describes its approach to software quality control and managing the software development lifecycle. This is a one-time deliverable that describes the contractor's approach to software development to include:
 - The contractor's quality control program (standards, roles, etc.);
 - Requirements management process;
 - Design and architecture process;
 - Source code management (environments, builds, etc.);
 - Change and configuration management;
 - Verification and validation of sprints and releases before delivery to COR; and
 - Templates for deliverables, including requirements documents and test plans.

5.6 Payment File Format

The contractor shall:

- Work with HHS/HRSA and designated project staff to develop a standardized payment file format. At a minimum, the file format shall include these payee identifiers, legal business name, Employer Identification Number (EIN)/ Tax Identification Number (TIN), Project ID, date, and amount; additional identifiers may include NPI, CCN, and business address as required by HHS.
 - HRSA for review
 - PSC for funding/treasury
 - PSC sends stuff to treasury every day, will include in normal transactions each day to treasury

5.7 Payment Files

The contractor shall:

- Provide HHS with a payment file for each payment cycle that includes the payees, identifiers, and payment amounts for at least five (5) business days prior to the payment submit date on the payment calendar. (file process: To HRSA for review then, PSC for funding/treasury; PSC sends information to treasury every day, will include in normal transactions each day to treasury)
- Develop a positive pay check issuance file to be sent to the bank for all checks issue during the payment cycle. The file shall be sent to the bank in a timely manner to ensure that checks presented for payment can be processed against it by the bank.
- Submit an expectations report to HHS for all returned checks.
- Scrub payment files against the Do Not Pay list to ensure payments are not deposited into these accounts.
- Notify the COR and HRSA Office of Budget and Finance when payees on the Do Not Pay list are identified on the payment file and these findings shall also be included in the exceptions report.

5.8 Payment Request for Each Payment Cycle

The Contractor shall:

- Send a payment request to the HRSA Office of Budget and Finance for approval and funds certification five (5) business days prior to the submit date during a payment cycle.
 - a. The payment requests shall provide the total funds requested.
 - b. After reviewing and approving the payment request, HRSA Office of Budget and Finance will process the payment request through UFMS to the Treasury. The Treasury will deposit the funds into the bank account per the payment date on the HHS calendar. The payment request from the contractor shall include the gross

payment totals for the project, the contractor EIN associated with the project bank account, the contractor's legal business name, and the date of the request. Additional documentation to support the payment may be requested by HHS.

- c. Due to the potential for unanticipated changes in enrollment such as late entry by participants, incomplete banking information, and other circumstances, HHS shall require the contractor to be capable of completing payment cycles as requested by the contractor.

5.9 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 payment 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.

5.10 Positive Pay Check Files to the Bank

The contractor shall:

- Send the positive pay check issuance file to the bank.
- Mail the paper checks with the attached remittance advice to the recipient addresses in accordance with the check issuance file.
- Schedule sending the positive paycheck files to the bank to ensure that paper checks can be processed correctly by the bank within 48 hours of the Treasury deposit.
- Only pay issued checks that have been cleared at the bank using best practice procedures with the bank.

5.11 Payment Cycle Reconciliation and Reporting

The contractor shall:

- Reconcile paper check payments using the clears file from the bank that contains the list of all checks that have been processed by the bank.
- Notify HHS that payments have been made and provide information to HHS regarding

any undeliverable checks on the exceptions report. The exceptions report shall be sent to COR and HRSA Office of Budget and Finance on a monthly basis.

- Provide COR and HRSA Office of Budget and Finance with a summarized payment history of all payments.

5.12 IRS 1099s to Payees

The contractor shall:

- Prepare and send IRS 1099-MISC, in accordance with IRS regulations, 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.

5.13 IRS Backup Withholding

- The contractor shall apply backup withholding to affected payments in compliance with IRS and Treasury laws and regulations.

5.15 Patient Verification

The contractor shall:

- Review Provider Attestation Documents
- Review opportunity to do other prepayment verifications
- Use other health information and deceased patient information at the time of service
- Participate in post-pay verification of patients

5.16 Overpayment Recovery

The contractor shall:

- Coordinate with HRSA to development an overpayment program, including: overpayment identification, issuing demand letters, and collections.
- Comply with Federal overpayment rules and regulations.
- Report monthly on overpayments identified and collections.

Task 6 Security Requirements

The contractor shall:

A. Baseline Security Requirements

- 1) **Applicability.** The requirements herein apply whether the entire contract or order (hereafter “contract”), or portion thereof, includes either or both of the following:
 - a. 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.
- b. 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.
- 2) **Safeguarding Information and Information Systems.** In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:
- a. Protect government information and information systems in order to ensure:
- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - **Availability**, which means ensuring timely and reliable access to and use of information.
- b. 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. 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.
- c. Adopt and implement the policies, procedures, controls, and standards required by 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.
- d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.
- 3) **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, 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:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Integrity:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Availability:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High
Overall Risk Level:	<input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> 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

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

- 4) **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: “...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:
- a. marked appropriately;
 - b. disclosed to authorized personnel on a Need-To-Know basis;
 - c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline if handled by a

Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and

- d. 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*.
- 5) **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 OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

See the HHS Standard for the Definition of Sensitive Information, for additional information in defining and protecting sensitive information.

- 6) **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 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 employee or subcontractor 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 HHS and *HRSA* policies. Unauthorized disclosure of information will be subject to the HHS/*HRSA* policies and/or governed by the following laws and regulations:

- a. 18 U.S.C. Section 641 (Criminal Code: Public Money, Property or Records); and
 - b. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
- 7) **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
- 8) **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). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all

times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

9) **Contract Documentation.** The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

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

- a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
- b. 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.) with FIPS 140-2 validated encryption solution.
- c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OpDiv-specific encryption standard requirements. 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).
- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR *within thirty days of contract award*.
- e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys <http://csrc.nist.gov/publications/>. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11) **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 OpDiv non-disclosure agreement 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.

12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the OpDiv 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.

- a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the

OpDiv SOP or designee with completing a PIA for the system or information within *4-6 weeks or prior to system implementation* 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*.

- b. The Contractor shall assist the OpDiv 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.

B. 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/OpDiv Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete *OS/OASH* 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. A copy of the training records shall be provided to the CO and/or COR within **30 days** after contract award and **annually** thereafter or upon request.

C. 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*.
- 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 OpDiv Information Security Awareness
- 3) Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

D. Incident Response

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) and OASH IRT teams **within 24 hours**, whether the response is positive or negative.

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.

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”.

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

- 1) 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 with FIPS 140-2 validated encryption.

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 *OS/OASH* approved notifications to affected individuals.

- 2) Report all suspected and confirmed information security and privacy incidents and breaches to the HRSA Security Operations Center (SOC) (csirt@hrsa.hhs.gov), 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, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

- a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;

- b. not include any sensitive information in the subject or body of any reporting e-mail; and
- c. encrypt sensitive information in attachments to email, media, etc.

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

3) 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. This may also involve physical access to contractor facilities during a breach/incident investigation.

E. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR).

F. 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*.

For additional information, see HSPD-12 policy at: <https://www.dhs.gov/homeland-security-presidential-directive-12>

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 and/or CO within one week of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within *1 week* 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.

G. Contract Initiation and Expiration

- 1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall

comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012).

HHS EA requirements may be located here:
<https://www.hhs.gov/ocio/ea/documents/proplans.html>

- 2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
- 3) **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 the 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*.
- 4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within *one week* before an employee stops working under this contract.
- 5) **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 *OS/OASH* policies.
- 6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the HHS OS/OASH Contractor Employee Separation Checklist when an employee terminates work under this contract within *14* days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. Records Management and Retention

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/OASH policies and shall not dispose of any records unless authorized by HHS/OASH.

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/OASH policies.

A. Privacy Act

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.

The System of Records Notice (SORN) that is applicable to this contract is: *A SORN will be developed.*

The disposition to be made of the Privacy Act records upon completion of contract performance.

B. Security Requirements for GOCO and COCO Resources

- 1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
- 2) **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 within the specified timeline(s). 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).

For an existing ATO, OpDiv must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such.

HHS/OASH 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 a *format/timeline/process as outlined in the project plan* to the CO and/or COR. The following SA&A deliverables are required to

complete the SA&A package

- **System Security Plan (SSP)** –The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and *OS/OASH* policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor’s bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least **annually** thereafter.
- **Security Assessment Plan/Report (SAP/SAR)** –The security assessment shall be conducted by *HHS/OCIO* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with **OS/OASH** shall *assist* in the assessment of the security controls and update the SAR at least **annually**.

- **Independent Assessment** - The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all “*high*” deficiencies. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).
- **POA&M** – The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. All high-risk weaknesses must be mitigated within *OS/OASH timeframes as agreed and documented within the project management plan* and all medium weaknesses must be mitigated within *OS/OASH timeframes as agreed and documented within the project management plan* from the date the weaknesses are formally identified and documented. *OS/OASH* 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, **OS/OASH** may require

designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least *quarterly*.

- **Contingency Plan and Contingency Plan Test** –The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and OpDiv policies. 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. Thereafter, the Contractor shall update and test the Contingency Plan at least *annually*.
- **E-Authentication Questionnaire** – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

- 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 FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and HHS IS2P. The following are the minimum requirements for ISCM:
- **Annual Assessment/Pen Test** - 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 (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates.
 - **Asset Management** - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least *quarterly by the CSP*. IT asset inventory information shall include IP address, machine name, operating system level,

security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

- **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, 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 standard HHS and government configuration baselines at least *at least quarterly*. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
 - **Vulnerability Management** - Use SCAP-compliant 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 HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least *quarterly*.
 - **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.
 - **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
- 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. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to 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, but is not limited to, 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. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
 - c. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
 - d. 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 HHS and FIPS 140-2 encryption 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
 - e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
 - Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a *monthly* basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

7. OPTIONAL TASKS – Not funded unless is exercised

Optional Task 1 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 (for a 120 day transition). The plan must support phases to allow collaboration with the outgoing contractor. The contractor must also submit a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees. The contractor(s) must also work with any future contractor(s) and HHS to facilitate complete operational transition, and this must be addressed in the transition plan.

- a. The plan shall ensure transition of all patients documented as receiving diagnostic testing to the new contractor responsible for the next phase of the contract with minimal disruption. The plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including, devices, equipment, databases and systems. 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.

8. **DELIVERABLES**

The contractor shall ensure all products and services delivered under this contract are compliant with HHS Section 508 requirements 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/) (<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) (<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) (<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 HHS 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 identified in the HHS Section 508 checklists

1.	Develop Payment File Format	4 weeks prior to payment	COR
2.	Develop Control File	4 weeks prior to payment	COR
3.	Conduct File Scrubbing	Each Payment Cycle	COR
4.	Develop Payment Files	Each Payment Cycle	COR
5.	Prepare Payment Request	5 business days prior to submit date	COR
6.	FPLP Offsets Withholding	Each Payment Cycle	COR
7.	Check Files to Bank	Each Payment Cycle	COR
8.	Payment History Report	Monthly	COR
9.	Payment Exception Report	3 business days after payment	COR
10.	Notification of Payment Report	3 business days after payment	COR
11.	Customer Service Help Desk Report	Monthly	COR
12.	IRS 1099s	Annually by January 31st	COR
13.	IRS Backup Withholding	As required	COR
14.	Authority to Operate (ATO)	As required	COR
15.	Quality Assurance Surveillance Plan	A draft is due 2 weeks after award with quarterly updates Updates due by the 5 th day of each quarter.	COR

		QASP Metrics should be delivered to HRSA along with the monthly contract status report.	
16.	Daily accounting extract file	Two weeks prior to payment file submission. Data field/elements, data attributes, unique identifiers, number of tables or files, for Government to track accounting activities of claims to payment file to disbursement to repayment, refund, etc.	COR
17.	Daily claims activity file	Two weeks prior to payment file submission. Data field/elements, data attributes, dates, unique identifiers, number of tables or files, specific to patient, physician, service provider at the claim-level.	COR

**ATTACHMENT A –SAMPLE QUALITY ASSURANCE SURVEILLANCE PLAN
(QASP)**

Task Area	Evaluation Measure	Performance Standard/Acceptable Quality Level (AQL)	Method Used	Frequency
All Tasks	Status reporting	Timely information on project status AQL: Submitted timely 97% of time	Inspection	Monthly
	Claims filing and processing	Claims filing and processing time AQL: Reduce by 40%	Inspection	Monthly
	Clean-claim rate	Clean-claim rate AQL: Increase by 9%	Inspection	Annually
	Documentation deliverable	Secure and confidential patient information AQL: 100% patient information is secured and confidential	Inspection	Monthly
	A/R Days	Correct and resubmit claims online AQL: Reduce by 50%	Inspection	Monthly
	Claims	Status of claims AQL: Processed within 30 days of receipt	Report	Monthly
	Duplicate Claims	Detect duplicate claims AQL: Corrected within 30 days	Report	Monthly
	Compliance Issues	Compliance issues AQL: Reduce by 80%	Report	Annually
	Adjudication rates	Increase adjudication rates AQL:	Inspection	Monthly

NOTE: This a sample. QASP submitted with proposal shall be commensurate to Final Performance Work Statement (PWS).

NON-DISCLOSURE AGREEMENT

WHEREAS, the United States Department of Health and Human Services, Health Services and Resources Administration (HRSA) will enter into a Contract with United Healthcare Services, Inc., on behalf of itself and its affiliates (UHC);

WHEREAS, in advance of the Contract, HRSA will send a data file containing provider information to UHC to facilitate payments to eligible providers from the Public Health and Social Services Emergency Fund under the Coronavirus Aid, Relief, and Economic Security (CARES) Act;

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.

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.

Signed for and on behalf of
HRSA

by /s/

by /s/

Payman Pezhman, Secretary and
Authorised Signatory

Thomas J. Engels
HRSA, Administrator

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 /s/

Payman Pezhman
Secretary and Authorized Signatory

Signed for and on behalf of
HRSA

By /s/

Thomas J. Engels
HRSA, Administrator

**Performance Work Statement (PWS)
Claims Processing Services for the Provider Relief Fund
Department of Health and Human Services (HHS)
Health Resources and Services Administration (HRSA)**

Date: April 07, 2021

I. Background

In December 2019, a novel (new) coronavirus known as SARS-CoV-2) was detected causing outbreaks of the coronavirus disease COVID-19 that has now spread globally. The Secretary 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 COVID19 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, the COVID-19 outbreak in the United States constituted a national emergency. On January 7th, 2021 the Secretary of Health and Human Services renewed the determination that a public health emergency still exists.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136), the Paycheck Protection Program (PPP) and Health Care Enhancement Act (P.L. 116-139), and the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act (P.L. 116-123) appropriated funds to reimburse eligible healthcare providers for healthcare related expenses or lost revenues attributable to coronavirus. These laws provide economic and financial support for individuals and business impacted by the coronavirus outbreak. To provide relief, Congress appropriated funding from the Public Health and Social Services Emergency Fund to reimburse eligible health care providers for health care related expenses or lost revenues that are attributable to coronavirus.

Provider Relief Fund legislation specifies that eligible health care providers may receive a payment or be reimbursed for health care related expenses or lost revenues that are attributable to coronavirus that have not been reimbursed from other sources or that other sources are obligated to reimburse. Eligible health care providers are public entities, Medicare or Medicaid enrolled suppliers and providers, and other entities the Secretary may specify, that provide diagnoses, testing, or care for individuals with possible or actual cases of COVID-19. The CARES funds can be used to provide a payment or reimburse eligible providers for lost revenues and costs related to the coronavirus outbreak including building or construction of temporary structures, leasing of properties, medical supplies and equipment including personal protective equipment and testing supplies, increased workforce and trainings, emergency operation centers, retrofitting facilities, and surge capacity.

In addition, the Paycheck Protection Program (PPP) and Health Care Enhancement Act (P.L. 116-139), provided \$225M in additional funding for COVID-19 testing and related expenses, through grants or other mechanisms, to rural health clinics as defined in section 1861(aa)(2) of the Social Security Act, with such funds also available to such entities for building or construction of temporary structures, leasing of properties, and retrofitting facilities as necessary to support COVID-19 testing: Provided further, that such funds shall be distributed using the procedures developed for the Provider Relief Fund authorized under the third paragraph in division B of the Coronavirus Aid, Relief, and Economic Security Act (Public Law 116-136); may be distributed using this contract.

II. Purpose and Scope

The purpose of this contract for the disbursement of payments to eligible health care providers for health care related expenses and/or lost revenues that are attributable to coronavirus. Based on the direction and information provided to the Contractor by HRSA and HHS, the Contractor shall process and distribute payments to eligible providers, provide customer service education, data support, communications outreach, escalation of provider issues, and project management for the Provider Relief Fund and related provider relief legislation as authorized by Congress. Subject to the changes clause, additional related funding, greater than the \$178B currently authorized for COVID-19 or provider relief disbursements and/ or reimbursements may be distributed through the Provider Relief Fund as authorized by public law, using the procedures and agreements developed under this contract.

The scope of this activity includes:

1. Project Management
2. Payment Distribution
 - a. Electronic Payment
 - b. Paper check payments
3. Payment Terms and Conditions Attestation
 - a. Create a new or leverage an existing web portal to ingest attestations for payment acceptance and/ or documentation
4. Reconciliation
 - a. Paper Remittance
 - b. General Payment Processing
 - c. Payment Recovery
 - d. Back-End Processing
 - e. Remittance Support
 - f. Attestation by the Provider
5. Provider Customer Service Program
 - a. Education and Outreach (electronic and paper mail)
 - b. Call Center
 - c. Microsites
6. Provider Payment and Integrity

7. Compliance Reporting Support
8. Data Security

III. General 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 Government assumes complete responsibility for the accuracy and sufficiency of the information and data provided to the Contractor, to include information concerning the providers to whom relief payments should be disbursed, the amount that each eligible provider is paid, and the communication related to disbursements process by the Contractor.

IV. Tasks

The Contractor shall perform the following tasks:

Task 1 – Project Management Support

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

The Contractor Shall:

- Be responsible for PRF Project Management.
- Execute program and project objectives and priorities as directed by the Government.
- Total responsibility for overall direction for program project work will fall under the direction of the Government.

Project Management activities include:

- Management of personnel;
- Utilizing existing commercial processes and procedures for PRF operations and contract management;
- Management of subcontractors as appropriate;
- Establish effective communications and reporting procedures with HRSA;
- Proper financial management of the contract funds; and
- Other program management tasks necessary to meet the requirements of this contract.

- Providing systems project management support for new portal functionality
- Overall scheduling and resource management; and
- Risk management; document control

Task 1.1 – 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’s 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 1.2 – Kickoff Meeting

The Contractor Shall:

- Meet with the COR and other HHS representatives to discuss current activities, communications, and the contracting process. The objectives of the kickoff meeting are to:
 - Initiate the communication process between HHS and the contractor by introducing key project participants and identifying their roles.
 - Ensure the contractor understands the expectations of key stakeholders regarding the scope of work and the effort described in this contract, including task requirements and objectives.
 - Review communication ground rules.

Task 1.3 – Conference Calls

The Contractor shall:

- Chair weekly/bi-weekly conference calls with HHS/HRSA representatives.
- Facilitate project updates and ad hoc reports. Ad hoc meetings will be held within 24 hours of a request by the Contractor or the COR.

Task 1.4 – Reports

The Contractor Shall:

Provide the following reports in the Contractor’s format:

Name of Report	Description	Format (Word, Excel, Data File, etc.)	Cadence

OptumBank ACH Payment File	Payment data reporting for each transaction by provider billing TIN for ACH transactions	Data File via Secure Transfer (e.g. (b) (4))	Daily
Optum Bank Check File	HHS requests banking data reporting for each transaction. Payment data reporting for each transaction by provider billing TIN for checks.	Data File via Secure Transfer (e.g. (b) (4))	Daily
Daily UHG HHS CARES Act Update for xx/xx/2021	Summary reporting for payments and operations and attestation reporting rolled up by status and Distribution #	Email	Daily
Attestation & Demographic Detail	Detailed attestation demographics reporting by provider TIN	CSV Data File via Secure Transfer (e.g. (b) (4))	Twice Weekly - Wednesday 6:00PM ET and Friday 11:59PM ET
Provider Populations Phase/Wave Grid	Detailed Phase/Wave grid that shows descriptions, dollar amounts, and dates of disbursements.	Word doc via Email	Daily

Task 1.4.1 – Risk Management

The Contractor Shall:

- Use its standard risk management practices.

Task 1.5 – Project Management

The Contractor Shall:

- Facilitate requirements workshops to:
 - Update the application portal, attestation portal, or payment process.
 - When the external facing portal or web pages are updated such as the Attestation

- Portal, Application Portal 1.0, Application Portal 2.0, the Contractor shall provide screenshots and walk through the process of the provider experience, the Contractor is only expected to walkthrough and document the parts of the system they manage.
- Participate in requirements meetings related to distributions or process of additional eligible providers within a distribution as defined by HRSA or HHS in a timely manner, except that Contractor shall not be required to participate in requirements meetings regarding funding exceeding the currently authorized amount of \$186,500,000,000.00.
 - Document HRSA requirements for the PRF payment processing
 - Discuss and document technical requirements to collect a daily extract file from the contractor's accounting system.
 - Maintain a history of payments.

Task 2 – Provider Payment

The PRF payments are divided into multiple distributions, as determined by HHS/HRSA.

See price schedule under Section B.2 for PRF payment quantities.

The Contractor Shall:

- Use its existing systems to:
 - Manage file transfers, control funding transfer requests, chain of custody, and money transfer workflow;
 - Implement and perform reconciliation controls to ensure funding transfer accuracy;
 - Provide a payment system that manages financial transactions, such as:
 - Interface with the bank,
 - Accept wire transfers, checks, and ACH,
 - Remit returned funds to HHS on a daily basis,
 - Reconcile and trace ACH and check payments to each distribution.
 - Disburse payments at intervals determined by HHS/HRSA. During the base year process up to 700,000 payments, in option year 1 process up to 150,000 payments, in option year 2 process up to 50,000 payments.
 - Process checks on a cleared basis and request reimbursement.
 - Process payment files with HHS/HRSA provided ACH addenda record descriptors. During the base year process up to 140 payment files; in option year 1 process up to 70 payment files; in option year 2 process up to 70 payment files.

Task 2.1 – Financial Management and Payment Distribution

The Contractor Shall:

- Distribute payments to eligible providers using files provided by the COR and approved by HHS/HRSA (Payment Files).

- The HHS files will include eligible providers, their TIN number, Provider address, phone number, amount of payment, and the ACH bank account information (if available).
- Use this information to make ACH or check payments to eligible providers in the amount specified by the Payment file via Optum Pay ACH, CMS ACH, provider submitted ACH (via application e.g. Portal 2.0) or paper check.
- Use the approved Wire Transfer Instructions and execute the Wire Transfer Instructions to HHS using an FDIC-protected Bank Account (“Bank Account”) as described in the TriPartite Agreement among the parties dated April 8, 2020 or later if a more current version is available.
- Validate that funds have been received in the Contractor’s bank account.
- Use and maintain a record of the ACH Addenda Record character descriptor approved by the HRSA designee for each ACH payment to eligible providers listed in Payment files.

Task 2.1.1 – Electronic ACH Payments

The Contractor Shall:

- Perform ACH Transaction Processing,
 - Base year: Process up to 650,000 ACH Transactions
 - Option year 1: Process up to 143,000 ACH Transactions
 - Option year 2: Process up to 48,000 ACH Transactions
- Distribute the funds in accordance with Payment Files using industry best practices and confirm distribution of funds within 24 hours.
- After distribution by ACH of each Payment File, the process will identify failed transactions and payment errors arising from the distribution and provide data files to the COR within 24 hours.
 - As determined by the COR or designee, contact providers as appropriate to re-originate payment.
 - Recommend a process for non-acceptance of payment, non-attestations and other forms of non-acceptance by the Providers and will implement the process approved by HHS/HRSA. Return to HHS funds that are not accepted or returned by providers.
 - Send, track, and reconcile paper checks issued to providers.

Task 2.1.2 – Paper Checks

The Contractor Shall:

- Process Paper Checks
 - Base year: Process up to 50,000 Paper Checks
 - Option year 1: Process up to 7,000 Paper Checks
 - Option year 2: Process up to 2,000 Paper Checks
- Send paper checks to eligible providers from the HHS Payment Files that do not have an ACH account on file with Optum Pay, HHS/HRSA or will not accept an electronic

payment.

- Fund the payment of the check; upon the presentment of the check by the eligible provider for payment.
- Request reimbursement from HRSA and track each check amount presented for payment by each eligible provider.
- Implement a standard commercial process to create and distribute checks.
- Develop and implement a process for undeliverable checks (returned mail per Task 3.1),
- Develop and implement a process to handle provider checks returned by mail, including reconciliation to the amount paid, and returning the funds to HHS/HRSA with associated reporting.
 - Base year: Process up to 500 checks per month.
 - Option year 1: Process up to 300 checks per month.
 - Option year 2: Process up to 30 checks per month.
- Implement the HHS/HRSA policy as directed for checks that do not get cashed within a specified number of days, and
- Implement a process agreed with HHS/HRSA for providers that do not attest within the time period established by HHS/HRSA.
- Return payments rejected by eligible providers to HRSA per treasury instructions.
- Track and reconcile paper checks to providers by disbursement Wave and funding request who cannot receive an ACH payment as determined by program policy.

Task 2.1.3 – Payment System

The Contractor Shall:

- Establish a payment system that will:
 - Provide the required accounting, firewalls, and funds control capabilities to ensure that all Treasury deposits and financial transactions are managed, maintained, and reported separately in a segregated bank account;
 - Manage, maintain and report payments;
 - Be capable of auditable funds control and management of all deposits and transactions;
 - Have quality assurance and payment integrity capabilities to ensure payments are processed accurately and without duplication;
 - Have full and ad hoc reporting capability for all financial transactions and shall comply with all HHS/HRSA security requirements.

Task 2.1.4 – Approved Bank Account

The Contractor Shall:

- Maintain a bank account capable of processing and managing all financial transactions in accordance with the Tripartite Agreement with the Bank and HRSA.
- Maintain a separate and dedicated bank account for the Provider Relief Fund.

- Return interest gained in the account to HRSA via wire transfer on a routine basis determined by the COR.
- Provide account safeguards, monitoring and access controls to PRF related financial transactions.
- Use the identified and agreed upon account to disburse payments.
- Return surplus funds received from providers due to voluntary returns to HHS/HRSA.

Task 2.1.5 – IRS 1099s to Payees

The Government shall provide Contractor with a file identifying providers who shall receive an IRS 1099-MISC, and the amounts paid to each provider under this program in the relevant calendar year.

The Contractor Shall:

- Process 1099s for providers using HRSA provided data.
 - Base year: Process up to 700,000 1099s.
 - Option year 1: Process up to 150,000 1099s.
 - Option year 2: Process up to 50,000 1099s.
- Prepare and send IRS 1099-MISC, in accordance with IRS regulations (<https://www.irs.gov/newsroom/frequently-asked-questions-about-taxationof-provider-relief-payments>), no later than January 31st to all payees that received payments in the prior calendar year.
 - For example, for payments made in 2021, the contract shall send the 1099 by January 31st, 2022.
- Send the electronic 1099 file with this information to the IRS in accordance with the IRS reporting deadline.
- Mail the 1099s and provide customer service for 1099 recipients.

Task 2.2 – Financial Management and Reporting

The Contractor Shall:

- Establish and maintain a payment integrity plan consistent with its commercial practices that ensures internal contractor controls that comply with payment process and bank regulatory standards.

Task 2.2.1 – Financial Accounting System

The Contractor Shall:

- Host the financial accounting system responsible for making payments.
- Secure routine and ad hoc execution of payment files;
 - Secure processing and storage of all payment records;
 - Secure reporting and file transfer capabilities;

- Secure interface with other HHS/HRSA internal systems and external systems such as US Treasury, and
- Ensure disaster recovery capabilities.
- Operate and maintain the financial accounting system.
 - Secure routine and ad hoc execution of payment files;
 - Secure processing and storage of payment records per Contractor's records retention program – See Task 7 – Records Management;
 - 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 with a daily extract of financial data from contractor's financial accounting system.
 - Provide detailed banking data files as necessary from the financial accounting system, excluding Optum Pay provider bank account information, that provides details of all financial transactions, including ACH, and check payments; original ACH payments shifted to paper check; re-issued payments, payments flagged for stop payment, checks cashed, etc. with the fields and columns agreed to by the HRSA financial oversight designee.
 - Coordinate with and provide the file structure, data elements, data dictionary, etc. to the HRSA financial oversight designee.
- Reconcile payment files with actual payments made and their payment method (ACH, paper check, re-issuance, etc.) or return type to ensure payments can be traced back to initial funding requests.

Task 2.2.2 – Payment Files

The Contractor Shall:

- Work with HHS/HRSA and designee project staff to develop a standardized payment file format.
- Provide a timeline of the deposit date for eligible providers paid via ACH for each Payment File.
- Ensure each Payment File recipient has ACH payment instructions as possible.
- Track each Payment File distribution amount, distribution date.
- Provide notification to HHS/HRSA of all returned ACH and check payments, including the ACH addenda record.
- Review payment files for quality control, ensuring that each provider has a TIN and a payment amount, and that the file totals agree with amounts communicated by HRSA.

Task 2.2.3 – Funding Requests

The Contractor Shall:

- Send payment requests to the COR for approval and funds certification at a duration of one (1) Business day prior to the submit date during a payment cycle.

- Distribute the total funds requested for the payment requests.
- For payments made by check, include itemized payment totals by distribution such as cleared checks, the Contractor's legal business name, and the date of the request.

Task 2.3 – Payment Returns

HHS/HRSA shall be responsible for recovering funds from providers.

The Contractor Shall:

- Maintain a procedure for handling returned funds from providers.
- Reconcile the financial data feed with returns captured by HRSA

Task 3 – Customer Support Services for Internal and External Users

The Contractor Shall:

- Establish a Customer Service Program to respond to provider telephone and email inquiries in an accurate and consistent manner to ensure satisfactory quality and performance standards are met as defined in the bullets below. In support of customer service, includes:
 - 8:00 a.m. to 8:00 p.m. Eastern Time during non-reporting period.
 - 8:00 a.m. to 11:00 p.m. Eastern Time during the Application and Reporting Period as defined by HRSA.
This ensures the customer service hours align with HRSA's Tier 2 customer service contractor for advanced reporting system inquiries.
 - Answer and respond to provider inquiries
 - Base year: Intake up to 822,000 calls
 - Option year 1: Intake up to 249,000 calls
 - Option year 2: Intake up to 107,000 calls
 - Establish the infrastructure to adequately support call volume; provide updates to IVR, training, and application access.
 - Review available PRF information to draft general responses to incoming questions. Define FAQ and talking points using information provided by HHS regarding the program.
 - Coordinate HHS/HRSA on response plans for external correspondence for both email and paper mail.
 - Provide effective provider education to answer questions and promote appropriate steps for payment requests related to eligibility, status, application process, and reporting process, as well as inquiries related to technical issues, such as Attestation, DocuSign, ACH and check troubleshooting.
 - Maintain a high level of provider service and satisfaction through good communication and relationships with providers.
 - Train call center staff to handle calls or emails from providers and conduct additional training as needed should changes in process or complexity require it.

- 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) defined in section F.4 Schedule of Deliverables.
- Create a defined internal escalation and issue tracking process with input from HRSA to review and respond to questions and to transfer escalated issues to HRSA to resolve.

Task 3.1 – Mail and Correspondence

The PRF receives a variety of documents via email and conventional mail. All forms and envelopes must comply with the HHS/HRSA Visual Style Guide and HHS/HRSA logo policy.

The Contractor shall:

- Establish, operate and maintain mail operations.
- Manage the inventory of all the forms and templates for outgoing correspondence. Process, print, and mail paper checks and letters to providers as defined by Task 2.
- Process forms and related correspondence as necessary to satisfy provider payment requirements.
- Receive and deposit check returns from providers with associated accounting reconciliation to the distributed amount and provider outreach.
- Track and electronically store information related to mailed checks and returns from check mailings for address correction. Or, incoming checks mailed by providers. Available upon request by COR.

Task 3.2 – Communications

The Contractor Shall:

- Contractor, in coordination with and subject to the approval of HHS/HRSA, will define communications and touchpoints with eligible providers for pre-payment, payment, and post-payment distributions and implement them on HHS/HRSA's behalf. HHS/HRSA will provide approved communication to the Contractor advising the eligible provider of the payment and required provider actions. Contractor will distribute the HHS/HRSA provided communication to eligible providers provided by HHS/HRSA.
- Process email communications.
 - Base year: Process up to 10,000,000 email communications
 - Option year 1: Process up to 5,000,000 email communications
 - Option year 2: Process up to 5,000,000 email communications
- Process paper letter communications.
 - Base year: Process up to 60,000 paper letter communications per month
 - Option year 1: Process up to 12,500 paper letter communications per

month

- Option year 2: Process up to 3,500 paper letter communications per month
- Subject to approval by HHS/HRSA, Contractor will draft emails and letters addressed to the Providers regarding relief fund payment distributions.
 - Base year: Draft up to 430 new communication templates
 - Option year 1: Draft up to 100 new communication templates
 - Option year 2: Draft up to 100 new communication templates
- HHS/HRSA will provide Contractor with all attestation language and will post all attestation language for each Payment File or distribution to HHS/HRSA's website.
- HHS/HRSA will provide a plain language description of the formula describing the calculations used to determine the payment to eligible providers in each Payment File HHS/HRSA provides to the Contractor. Contractor will include the HHS/HRSA provided formula description in communications to providers.

Task 3.3 – Provider Outreach and Education (POE)

The Contractor Shall:

- Educate providers about the PRF via phone and email through customer support, system portals, webinars and focus groups in coordination with HHS. POE may be delivered to groups, to individuals and through various media channels in consultation with HRSA COR and Subject Matter Experts.
 - Base year: Provide up to 6 provider education webinars with a maximum of 3 webinars per month.
 - Option year 1: Provide up to 4 provider education webinars with a maximum of 2 webinars per month.
 - Option year 2: Provide up to 3 provider education webinars with a maximum of 1 webinars per month.
- Research and resolve inquiries received outside of the contact center.
- Follow up with providers as requested by HRSA to resolved complex policy questions.

Task 4 – IT Services

The Contractor Shall:

- Responsible for management of contractor provided software resources and for coordinating with other program systems (e.g. CA Agile, DocuSign, etc.) to perform the activities of PRF.
- Provide resources to support operations and corrective maintenance of supporting software.
- Provide release notes and screenshots after each system change to the COR.

- Provide system demo as requested by the COR, no more than once per month and no more than six (6) demos per calendar year, excluding OIG interviews.
- Provide both emergency and routine system support as needed within agreed upon timeframes and standard Provider deployment windows as consistent with the normal course of business.
- Ensure all contractor owned contractor operated (COCO) and commercial off the shelf software (COTS) software is maintained, patched, and updated to maintain or exceed the security baseline identified in the security task.
- Deploy software releases for enhancements and defect fixes supporting Attestation and Payment portals.
 - Base year: 2 software releases per month with a maximum of 18 releases
 - Option year 1: 1 software releases per month with a maximum of 12 releases
 - Option year 2: 1 software release per month with a maximum of 12 releases

Task 4.1 – Microsite Support

The Contractor Shall:

- Provide input into the development of a landing page to communicate overall program, FAQ's and provide key links at <https://hhs.gov/providerrelief>.

Task 4.2 Attestation Portal

The Contractor Shall:

- Implement and maintain a portal based on HHS/HRSA provided requirements to allow eligible providers to submit their required attestations to accept or reject the terms and conditions associated with the payments they've received.
- Implement methodology as approved by HHS/HRSA to validate the provider is authorized to accept or reject the terms and conditions.
 - For example, use the results (successfully processed ACH payments & mailed checks) from the processed payment file to validate provider information including Tax Identifier Number/TIN (either EIN or SSN), Account Number (if ACH), Check Number (if Physical Check), Payment Amount, and Date (if multiple payments were issued to exact same provider on different days).
- Configure the portal so that it can be closed.
- Retain all data and provide reports with specific factors as determined by the COR including cross referencing a provider's attestation with and payment disbursement status.
- Perform post processing of attestation data to reconcile the provider attestation status to match the provider's payment action status as defined by PRF policy. For example, adding additional meta-data to the original record post attestation to indicate the provider's acceptance or rejection based on their retention or return of the provider payment.

- Maintain the integrity of the original provider records.
- Clearly identify added reconciled status meta-data.
- Provide attestation data files to HRSA in CSV format twice per week on Wednesday by 6:00PM ET and Friday by 11:59PM ET and ad hoc reports as requested by the COR on portal use and data submitted to the portal.

Task 4.3 – Software Quality Control and Systems Development Management Plan

The Contractor Shall:

- Implement quality standards for all Contractor managed systems that meet the standards of auditability, confidentiality, availability, integrity, and quality and compliance practices associated with the distribution of payments, handling of Personally Identifiable Information (PII), customer service and reporting.

Task 4.4 – Provider Applications

The Contractor Shall:

- Provide and maintain mechanisms to collect applicant information from providers (i.e. Portal 1.0 and Portal 2.0) and perform data validation checks on the format of the data determined by HHS/HRSA via the COR.
- Provide and maintain the ability to require applicant providers to move through the portal in a sequential flow.
 - Require applicant providers to register in a portal; submit their TIN and business information; validate the submitted TIN and business information with the IRS; if the applicant provider's TIN is on a list provided by HRSA, only then reveal the revenue application link, allow providers whose TIN is on a 'curated list' of TINs provided by HRSA.
- Support the integration of a provider application with the Attestation Portal and other validation and authentication mechanisms.
- Maintain the ability to verify the provider's TIN with IRS to ensure the TIN exists and inputted business name associated with the TIN is valid and is not on the IRS TAF list of fraudulent providers. Inform the provider via email if they completed or failed the IRS check.
- Provide and maintain mechanisms to create a validation point within the application process to compare the provider's submitted TIN(s) against a list of eligible curated TINs provided by HRSA. If the provider's TIN passes IRS validation and is on the curated list, then send the provider an email to continue their application and show the link for the DocuSign web form provided by HRSA. DocuSign is maintained by HRSA and is used to capture revenue application data from the applicant. If the provider's TIN is not on the curated but passed the IRS TIN validation process then send them an email with content provided by HRSA.
- Detect and notify the COR within one calendar day when fraudulent activity is detected with a provider that is registering for a payment or has received payment utilizing the following processes:

- In cases where a Provider is applying for funds and is not already registered with the contractor, the provider is directed to register on the CARES Payment Portal. As part of this registration, the contractor verifies the provider's TIN with IRS to ensure the TIN exists and inputted business name associated with the TIN is valid and is not on the IRS TAF list of fraudulent providers.
- Run a check on the list of providers in the payment files provided by HRSA to identify any fraudulent providers and will monitor new enrollments for HRSA PRF payments for account takeover attempts. If fraud is identified in either event, the contractor will report through their security incident and response team.
- In the event one or more providers in the payment file are identified as potential fraudulent activity, UHCS shall release all payments. HRSA will direct UHCS to perform a reverse ACH against specified providers. UHCS will perform requested reversals if allowable within the prescribed timeframes for reversals specified in the National Automated Clearing House Association (Nacha) Operating Rules & Guidelines.
- Integrate and maintain the integration between the contractor's provider application portal and the revenue application web-form (currently in DocuSign). Ensure that when an applicant clicks the DocuSign link and is redirected from the contractor's application portal to the DocuSign web form, selected application data is securely transferred and prepopulated in the revenue web form. HRSA will coordinate the integration meeting with DocuSign. Any data collected in DocuSign is not accessible by the Contractor's web portal, except the envelope status.

Task 4.5 – 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 5 – Support for Program Operations

This task section identifies Contractor specific requirements for program tasks such as compliance and disputes.

Task 5.1 – Compliance

The Contractor Shall:

- Support reporting per Task 1.4. HRSA shall review the reporting provided in order to:
- Support mass correspondence and communications via email, letters, or webinar.
- Support HRSA in executing planned and focused compliance efforts.
- Support compliance efforts by other contractors.
- Support assessment of attestation compliance.
- Evaluate cases involving complex policy questions or business rules.

Task 5.2 – Payment Dispute Process

The Contractor Shall:

- At any time, a provider may dispute their eligibility to receive payment or the payment they received, including, but not limited to overpayment, underpayment, or incorrect payments such as change of ownership.
- When a dispute is reported to the call center, the Contractor will attempt to clarify the dispute first with the available policy information, if it cannot be resolved the contractor shall escalate the dispute to HRSA. Escalated cases are sent daily to ProviderReliefContact@hrsa.gov.

Task 5.3 – Respond to Data Requests

The Contractor shall:

- Respond to OIG TIN investigation requests:
 - Base year: up to 140 individual TIN investigations
 - Option year 1: up to 120 individual TIN investigations
 - Option year 2: up to 120 individual TIN investigations
- Respond to A-123 audits.
 - Base year: up to 1 A-123 audit
 - Option year 1: up to 1 A-123 audit
 - Option year 2: up to 1 A-123 audit
- Respond to OIG interview requests.
 - Base year: up to 1 OIG audit per quarter
 - Option year 1: up to 1 OIG audit per quarter
 - Option year 2: up to 1 OIG audit per quarter
- Provide data reports (through the designated POC and the COR) to components within Federal Government using PRF provided or generated data. In response to data requests the Contractor may exclude pre-PRF data.
 - Data requests shall be fulfilled within 4 business days of request from the COR.
 - Urgent data reports shall be fulfilled within 2 business days of request.
 - Written extension is requested and approved by the designated POC and the COR.
 - Some requests may involve data that may be withheld under the terms of the Privacy Act of 1974, as amended (5 U.S.C. ' 552a), the Trade Secrets Act (18 U.S.C. ' 1905), the Freedom of Information Act (FOIA) (5 U.S.C. ' 552), or other applicable laws. For example, any personally-identified or personally identifiable data maintained in the OPTN/SRTR/HRSA Data System of Records, HHS/HRSA/HSB/DoT, No. 09-15-0055, including data maintained electronically, must be disclosed consistent with the Privacy Act and the Systems Routine Uses.

Task 6 – Security Requirements

1. Applicability. The requirements herein apply whether the entire contract or order (hereafter

“contract”), or portion thereof, includes either or both of the following:

- a. 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.
- b. 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.

2. Safeguarding Information and Information Systems. In accordance with the Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:

- a. Protect government information and information systems in order to ensure:
 - Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - Availability, which means ensuring timely and reliable access to and use of information.
- b. 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.
- c. Adopt and implement the policies, procedures, controls, and standards required by 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.
- d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.

3. Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST Special Publication (SP) 800-60, Volume II: Appendices of Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, 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

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

4. 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:

- a. marked appropriately;
- b. disclosed to authorized personnel on a Need-To-Know basis;
- c. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and

- d. 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.

5. 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 OMB Memorandum M-06-16, Protection of Sensitive Agency Information by securing it with a FIPS 140-2 validated solution.

6. 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 HHS and HRSA policies. Unauthorized disclosure of information will be subject to the HHS/HRSA sanction policies and/or governed by the following laws and regulations:

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

7. Internet Protocol Version 6 (IPv6). All acquisitions using Internet Protocol shall comply with FAR sections: FAR 7.105(b)(5), FAR 11.002(g), and FAR 12.202(e).

8. 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). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

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

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

- a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
- b. 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.) with FIPS 140-2 validated encryption solution.
- c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and HRSA-specific encryption standard requirements. 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).
- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR prior to the EPLC Design Readiness Review (DRR).
- e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11. 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 D), as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) within 14 days of the effective date of the contract.

12. 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.

- a. 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.
- b. 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.

13. Training.

- a. **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.
- b. **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.
- c. **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.

14. Rules of Behavior.

- a. 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.
- b. 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.

15. Incident Response.

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.

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”.

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 with FIPS 140-2 validated encryption.
- 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:
 - 1) cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
 - 2) not include any sensitive information in the subject or body of any reporting e-mail; and
 - 3) encrypt sensitive information in attachments to email, media, etc.
- d. 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.
- e. 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.

16. Position Sensitivity Designations.

All Contractor (and/or any subcontractor) employees accessing HRSA systems must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

TBD

17. 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, with a copy to the Contracting Officer, 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.

18. Contract Initiation and Expiration.

- a. General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HRSA EPLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012).
- b. System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require

artifact review and approval.

- c. 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.
- d. 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.
- e. 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.
- f. 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.

19. Contractor Owned Contractor Operated System Security Requirements.

- a. Federal Policies. The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the HHS Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53, Security and Privacy Controls for Federal Information Systems and Organizations; Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
- b. 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).

For an existing ATO, HRSA must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such.

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.

1) 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:

- System Security Plan (SSP) – Initial draft version due within 30 days of the EPLC Performance Baseline Review. Final draft due 120 days prior to the Operational Readiness Review. Final version due 30 days prior to the Operational Readiness Review.

The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS and HRSA policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter.

- Security Assessment Plan/Report (SAP/SAR) – due 30 days prior to the Operational Readiness Review. The security assessment shall be conducted by HRSA's Security Assessment Team and be consistent with NIST SP 800-53A, NIST SP 800-30, latest revisions, and HHS and HRSA policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with HRSA shall assist in the assessment of the security controls annually and update the SAR at least annually.

- 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.
- E-Authentication Questionnaire – The Contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, Electronic Authentication Guidelines.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

- 2) 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 FISMA and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and HHS IS2P. 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 specified due date [OpDiv provided].

- Asset Management - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. The inventory information is required to be produced within 30 days of the EPLC Performance Baseline Review. Final version due within 30 days prior to the Operational Readiness Review and reviewed and updated on a monthly basis thereafter. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
- Configuration Management - Use available SCAP-compliant automated tools, per NIST IR 7511, 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 standard HHS and government configuration baselines prior to the EPLC Operational Readiness Review. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- Vulnerability Management - Use SCAP-compliant 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 HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. If externally-hosted and HRSA is unable to directly scan the system/application, the contractor (and/or any subcontractor) shall provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency prior to the EPLC ORR and at least monthly thereafter and upon request.
- 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; and
 - 180 days for Low risk vulnerabilities.
- Secure Coding - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - Boundary Protection - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
- c. 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:
- 1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to 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.

- 2) 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, but is not limited to, 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. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
- 3) Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
 - 4) Cooperate with inspections, audits, investigations, and reviews.
- d. 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.
- e. 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:
- 1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-2 encryption standards.
 - 2) Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and HHS Minimum Security Configuration Standards;
 - 3) Maintain the latest operating system patch release and anti-virus software definitions;
 - 4) Validate the configuration setting 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
 - 5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security

configuration assessment scanning; and

- f. Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

20. HHS FedRAMP Privacy and Security Requirements.

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

- a. FedRAMP Compliant ATO. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.
 - 1) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The HHS Information Security and Privacy Policy (IS2P) and HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.
 - 2) A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
- b. 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.
- c. 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.

21. Protection of Information in a Cloud Environment.

- a. 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.

- b. 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.
- c. 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.
- d. The Contractor shall support a system of records in accordance with NARA- approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
 - 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.
- e. 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.
- f. 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.

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

- a. The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/HRSA security policies.
 - 1) In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the HRSA authorizing official (AO) prior to implementation of system and/or service being acquired.
 - 2) CSP systems categorized as Federal Information Processing Standards (FIPS) 199

high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

- 3) For all acquired cloud services, the SA&A package must contain the following documentation:
 - a) Privacy Impact Assessment (PIA)
 - b) FedRAMP Test Procedures and Results
 - c) Security Assessment Plan (SAP)
 - d) Security Assessment Report (SAR)
 - e) System Security Plan (SSP)
 - f) IT System Contingency Plan (CP)
 - g) IT System CP Test Results
 - h) Plan of Action and Milestones (POA&M)
 - i) Continuous Monitoring Plan (CMP)
 - j) FedRAMP Control Tailoring Workbook
 - k) Control Implementation Summary Table
 - l) Results of Penetration Testing
 - m) Software Code Review
 - n) E-Authentication Questionnaire
 - o) System of Record Notice (SORN)
 - p) Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/HRSA policies.

- b. 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.
- c. 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.

- d. 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. HRSA will determine the risk rating of vulnerabilities using FedRAMP baselines.
- e. 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.

23. Reporting and Continuous Monitoring.

- a. 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. [OpDiv include meetings/deliverables timelines as applicable/necessary]
- b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis:
 - 1) Operating system, database, Web application, and network vulnerability scan results;
 - 2) Updated POA&Ms;
 - 3) Any update authorization package documentation as required by the annual attestation/assessment/review or as requested by the HRSA System Owner or AO; and
 - 4) 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.

24. Configuration Baseline.

- a. The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/HRSA configuration baseline.
- b. The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

25. Media Transport

- a. 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).
- b. 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.

26. Boundary Protection: Trusted Internet Connections (ITS)

- a. 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.
- b. The contractor shall route all external connections through a TIC.
- c. Non-Repudiation. The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

Task 7 – 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 HRSA or deletion of temporary records in accordance with NARA-approved retention schedules.

Task 8 – 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 HHS Records Management Training before performing work under this contract, and thereafter completing the annual refresher course during the life of the contract.

The training is located at

https://humancapital.learning.hhs.gov/courses/2020recordsmanagement/01_index.html. At the end of the Records Management training, the “Congratulations” slide is considered your certificate of completion. Please send the completion certificates to the Contracting Officer Representative (COR) of the contract. 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.

Optional Tasks and Quantities – Not funded unless exercised.

Optional Task 1 – 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). The plan must support phases to allow collaboration with the outgoing contractor.

The contractor must also submit a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees. The contractor(s) must also work with any future contractor(s) and HHS/HRSA to facilitate complete operational transition,

and this must be addressed in the transition plan. This transition plan is predicated on the incoming contractor being available on day one to shadow Contractor staff, be available for all knowledge transfer meetings, and ensure that their staffing is complete at the end of the transition period. The Contractor is not responsible for the incoming contractor's performance during transition.

- a. The plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including, devices, equipment, databases and systems. 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 Contractor proprietary or competitively sensitive information regarding its information, data, systems and processes used to execute this contract.

Optional PRF Reimbursement Quantities

The Government reserves the right to exercise additional quantities of PRF reimbursements. The PRF reimbursements are divided into multiple distributions, as determined by HHS/HRSA (See Task 2 of the PWS). See price schedule under Section B.3.

Performance Work Statement (PWS)
COVID-19 Claims Reimbursement to Health Care Providers and Facilities For Testing,
Treatment and Vaccine Administration for the Uninsured
Dated: April 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 January 7, 2021, the Secretary of Health and Human Services renewed the determination that a public health emergency still exists.

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.

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 and Facilities for Testing, Treatment, and Vaccine Administration for 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 appropriated \$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 provided \$100 billion in relief funds, including to hospitals and other health care providers on the front lines of the COVID-19 response, the PPPHCEA, which appropriated an additional \$75 billion in relief funds, and the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act, which appropriated an additional \$3 billion (Provider Relief Fund). Within the Provider Relief Fund, a portion of the funding will be used to support healthcare-related expenses attributable to the COVID-19 testing of the uninsured, treatment of uninsured individuals with COVID-19, and COVID-19 vaccine administration to the uninsured.

As part of the PPPHCEA, CARES Act, and CRRSA 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, for treating uninsured individuals with a COVID-19 diagnosis, and administering FDA-licensed or authorized COVID-19 vaccines to uninsured individuals. 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 to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured until all funds are expended.

Funding for claims reimbursement to health care providers will be limited to approximately \$10 Billion. The original FFCRA and PPPHCEA appropriations for testing related claims have been disbursed.

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 and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Program (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), lab tests for the virus, and vaccine administration 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. Exceptions may occur when Medicare does not publish a national rate and the contractor will utilize regional rates set by Medicare Administrative Contractors. 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, regardless of the result, 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).
 - Z11.52 – Encounter for screening for COVID-19 (asymptomatic).
 - Z20.822 – Contact with and (suspected) exposure to COVID-19.
 - Z86.16 – Personal history of COVID-19.
 - 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, 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).
 - Z11.52 – Encounter for screening for COVID-19 (asymptomatic).
 - Z20.822 – Contact with and (suspected) exposure to COVID-19.
 - Z86.16 – Personal history of COVID-19.
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, 87426.

- 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. Vaccine administration fees will be priced based on Medicare rates, including if Medicare raises the rate. Current reimbursement rates are outlined below:
- Administration of a single-dose COVID-19 vaccine (0031A) - \$28.39.
 - Administration of the first dose of a COVID-19 vaccine requiring a series of two or more doses (0001A, 0011A, 0021A) - \$16.94.
 - Administration of the final dose of a COVID-19 vaccine requiring a series of two or more doses (0002A, 0012A, 0022A) - \$28.39.
 - 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.

- 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.
 - Health care 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 perform an eligibility verification to ensure that the patient on the claim is not eligible for other insurance before payment.
- 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.

6. Claims Processing

- The microsite is the source of truth for all detail and guidance related to the testing, treatment, and vaccine administration for the Uninsured Program, including applicable coding and fee schedules for claims processing.
- If the contractor denies the claims after pre-processing, the provider should not resubmit the claim because all claim decisions are final; however, corrected claim submissions are not rejected from processing.
- A claim may be adjusted if it is determined that the claim was originally processed incorrectly, or Medicare has issued a retro-active change.
- Perform prepayment verification of patients' insurance status when a valid social security number is provided, to determine their eligibility by checking if the patient has healthcare coverage during the date(s) of service. The contractor will not issue a temporary member ID if valid health insurance coverage is found for the patient during the date(s) of service. The contractor completes an eligibility verification check of patient(s) to identify changes in eligibility that occurred after the request for payment was processed.

7. Payment Integrity

- (b) (4) [REDACTED]
- The contractor shall initiate discovery and requirements gathering, post-award, to conduct a feasibility assessment, develop a solution and propose a schedule and a price to implement and operationalize fraud detection for claims processing.
- To support patient verification using deceased patient information at the time of service, the contractor will be provided a file containing the deceased patients, including agreed upon identifiers, and corresponding date of death at a to be determined cadence. This file will be utilized to compare the date of service (DOS) and the date of death (DOD) upon receipt of patient roster upload via the portal and during the retrospective eligibility check process.
- If the requirement to have a valid social security number to determine patient

eligibility the contractor would incorporate that requirement into its existing processes. The contractor would conduct requirement gathering meetings with HRSA and develop a project plan with a timeline to implement the process.

8. Provider Communications

- Updates or content posted on the contractor-maintained education portal may also need to be published to the government website. Those changes, such as FAQs, on the government site are the responsibility of government marketing and communications team.
- Deployment of any social media content developed by the contractor, in collaboration with government will be executed by the government marketing and communications team.
- The contractor will leverage existing capabilities of the currently developed educational and testimonial videos when developing any new videos per the government's request. The contractor will work with the COR to assess feasibility, schedule, cost and impact if new capabilities are required for developing videos that COR requests.

9. Reporting:

- All reports and data-files will be delivered through (b) (4), secured-email or via Secure File Transfer Protocol (SFTP).
- No significant changes will be made to the layout, format, or cadence of the daily and weekly reports.
- Support for up to one (1) ad hoc report each month for the period of performance (POP).
- The contractor will work with the COR on developing and scheduling the change to add race/ethnicity to the weekly data files. This information is not currently being collected for uninsured patients, the updated weekly data files will include this information only for new patients after this change is implemented.

10. Audit Requests:

- Support for up to four (4) audit/data requests per month in the Base Period and up to three (3) audit/data requests per month in Option Period One and Two, each requesting data for up to ten (10) providers.
- COR and OIG will utilize the reports delivered to first to obtain the necessary information before submitting an audit/data request to the contractor.
- Turn-around time to fulfill each audit/data request can be up to three (3) weeks.
- Support up to one (1) Office of Management and Budget (OMB) A-123 audit per year.
- Contractor will support up to one data-pull, development of one report and attend one meeting for up to two (2) hours for each TIN investigation. If more than one data-pull, report or meeting is required for the same TIN investigation, subsequent requests will be counted as additional TIN investigations towards the total number of TIN

investigations conducted by the contractor during each contract period.

- The Contractor will support OIG interview requests by participating in one (1) meeting up to two (2) hours. If more than one meeting is required for the same OIG request. Additional number of units may be exercised as needed. Subsequent research and data requests resulting from the OIG interview will count towards the total number of TIN investigations conducted by the contractor during each contract period.

11. 1099 Processing

- Contractor will not support Puerto Rico reporting (Form 4806-SP/Form 1042-S).
- If a provider has previously established an account with the contractor and elected to receive electronic copies only, they will not receive a mailed copy.

III. 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 HHS Records Management Training before performing work under this contract, and thereafter completing the annual refresher course during the life of the contract. The training is located at https://humancapital.learning.hhs.gov/courses/2020recordsmanagement/01_index.html. At the end of the Records Management training, the “Congratulations” slide is considered your certificate of completion. Please send the completion certificates to the Contracting Officer Representative (COR) of the contract. 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.

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. Submit Program/Project Management Plan to COR.
- Establish and maintain the process for the claims reimbursement workflow with an end-to-end process.
- Meet Reporting and analytics requirements for claims processing.
- 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.
- Provision of full systems life cycle project management support for new and existing system functionality.
- 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 ten (10) 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, providing an agenda by 5:00 PM (Eastern Time) the day prior, and update the agenda

with action items and any corrections within 24 hours of the meeting.

- Provide project updates at these semi-weekly conference call meetings, and as requested by the COR. Up to four Ad hoc meetings will be scheduled per month as necessary. This is a total of twelve (12) meetings per month.
- Attend biweekly conference calls with the COR to discuss contract management and operations, providing an agenda by 5:00 PM (Eastern Time) the day prior, and update the agenda with action items and any corrections within 24 hours of the meeting.

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 3.5.1 – Monthly Status Reports

The Contractor shall:

- Provide the COR, PPM and other stakeholders a Monthly Status Report for each monthly reporting period, due on or before the 17th of each month. This report shall contain, as applicable, the following sections:
 - Project description.
 - Activities planned for the upcoming reporting period.
 - Activities performed during the prior reporting period.
 - Progress on deliverables as stated in the Project Management Plan.
 - Project issues and risks that may impact schedule, budget, and/or quality.
 - Provide financial management and reporting, including cost management.
 - Funding status.
 - Performance Metrics.
 - Number of claims reimbursed.
 - The number of attestations and claims reimbursements completed. This list must include information on Provider types and the geographic distribution.
 - The breakdown of testing versus treatment reimbursements.

The contractor will work with the COR on developing and scheduling the addition of the following information to the monthly report:

- The number of attestations and claims reimbursements completed. This list will include information on Provider types and the geographic distribution.

Task 3.5.2 – Weekly Reports

The Contractor shall:

- Provide a weekly report to the COR due on each Wednesday by 6:00 PM (Eastern Time). The Weekly Status Report shall be cumulative and contain key data, such as customer service summary statistics, and reimbursement and return details. The COR may request changes in the data on the weekly report.

Identified Weekly Report Titles:

- 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 and Testing 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 age, race/ethnicity, gender, and state of residence.

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, treating, and vaccinating 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 map showing uninsured patients for whom claims were submitted.
 - 16) Heat maps showing uninsured patients' submitted/state population.
- Daily Financial Report. This shall provide a daily payment reconciliation report to the COR and the Chief, Budget Execution and Management Branch that includes cumulative reimbursements to providers for “testing” “treatment” and “vaccine administration” 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 twelve ad hoc reports as requested by the COR per year, to ensure the performance of the Uninsured 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 – Risk Management

The Contractor shall:

- Create, maintain and submit to the COR a Risk Management Plan by identifying, documenting, analyzing, and prioritizing risks associated with the Uninsured Program. Manage and develop strategies to handle identified risks, and monitor the health of the program throughout its life cycle.

Task 3.7 – 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 3.8 – 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 3.9 – Performance and Quality Metrics

The Contractor shall:

Develop and implement contractor performance and quality metrics in the QASP. The COR will evaluate the contractor using these metrics on a weekly basis. HHS/HRSA will require frequent updates on total claims reimbursements to ensure that the COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured stays within statutory funding limits.

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

Task 4.1 – Provider Outreach and Education

The Contractor shall:

- Conduct webinars for Outreach and Education up to:
 - Base year: 2 webinars
 - Option year 1: 2 webinars
 - Option year 2: 1 webinar
- Develop testimonial videos up to:
 - Base year: 3 videos
 - Option year 1: 2 videos
 - Option year 2: 1 video
- Support email communications up to
 - Base year: 3.9 million
 - Option year 1: 636,000
 - Option year 2: 363,000

- 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 COR and OC on information and education that may need to be disseminated nationally through channels other than the contractor's website. Support up to:
 - Base year: Three testimonial videos
 - Option year 1: Two testimonial videos
 - Option year 2: One testimonial videos
- 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. Support up to:
 - Base year: Two webinars
 - Option year 1: Two webinars
 - Option year 2: One webinar

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.

- Contractor will ensure HRSA and HHS logos/branding are prominent on all materials developed under the contract. Contractor shall not use its own branding.
- 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 4.2 – Microsite

The Contractor shall:

- Provide input into the development of a landing page on its website to communicate overall program, FAQ's and provide key links for Health Care Providers to input data necessary for reimbursement of eligible COVID-19 testing, treatment, and vaccine administration claims.

- Develop content to support a provider educational website. The primary audience of the website will be the provider community serving the uninsured across the country.
- Provide up-to-date information on provider billing for COVID-19 related claims for the uninsured and include links to the CDC and other responsible sources for public health updates on this website. Site content shall follow Federal plain language guidelines at <https://plainlanguage.gov/guidelines/>.

Task 4.3 – Stakeholder Communications

The Contractor shall:

- Coordinate external communications related to the work contained in this PWS with Federal stakeholders and professional associations, which includes targeted email messages, promotional toolkits, fact sheets, and videos/graphics, etc.
- Create social media plans and content to address eligible provider concerns in coordination with HRSA 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 communications branch and subject to HRSA OC and HHS ASPA approval.

Task 4.3.1 – 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.
 - Respond to TIN investigation requests:
 - Base year: up to 140 individual TIN investigations
 - Option year 1: up to 120 individual TIN investigations
 - Option year 2: up to 120 individual TIN investigations
 - Respond to A-123 audits.
 - Base year: up to 1 A-123 audit
 - Option year 1: up to 1 A-123 audit
 - Option year 2: up to 1 A-123 audit
 - Respond to OIG interview requests.
 - Base year: 25 interviews
 - Option year 1: 25 interviews
 - Option year 2: 25 interviews
 - Data requests shall be fulfilled within 3 business days of request from the COR. Where circumstances make meeting that deadline unfeasible, notify COR within 2

- business days with the reason(s) for the delay and request new data submission date.
- Urgent data reports shall be fulfilled within 1 business days of request.
 - Written extension is requested and approved by the designated POC and the COR.
 - Some requests may involve data that may be withheld under the terms of the Privacy Act of 1974, as amended (5 U.S.C. ' 552a), the Trade Secrets Act (18 U.S.C. ' 1905), the Freedom of Information Act (FOIA) (5 U.S.C. ' 552), or other applicable laws. For example, any personally-identified or personally identifiable data maintained in the OPTN/SRTR/HRSA Data System of Records, HHS/HRSA/HSB/DoT, No. 09-15-0055, including data maintained electronically, must be disclosed consistent with the Privacy Act and the Systems Routine Uses, outlined in the applicable System of Records Notice (73 Fed. Reg. 19519, as amended).
- Notify through the designated POC and the COR within 3 days of the request 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 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.
- Retain all data and provide reports with specific factors as determined by the COR including cross referencing providers attestations and submissions with claims reimbursement data. Perform retrospective review of claims reimbursements to ensure that Providers' attestations were compliant with their patients' defined uninsured status.
- 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. Maintain a list of the providers that have been required to register with such bank.

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.
- Detect and notify the COR within one (1) calendar day from when fraudulent activity is detected and/or when an entity that is under investigation by any other Federal Government agency that submits a claim
- 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 all financial transactions, such as:
 - Interface with the bank.
 - Accept wire transfers.
 - Return any returned funds to HHS on a weekly basis.
- Disburse claims reimbursements daily, Monday through Friday, with the exception of any Federal Reserve Bank holidays.

Task 7 – Claim Processing

The Contractor shall:

- Process claims billed
 - Base year: Up to 42,862,928
 - Option year 1: Up to 7,000,000
 - Option year 2: Up to 4,000,000
- Auto-adjudication rate of claims
 - Base year: 98%
 - Option year 1: 98%
 - Option year 2: 98%

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 a coordination of benefits for individuals with limited or supplemental Medicaid coverage.
- Perform an eligibility verification to ensure that the patient on the claim is not eligible for other insurance
- Provide HRSA with adjudicated claims upon request.

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 Medicare Revocation List.
 - CMS Medicaid Termination List.
 - CMS Compliance Holds.
 - 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.

See price schedule under Section B.2 for payment quantities.

Task 7.3 – Back-End Processing

The Contractor shall:

- Perform a back-end processing to close out and verify claims payments. Reconfirmation of each claim's eligibility after 30-days, 60-days, and 90-day to review for improper payments.
- Provide a report to HRSA every two weeks identifying overpayments or improper payments.
- For claim overpayments the contractor shall off set future claims to correct the overpayments.

Task 7.4 – Remittance Advice

The Contractor shall:

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

Task 8 – Financial Management and Claims Reimbursements

The Contractor shall:

- Process claims paid
 - Base year: Up to 29,488,437
 - Option year 1: Up to 3,000,000
 - Option year 1: Up to 1,000,000

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 as 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, treatment, or vaccine administration 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.
- Validate that the funds have been received in the contractor’s bank account.
- Maintain a record of the claims reimbursed to eligible providers, broken down by testing, treatment, and vaccine administration and submit this “FedFile” on a daily basis to the HRSA finance team as coordinated by the COR.

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 claims 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 EIN associated with the program bank account, the contractor's legal business name, and the date of the request.
- Identify the reimbursements as "testing", "treatment", or "vaccine administration" within 24 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 weekly 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 quality assurance and payment integrity capabilities and use Contractor defined processes to ensure reimbursements are processed accurately and without duplication. Submit the process to the COR.
- Have reporting capability consistent with Reporting requirements of this program for claims reimbursement transactions and audits, and shall comply with all HHS/HRSA Security requirements.

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 on a daily basis or otherwise

determined by the COR. 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's Office of Provider Support (OPS)/Division of Data Analytics and Program Integrity 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 by 1:00 PM (ET) 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:

- Process ACH transactions for TINs/Providers registered in UHG/Optum Pay system or HHS wire through Optum Bank ACH, up to:
 - Base year: 636,000 ACH transactions
 - Option year 1: 64,000 ACH transactions
 - Option year 2: 21,000 ACH transactions
- 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 designated bank account for HRSA's Uninsured Program. Upon receipt, contractor's bank will release the corresponding ACH reimbursements to health care providers serving the uninsured for COVID-19 claims for testing, treatment, and vaccine administration 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:

- Review Provider Attestation Documents.
- Perform prepayment verifications of patients' insurance status.
- Use other health information and deceased patient information at the time of service.
- 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:

- Provide post-pay support for Payment Integrity (includes (b) (4) (b) (4) for up to:
 - Base year: 222,000 claims
 - Option year 1: 22,000 claims
 - Option year 2: 7,000 claims
- 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 source account(s), 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.
- Provide HRSA with aggregate list of providers with over payment who stopped billing

for a period of 30-days after being identified as having received overpayments. Submit this process to the COR.

- If 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 or repayments.
- Develop a methodology or procedure to recover claims reimbursements, including: contacting the provider, bank returns, letter of identification, issuing demand letters, etc.
- 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:

- Process unique 1099s up to:
 - Base year: 225,000
 - Option year 1: 22,000
 - Option year 2: 7,000
- 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 Uninsured Program. 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 ET to respond to provider telephone inquiries.
 - Establish the infrastructure to adequately support call volume. Support up to:
 - Base year: 204,000 calls
 - Option year 1: 34,000 calls
 - Option year 2: 19,000 calls
 - 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, treating, and vaccinating 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 9.2 – Email

The Contractor shall:

The Uninsured Program receives a variety of documents via email. All emails must comply with the HHS Visual Style Guide and HHS logo policy.

- Establish, operate and maintain email operations.
- Manage the inventory of all the forms and templates incoming and outgoing correspondence.
- Track and electronically store any and all information related to outgoing and returned email correspondence.

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 a demo and screenshots of each provider facing system after each system change to the COR.
- 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.

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.
- Provide support to evaluate cases involving complex policy questions or business rules.
- 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.
- Proactively identify data anomalies and work to help HRSA improve the reliability and integrity of the data:
 - 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. Safeguarding Information and Information Systems. In accordance with the Federal Information Processing Standards Publication (FIPS)199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:

Protect government information and information systems in order to ensure:

- Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - Availability, which means ensuring timely and reliable access to and use of information.
4. 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.
5. Adopt and implement the policies, procedures, controls, and standards required by 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.
6. 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 NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and
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 OMB Memorandum M-06-16, Protection of Sensitive Agency Information by securing it with a FIPS 140-2 validated solution.

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 HHS and HRSA policies. Unauthorized disclosure of information will be subject to the HHS/HRSA 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).

G. Internet Protocol Version 6 (IPv6). All acquisitions using Internet Protocol shall comply with FAR sections: FAR 7.105(b) (5), FAR 11.002(g), and FAR 12.202(e).

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). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

I. Contract Documentation. The Contractor shall use HRSA-provided templates, policies, 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 HHS 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.) with FIPS 140-2 validated encryption solution.
3. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and HRSA-specific encryption standard requirements. 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).

4. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2 at <https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf>. The Contractor shall provide a written copy of the validation documentation to the COR prior to the EPLC Design Readiness Review (DRR).
5. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

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 F), 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 with FIPS 140-2 validated encryption.
- 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, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HRSA EPLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012).
2. System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
3. 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.
4. 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.
5. 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.

6. 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. Federal Policies. The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the HHS Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
2. 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:
 - System Security Plan (SSP) – Initial draft version due within 30 days of the EPLC Performance Baseline Review. Final draft due 120 days prior to the Operational Readiness Review. Final version due 30 days prior to the Operational Readiness Review.
 - The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing

Standard (FIPS) 200, Recommended Security Controls for Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS and HRSA policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter.

- Security Assessment Plan/Report (SAP/SAR) – due 30 days prior to the Operational Readiness Review. The security assessment shall be conducted by HRSA's Security Assessment Team and be consistent with NIST SP 800-53A, NIST SP 800-30, latest revisions, and HHS and HRSA policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with HRSA shall assist in the assessment of the security controls annually and update the SAR at least annually.

- 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.

- E-Authentication Questionnaire – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, Electronic Authentication Guidelines.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

- 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 FISMA and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and HHS IS2P. 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.
- Asset Management - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. The inventory information is required to be produced within 30 days of the EPLC Performance Baseline Review. Final version due within 30 days prior to the Operational Readiness Review and reviewed and updated on a monthly basis thereafter. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
- Configuration Management - Use available SCAP-compliant automated tools, per NIST IR 7511, 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 standard HHS and government configuration baselines prior to the EPLC Operational Readiness Review. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

- Vulnerability Management - Use SCAP-compliant 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 HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. If externally-hosted and HRSA is unable to directly scan the system/application, the contractor (and/or any subcontractor) shall provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency prior to the EPLC ORR and at least monthly thereafter and upon request.
 - 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, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and 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. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.
 - b. The Government includes but is not limited to 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.
 - c. 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, but is not limited to, 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. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
 - d. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
 - e. 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 HHS and FIPS 140-2 encryption 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
- e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
- f. Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

S. HHS FedRAMP Privacy and Security Requirements

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

1. FedRAMP Compliant ATO. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.
 - a. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline at www.FedRAMP.gov. The HHS Information Security and Privacy Policy (IS2P) and HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance further define the baseline policies as well as roles

and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.

- b. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
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 contractor shall support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
 - a. Maintenance of links between records and metadata, and
 - b. 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.

5. 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.
6. 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.

A SORN is in development by Program.

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

1. The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/HRSA security policies.
 - a. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the HRSA authorizing official (AO) prior to implementation of system and/or service being acquired.
 - b. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
 - c. For all acquired cloud services, the SA&A package must contain the following documentation:
 - 1) Privacy Impact Assessment (PIA).
 - 2) FedRAMP Test Procedures and Results.
 - 3) Security Assessment Plan (SAP).
 - 4) Security Assessment Report (SAR).
 - 5) System Security Plan (SSP).
 - 6) IT System Contingency Plan (CP).
 - 7) IT System CP Test Results.
 - 8) Plan of Action and Milestones (POA&M).

- 9) Continuous Monitoring Plan (CMP).
 - 10) FedRAMP Control Tailoring Workbook.
 - 11) Control Implementation Summary Table.
 - 12) Results of Penetration Testing.
 - 13) Software Code Review.
 - 14) E-Authentication Questionnaire.
 - 15) System of Record Notice (SORN).
 - 16) Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.
- d. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/HRSA policies.
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. HRSA will determine the risk rating of vulnerabilities using FedRAMP baselines.
 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 the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/HRSA configuration baseline.
2. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations 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.
3. Non-Repudiation. The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

Optional Tasks – Not funded unless exercised.

Optional Task 1 – 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.
 - Ensure transition of all provider documentation about eligible reimbursement claims to the new contractor responsible for the next phase of the contract with minimal disruption.
 - Include the transition of the documentation, operating procedures and other resources, including, all data generated as a result of this contract.
 - Develop a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees. The plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including, devices, equipment, databases and systems. 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 Contractor 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 Contractor staff, be available for all knowledge transfer meetings, and ensure that their staffing is complete at the end of the transition period. The Contractor is not responsible for the incoming contractor's performance during transition.
- 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.

Optional Task 2 – Fraud Detection

- Implement fraud detection processes equivalent to commercial standards for processing claims. Detect and notify the COR within one (1) calendar day from when fraudulent activity is detected and/or when an entity that is under investigation by any other Federal Government agency that submits a claim. Payments shall not be issued to an entity in the event that fraudulent activity is detected and/or the entity is under investigation by any other Federal Government unless approval is given by the COR.

Optional Quantities

1. Optional Fee per Submitted (billed) Claims, Fee per Paid Claims, OIG Interviews and TIN Investigations.

The Government reserves the right to exercise additional quantities of Fee per Submitted (billed) Claims, Fee per Paid Claims, OIG Interviews and TIN Investigations. The Fee per Submitted (billed) Claims, Fee per Paid Claims, OIG Interviews and TIN Investigations are divided into multiple distributions, as determined by HHS/HRSA (See Task 4, 7 and 8 of the PWS). See price schedule under Section B.3.

**Performance Work Statement (PWS)
Claims Processing Services for Provider Relief and Protection Fund (PRF)
Department of Health and Human Services (HHS)
Health Resources and Services Administration (HRSA)**

March 9, 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 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 COVID19 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 27, 2020, the Coronavirus Aid, Relief and Economic Security (CARES) Act (P.L. 116 - 136) became law. The CARES Act provides economic and financial support for individuals and business impacted by the coronavirus outbreak. To provide relief, Congress appropriated funding from the Public Health and Social Services Emergency Fund to reimburse eligible health care providers for health care related expenses or lost revenues that are attributable to coronavirus.

Provider Relief Fund legislation specifies that eligible health care providers may receive a payment or be reimbursed for health care related expenses or lost revenues that are attributable to coronavirus that have not been reimbursed from other sources or that other sources are obligated to reimburse. Eligible health care providers are public entities, Medicare or Medicaid enrolled suppliers and providers, and other entities the Secretary may specify, that provide diagnoses, testing, or care for individuals with possible or actual cases of COVID-19. The CARES funds can be used to provide a payment or reimburse eligible providers for lost revenues and costs related to the coronavirus outbreak including building or construction of temporary structures, leasing of properties, medical supplies and equipment including personal protective equipment and testing supplies, increased workforce and trainings, emergency operation centers, retrofitting facilities, and surge capacity.

In addition, the Paycheck Protection Program and Health Center Enhancement Act provides \$225M in additional funding for COVID-19 testing and related expenses, through grants or other mechanisms, to rural health clinics as defined in section 1861(aa)(2) of the Social Security Act,

with such funds also available to such entities for building or construction of temporary structures, leasing of properties, and retrofitting facilities as necessary to support COVID-19 testing: Provided further, that such funds shall be distributed using the procedures developed for the Provider Relief Fund authorized under the third paragraph in division B of the Coronavirus Aid, Relief, and Economic Security Act (Public Law 116-136); may be distributed using this contract.

II. Purpose and Scope

The purpose of this contract is the disbursement of payments to eligible health care providers for health care related expenses and/or lost revenues that are attributable to coronavirus. Based on the direction and information provided to the Contractor by HRSA and HHS, the Contractor shall process and distribute payments to eligible providers, provide customer service education, data support, outreach and escalation of provider issues, and project management for the Provider Relief Fund and related provider relief legislation as authorized by Congress. Subject to the Changes clause, additional related funding, greater than the \$175B currently authorized for COVID-19 or provider relief disbursements and/or reimbursements may be distributed through the Provider Relief Fund as authorized by public law, using the procedures and agreements developed under this contract.

The scope of this activity includes:

1. Project Management
2. Payment Distribution
 - a. Electronic Payment
 - b. Paper check payments
3. Payment Terms and Conditions Attestation
 - a. Create a new or leverage an existing web portal to ingest attestations for payment acceptance and/ or documentation
4. Reconciliation
 - a. Paper Remittance
 - b. General Payment Processing
 - c. Payment Recovery
 - d. Back-End Processing
 - e. Remittance Support
 - f. Attestation by the Provider
5. Provider Customer Service Program
 - a. Education and Outreach
 - b. Call Center
 - c. Microsite
6. Provider Payment and Integrity
7. Compliance Reporting Support
8. Data Security

III. Period of Performance / Place of Performance

A. Period of Performance

The period of performance is for a Base period of 12 months (April 07, 2020 - April 06, 2021).

B. Place of Performance

Work shall be performed under this contract off-site, primarily at the contractor's facilities, which includes work performed by staff that telecommute.

IV. General 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, using existing systems and processes, 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 Government assumes complete responsibility for the accuracy and sufficiency of the information and data provided to the Contractor, to include information concerning the providers to whom relief payments should be disbursed, the amount that each eligible provider is paid, and the communication related to disbursements process by the Contractor.

V. Tasks

The Contractor shall perform the following tasks:

Task 1 – Project Management Support

This task details the contractor's responsibilities for managing the overall contract performance, personnel, project planning, and project scheduling. Total responsibility for overall direction for program project work will fall under the direction of the Government.

The Contractor Shall:

- Be responsible for PRF Project Management.
- Execute program and project objectives and priorities as directed by the Government.

Project Management activities include:

- Management of personnel;

- Utilizing existing commercial processes and procedures for PRF operations and contract management;
- Management of subcontractors as appropriate;
- Establish effective communications and reporting procedures with HRSA;
- Proper financial management of the contract funds;
- Other program management tasks necessary to meet the requirements of this contract;
- Providing systems project management support for new portal functionality;
- Overall scheduling and resource management; and
- Risk management document control

Task 1.1 – 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's 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 1.2 – Kickoff Meeting

The Contractor Shall:

- Meet with the COR and other HHS representatives to discuss current activities, communications, and the contracting process. The objectives of the kickoff meeting are to:
 - Initiate the communication process between HHS and the contractor by introducing key project participants and identifying their roles.
 - Ensure the contractor understands the expectations of key stakeholders regarding the scope of work and the effort described in this contract, including task requirements and objectives.
 - Review communication ground rules.

Task 1.3 – Conference Calls

The Contractor shall:

- Chair weekly/bi-weekly conference calls with HHS/HRSA representatives.
- Facilitate project updates and ad hoc reports. Ad hoc meetings will be held within 24 hours of a request by the Contractor or the COR.

Task 1.4 – Reports

The Contractor Shall:

Provide the following reports in the Contractor's format:

Name of Report	Description	Format (Word, Excel, Data File, etc)	Cadence
ACH Payment File	Payment data reporting for each transaction by provider billing TIN for ACH transactions	Data File via (b) (4)	Daily
Check File	HHS requests banking data reporting for each transaction. Payment data reporting for each transaction by provider billing TIN for checks.	Data File via (b) (4)	Daily
Daily Contractor HHS CARES Act Update	Summary reporting for payments and operations and attestation reporting rolled up by status and Distribution #	Email	Daily
Attestation/Demographic Detail	Detailed attestation demographics reporting by provider TIN	Data File via (b) (4)	Twice Weekly – Wednesday and Friday
Provider Populations Phase/Wave Report	Detailed Phase/Wave grid that shows descriptions, dollar amounts, and dates of disbursements.	Word doc via Email	Daily

Task 1.4.1 – Risk Management

The Contractor Shall:

- Use its standard risk management practices.

Task 1.5 – Project Management

The Contractor Shall:

- Facilitate requirements workshops:
 - Update the application portal, attestation portal, or payment process.
 - When the external facing portal or web pages are updated such as the Attestation Portal, Application Portal 1.0, Application Portal 2.0, provide a walkthrough of the process of the provider experience, the Contractor is only expected to walkthrough and document the parts of the system they manage.
 - Participate in requirements meeting related to distributions or process of additional eligible providers within a distribution as defined by HRSA or HHS in a timely manner, except that Contractor shall not be required to participate in requirements meetings regarding funding exceeding the currently authorized amount of \$175,000,000.00.

- Document HRSA requirements for the PRF payment processing.
- Discuss and document technical requirements to collect a daily extract file from the contractor's accounting system.
- Maintain a history of payments.

Task 2 – Provider Payment

The PRF will be divided into multiple distributions, as determined by HHS/HRSA.

The Contractor Shall:

- Use its existing systems to:
 - Manage file transfers, control funding transfer requests, chain of custody, and money transfer workflow;
 - Implement and perform reconciliation controls to ensure funding transfer accuracy;
 - Provide a payment system that manages financial transactions, such as:
 - Interface with the bank,
 - Accept wire transfers, check, and ACH,
 - Remit returned funds to HHS on a daily basis,
 - Reconcile and trace ACH and check payments to each distribution.
 - Disburse payments at intervals determined by HHS/HRSA.
 - Process checks on a cleared basis and request reimbursement.
 - Process payment files with HHS/HRSA provided ACH addenda record descriptors.

Task 2.1 – Financial Management and Payment Distribution

The Contractor Shall:

- Distribute payments to eligible providers using files provided by the COR and approved by HHS/HRSA (Payment Files).
 - The HHS files will include eligible providers, their TIN number, Provider address, phone number, amount of payment, and the ACH bank account information (if available).
 - Use this information to make ACH or check payments to eligible providers in the amount specified by the Payment file via Optum Pay ACH, CMS ACH, provider submitted ACH (Portal 2.0) or paper check.
 - Use the approved Wire Transfer Instructions and execute the Wire Transfer Instructions to HHS using an FDIC-protected Bank Account (“Bank Account”) as described in the TriPartite Agreement among the parties dated April 8, 2020.
 - Validate that funds have been received in the Contractor's bank account.
 - Use and maintain a record of the ACH Addenda Record character descriptor approved by the HRSA designee for each ACH payment to eligible providers listed in Payment files.

Task 2.1.1 – Electronic ACH Payments

The Contractor Shall:

- Distribute the funds in accordance with Payment Files using industry best practices and confirm distribution of funds within 24 hours.
- After distribution by ACH of each Payment File, the process will identify failed transactions and payment errors arising from the distribution and provide data files to the COR within 24 hours.
- As determined by the COR or designee, contact providers as appropriate to re-originate payment.
- Recommend a process for non-acceptance of payment, non-attestations and other forms of non-acceptance by the Providers and will implement the process approved by HHS/HRSA.
- Return to HHS funds that are not accepted or returned by providers.
- Send, track, and reconcile paper checks issued to providers.

Task 2.1.2 – Paper Checks

The Contractor Shall:

- Send paper checks to eligible providers from the HHS Payment Files that do not have an ACH account on file with Optum Pay, HHS/HRSA or will not accept an electronic payment.
- Fund the payment of the check; upon the presentment of the check by the eligible provider for payment.
- Request reimbursement from HRSA and track each check amount presented for payment by each eligible provider.
- Implement a standard commercial process to create and distribute checks.
- Develop and implement a process for undeliverable checks (returned mail per Task 3.1),
- Develop and implement a process to handle provider checks returned by mail, including reconciliation to the amount paid, and returning the funds to HHS/HRSA with associated reporting.
- Implement the HHS/HRSA policy as directed for checks that do not get cashed within a specified number of days, and
- Implement a process agreed with HHS/HRSA for providers that do not attest within the time period established by HHS/HRSA.
- Return payments rejected by eligible providers to HRSA per treasury instructions.
- Track and reconcile paper checks to providers by disbursement Wave and funding request who cannot receive an ACH payment as determined by program policy.

Task 2.1.3 – Payment System

The Contractor Shall:

- Establish a payment system that will:

- Provide the required accounting, firewalls, and funds control capabilities to ensure that all Treasury deposits and financial transactions are managed, maintained, and reported separately in a segregated bank account;
- Manage, maintain and report payments;
- Be capable of auditable funds control and management of all deposits and transactions;
- Have quality assurance and payment integrity capabilities to ensure payments are processed accurately and without duplication;
- Have full and ad hoc reporting capability for all financial transactions and shall comply with all HHS/HRSA security requirements.

Task 2.1.4 – Approved Bank Account

The Contractor Shall:

- Maintain a bank account capable of processing and managing all financial transactions in accordance with the Tripartite Agreement with the Bank and HRSA.
- Maintain a separate and dedicated bank account for the Provider Relief Fund.
 - Return interest gained in the account to HRSA via wire transfer on a routine basis determined by the COR.
 - Provide account safeguards, monitoring and access controls to PRF related financial transactions.
- Use the identified and agreed upon account to disburse payments.
- Return surplus funds received from providers due to voluntary returns to HHS/HRSA.

Task 2.1.5 – IRS 1099s to Payee

The Government shall provide Contractor with a file identifying providers who shall receive an IRS 1099-MISC, and the amounts paid to each provider under this program in the relevant calendar year.

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 February 1st, 2021 to all payees that received payments during the prior calendar year for payments made in 2020. Any payments or adjustments that extend beyond 2020 are the responsibility of the government.
- Send the electronic 1099 file with this information to the IRS in accordance with the IRS reporting deadline.

Task 2.2 – Financial Management and Reporting

The Contractor Shall:

- Establish and maintain a payment integrity plan consistent with its commercial practices

that ensures internal contractor controls that comply with payment process and bank regulatory standards.

Task 2.2.1 – Financial Accounting System

The Contractor Shall:

- Host the financial accounting system responsible for making payments.
- Secure routine and ad hoc execution of payment files;
 - Secure processing and storage of all payment records;
 - Secure reporting and file transfer capabilities;
 - Secure interface with other HHS/HRSA internal systems and external systems such as US Treasury, and
 - Ensure disaster recovery capabilities.
- Operate and maintain the financial accounting system.
 - Secure routine and ad hoc execution of payment files;
 - Secure processing and storage of payment records per Contractor’s records retention program – See Task 7 – Records Management;
 - 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 with a daily extract of financial data from contractor’s financial accounting system.
 - Provide detailed banking data files as necessary from the financial accounting system, excluding Optum Pay provider bank account information, that provides details of all financial transactions, including ACH, and check payments; original ACH payments shifted to paper check; re-issued payments, payments flagged for stop payment, checks cashed, etc. with the fields and columns agreed to by the HRSA financial oversight designee.
 - Coordinate with and provide the file structure, data elements, data dictionary, etc. to the HRSA financial oversight designee.
- Reconcile payment files with actual payments made and their payment method (ACH, paper check, re-issuance, etc.) or return type to ensure payments can be traced back to initial funding requests.

Task 2.2.2 – Payment Files

The Contractor Shall:

- Work with HHS/HRSA and designee project staff to develop a standardized payment file format.
- Provide a timeline of the deposit date for eligible providers paid via ACH for each Payment File.
- Ensure each Payment File recipient has ACH payment instructions as possible.
- Track each Payment File distribution amount, distribution date.

- Provide notification to HHS/HRSA of all returned ACH and check payments, including the ACH addenda record.
- Review payment files for quality control, ensuring that each provider has a TIN and a payment amount, and that the file totals agree with amounts communicated by HRSA.

Task 2.2.3 – Funding Requests

The Contractor Shall:

- Send payment requests to the COR for approval and funds certification at a duration of one (1) Business day prior to the submit date during a payment cycle.
- Distribute the total funds requested for the payment requests.
- For payments made by check, include itemized payment totals by distribution such as cleared checks, the Contractor's legal business name, and the date of the request.

Task 2.3 – Payment Returns

HHS/HRSA shall be responsible for recovering funds from providers.

The Contractor Shall:

- Maintain a procedure for handling returned funds from providers.

Task 3 – Customer Support Services for Internal and External Users

The Contractor Shall:

- Establish a Customer Service Program to respond to provider telephone and email inquiries in an accurate and consistent manner to ensure satisfactory quality and performance standards are met as defined in the bullets below. In support of customer service, includes:
 - Provide Call Center Services from 8:00am to 8:00pm in continental U.S. time zones, Monday-Friday.
 - Establish the infrastructure to adequately support call volume; provide updates to IVR, training, and application access.
 - Review available PRF information to draft general responses to incoming questions. Define FAQ and talking points using information provided by HHS regarding the program.
 - Coordinate HHS/HRSA on response plans for external correspondence.
 - Provide effective provider education to answer questions and promote appropriate steps for payment requests related to eligibility, status, and application process as well as inquiries related to technical issues, such as Attestation, DocuSign, ACH and check troubleshooting.
 - Maintain a high level of provider service and satisfaction through good communication and relationships with providers.
 - Train call center staff to handle calls or emails from providers and conduct additional

- training as needed should changes in process or complexity require it.
- Provide Federal Telecommunications Services (FTS) lines for toll-free access to the customer support service.
- Create a defined internal escalation and issue tracking process with input from HRSA to review and respond to questions and to transfer escalated issues to HRSA to resolve.

Task 3.1 – Mail and Correspondence

The PRF receives a variety of documents via email and conventional mail. All forms and envelopes must comply with the HHS/HRSA Visual Style Guide and HHS/HRSA logo policy.

The Contractor shall:

- Establish, operate and maintain mail operations.
- Manage the inventory of all the forms and templates for outgoing correspondence. Process, print, and mail paper checks and letter to providers as defined by Task 2.
- Process forms and related correspondence as necessary to satisfy provider payment requirements.
- Receive and deposit check returns from providers with associated accounting reconciliation to the distributed amount and provider outreach.
- Track and electronically store information related to mailed checks and returns from check mailings for address correction and, incoming checks mailed by providers.

Task 3.2 – Communications

The Contractor Shall:

- In coordination with and subject to the approval of HHS/HRSA, define communications and touchpoints with eligible providers for pre-payment, payment, and post-payment distributions and implement them on HHS/HRSA's behalf. HHS/HRSA will provide approved communication to the Contractor advising the eligible provider of the payment and required provider action. Contractor will distribute the HHS/HRSA provided communication to eligible providers provided by HHS/HRSA via email or letter, as applicable.
- Subject to approval by HHS/HRSA, draft emails and letters addressed to the Providers regarding relief fund payment distributions.

HHS/HRSA Shall:

- Provide Contractor with all attestation language and will post all attestation language for each Payment File or distribution to HHS/HRSA's website.
- Provide a plain language description of the formula describing the calculations used to determine the payment to eligible providers in each Payment File

HHS/HRSA provides to the Contractor. Contractor will include the HHS/HRSA provided formula description in communications to providers.

Task 3.3 – Provider Outreach and Education (POE)e

The Contractor Shall:

- Educate providers about the PRF via phone and email through customer support, system portals, webinars and focus groups in coordination with HHS. POE may be delivered to groups, to individuals and through various media channels in consultation with HRSA COR and Subject Matter Experts.
- Research and resolve inquiries received outside of the contact center.
- Follow up with providers as requested by HRSA to resolved complex policy questions.

Task 4 – IT Services

The Contractor Shall:

- Be responsible for management of contractor provided software resources and for coordinating with other program systems (e.g. CA Agile, DocuSign, etc.) to perform the activities of PRF.
- Provide resources to support operations and corrective maintenance of supporting software.
- Provide a demo or screenshots of each Provider facing system after each system change to the COR.
- Provide both emergency and routine system support as needed within agreed upon timeframes and standard Provider deployment windows as consistent with the normal course of business.
- Ensure all contractor owned contractor operated (COCO) and commercial off the shelf software (COTS) software is maintained, patched, and updated to maintain or exceed the security baseline identified in the security task.

Task 4.1 – Microsite Support

The Contractor Shall:

- Provide input into the development of a landing page to communicate overall program, FAQ's and provide key links at <https://hhs.gov/providerrelief>.

Task 4.2 Attestation Portal

The Contractor Shall:

- Implement and maintain a portal based on HHS/HRSA provided requirements to allow

eligible providers to submit their required attestations to accept or reject payments received.

- Implement methodology as approved by HHS/HRSA to validate the provider is authorized to accept or reject the terms and conditions.
 - For example, use the payment file to validate provider information including Tax Identifier Number/TIN (either EIN or SSN), Account Number (if ACH), Check Number (if Physical Check), Payment Amount, and Date (if multiple payments were issued to exact same provider on different days).
- Configure the portal so that it can be closed.
- Retain all data and provide reports with specific factors as determined by the COR including cross referencing a provider's attestation with and payment disbursement status.
- Perform post processing of attestation data to reconcile the provider attestation status to match the provider's payment action status as defined by PRF policy. For example, adding additional meta-data to the original record post attestation to indicate the provider's acceptance or rejection based on their retention or return of the provider payment.
 - Maintain the integrity of the original provider records.
 - Clearly identify added reconciled status meta-data.
- Provide regular reports and ad hoc reports as requested by the COR on portal use and data submitted to the portal.

Task 4.3 – Software Quality Control and Systems Development Management Plan

The Contractor Shall:

- Implement quality standards for all Contractor managed systems that meet the standards of auditability, confidentiality, availability, integrity, and quality and compliance practices associated with the distribution of payments, handling of Personally Identifiable Information (PII), customer service and reporting.

Task 4.4 – Provider Applications

The Contractor Shall:

- Provide and maintain mechanisms to collect information from providers (i.e. Portal 1.0 and Portal 2.0) and perform validation checks on the input format of the data so that HHS can determine program eligibility.
- Support the integration of a provider application with the Attestation Portal and other validation mechanisms.
- Integrate and maintain the integration of the provider applications with the DocuSign system forms, ensuring that data collected in DocuSign is not accessible to Contractor, except the envelope status.
- Maintain the ability to verify provider TIN with IRS to ensure the TIN exists and inputted TIN name is valid as well as the IRS TAF list of fraudulent providers.

Task 4.5 – 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 5 – Support for Program Operations

This task section identifies Contractor specific requirements for program tasks such as compliance and disputes.

Task 5.1 – Compliance

The Contractor Shall:

- Provide reporting per Task 1.4. HRSA shall review the reporting provided in order to:
- Support HRSA in executing planned and focused compliance efforts.
- Support compliance efforts by other contractors.
- Support assessment of attestation compliance.
- Evaluate cases involving complex policy questions or business rules.

Task 5.2 – Payment Dispute Process

The Contractor Shall:

- At any time, a provider may dispute their eligibility to receive payment or the payment they received, including, but not limited to overpayment, underpayment, or incorrect payments such as change of ownership.
- When a dispute is reported to the call center, the Contractor will attempt to clarify the dispute first with the available policy information, if it cannot be resolved the contractor shall escalate the dispute to HRSA. Escalated cases are sent daily to ProviderReliefContact@hrsa.gov.

Task 6 – Security Requirements

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

- a. 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.
- b. 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.

2. Safeguarding Information and Information Systems. In accordance with the Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:

- a. Protect government information and information systems in order to ensure:
 - Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - Availability, which means ensuring timely and reliable access to and use of information.
- b. 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.
- c. Adopt and implement the policies, procedures, controls, and standards required by 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.
- d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.

3. Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST Special Publication (SP) 800-60, Volume II: Appendices of Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, 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

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

4. 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:

- a. marked appropriately;
- b. disclosed to authorized personnel on a Need-To-Know basis;
- c. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and
- d. 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.

5. 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 OMB Memorandum M-06-16, Protection of Sensitive Agency

Information by securing it with a FIPS 140-2 validated solution.

6. 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 HHS and HRSA policies. Unauthorized disclosure of information will be subject to the HHS/HRSA sanction policies and/or governed by the following laws and regulations:

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

7. Internet Protocol Version 6 (IPv6). All acquisitions using Internet Protocol shall comply with FAR sections: FAR 7.105(b)(5), FAR 11.002(g), and FAR 12.202(e).

8. 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). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

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

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

- a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
- b. 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.) with FIPS 140-2 validated encryption solution.

- c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and HRSA-specific encryption standard requirements. 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).
- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR prior to the EPLC Design Readiness Review (DRR).
- e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11. 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, 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.

12. 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.

- a. 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.
- b. 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.

13. Training.

- a. 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.

- b. **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.
- c. **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.

14. Rules of Behavior.

- a. 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.
- b. 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.

15. Incident Response.

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.

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”.

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 with FIPS 140-2 validated encryption.
- 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:
 - 1) cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
 - 2) not include any sensitive information in the subject or body of any reporting e-mail; and
 - 3) encrypt sensitive information in attachments to email, media, etc.
- d. 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.
- e. 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.

16. Position Sensitivity Designations.

All Contractor (and/or any subcontractor) employees accessing HRSA systems must obtain a background investigation commensurate with their position sensitivity designation that complies

with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

TBD

17. 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, with a copy to the Contracting Officer, 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.

18. Contract Initiation and Expiration.

- a. General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HRSA EPLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012).
- b. System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
- c. 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.

- d. 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.
- e. 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.
- f. 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.

19. Contractor Owned Contractor Operated System Security Requirements.

- a. Federal Policies. The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the HHS Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53, Security and Privacy Controls for Federal Information Systems and Organizations; Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
- b. 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).

For an existing ATO, HRSA must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such.

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.

1) 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:

- System Security Plan (SSP) – Initial draft version due within 30 days of the EPLC Performance Baseline Review. Final draft due 120 days prior to the Operational Readiness Review. Final version due 30 days prior to the Operational Readiness Review.

The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS and HRSA policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter.

- Security Assessment Plan/Report (SAP/SAR) – due 30 days prior to the Operational Readiness Review. The security assessment shall be conducted by HRSA's Security Assessment Team and be consistent with NIST SP 800-53A, NIST SP 800-30, latest revisions, and HHS and HRSA policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with HRSA shall assist in the assessment of the security controls annually and update the SAR at least annually.

- 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.
- E-Authentication Questionnaire – The Contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, Electronic Authentication Guidelines.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

2) 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 FISMA and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and HHS IS2P. 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 specified due date [OpDiv provided].
- Asset Management - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-

owned information/data. The inventory information is required to be produced within 30 days of the EPLC Performance Baseline Review. Final version due within 30 days prior to the Operational Readiness Review and reviewed and updated on a monthly basis thereafter. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

- Configuration Management - Use available SCAP-compliant automated tools, per NIST IR 7511, 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 standard HHS and government configuration baselines prior to the EPLC Operational Readiness Review. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- Vulnerability Management - Use SCAP-compliant 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 HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. If externally-hosted and HRSA is unable to directly scan the system/application, the contractor (and/or any subcontractor) shall provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency prior to the EPLC ORR and at least monthly thereafter and upon request.
- 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; and
 - 180 days for Low risk vulnerabilities.
- Secure Coding - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will

limit system software vulnerability exploits.

- Boundary Protection - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
- c. 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:

- 1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to 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.

- 2) 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, but is not limited to, 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. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
- 3) Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of

information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

- 4) Cooperate with inspections, audits, investigations, and reviews.
- d. 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.
 - e. 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:
 - 1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-2 encryption standards.
 - 2) Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and HHS Minimum Security Configuration Standards;
 - 3) Maintain the latest operating system patch release and anti-virus software definitions;
 - 4) Validate the configuration setting 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
 - 5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
 - f. Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
20. HHS FedRAMP Privacy and Security Requirements.

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

- a. FedRAMP Compliant ATO. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.
 - 1) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The HHS Information Security and Privacy Policy (IS2P) and HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.
 - 2) A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
- b. 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.
- c. 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.

21. Protection of Information in a Cloud Environment.

- a. 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.
- b. 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.
- c. 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.

- d. The Contractor shall support a system of records in accordance with NARA- approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
 - 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.
- e. 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.
- f. 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.

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

- a. The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/HRSA security policies.
 - 1) In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the HRSA authorizing official (AO) prior to implementation of system and/or service being acquired.
 - 2) CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
 - 3) For all acquired cloud services, the SA&A package must contain the following documentation:
 - a) Privacy Impact Assessment (PIA)
 - b) FedRAMP Test Procedures and Results
 - c) Security Assessment Plan (SAP)

- d) Security Assessment Report (SAR)
- e) System Security Plan (SSP)
- f) IT System Contingency Plan (CP)
- g) IT System CP Test Results
- h) Plan of Action and Milestones (POA&M)
- i) Continuous Monitoring Plan (CMP)
- j) FedRAMP Control Tailoring Workbook
- k) Control Implementation Summary Table
- l) Results of Penetration Testing
- m) Software Code Review
- n) E-Authentication Questionnaire
- o) System of Record Notice (SORN)
- p) Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/HRSA policies.

- b. 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.
- c. 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.
- d. 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. HRSA will determine the risk rating of vulnerabilities using FedRAMP baselines.
- e. 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.

23. Reporting and Continuous Monitoring.

- a. 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. [OpDiv include meetings/deliverables timelines as applicable/necessary]
- b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis:
 - 1) Operating system, database, Web application, and network vulnerability scan results;
 - 2) Updated POA&Ms;
 - 3) Any update authorization package documentation as required by the annual attestation/assessment/review or as requested by the HRSA System Owner or AO; and
 - 4) 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.

24. Configuration Baseline.

- a. The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/HRSA configuration baseline.
- b. The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

25. Media Transport

- a. 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).
- b. 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.

26. Boundary Protection: Trusted Internet Connections (ITS)

- a. 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.
- b. The contractor shall route all external connections through a TIC.
- c. Non-Repudiation. The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

27. 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.

28. 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.

Optional Tasks – Not funded unless exercised.

Optional Task 1 – 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). The plan must support phases to allow collaboration with the outgoing contractor. The contractor must also submit a stakeholder management plan outlining, in detail, what steps will be taken to ensure a smooth transition for current employees. The contractor(s) must also work with any future contractor(s) and HHS/HRSA to facilitate complete operational transition, and this must be addressed in the transition plan. This transition plan is predicated on the incoming contractor being available on day one to shadow Contractor staff, be available for all knowledge transfer meetings, and ensure that their staffing is complete at the end of the transition period. The Contractor is not responsible for the incoming contractor's performance during transition.

- a. The plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including, devices, equipment, databases and systems. 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 Contractor proprietary or competitively sensitive information regarding its information, data, systems and processes used to execute this contract.

VI. Deliverables

The contractor shall ensure all products and services delivered under this contract are compliant with HHS Section 508 requirements 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 Standard 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 HHS 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 identified in the HHS Section 508 checklists;

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
1	Secure File Transfer Mechanism.		EDOC	Electronic Format	Email to COR.
2	Program/ Project Plan.		EDOC	Electronic Format	Email to COR.
3	Program Status Report. (Daily Contractor HHS CARES Act Update)		Daily (M-F)	Electronic Format	Email to COR. And to HHS/HRSA defined distribution list

4	Accounting Extract File Format.		Two Weeks After EDOC	Electronic Format	Email to COR.
5	Payment File Integrity Validation.		Each Payment File – notification to HRSA upon failure only.	Electronic Format	Email to COR and Alex Huttinger/HRSA
6	Funding Request.		Prior To An Approved Payment Disbursement Or Upon Check Clearance	Electronic Format	Email to COR. And HHS/HRSA defined distribution list
7	Payment Data File. (ACH Payment File and Check File)		Daily	Electronic Format	Secure file transfer mechanism
8	Provider Payment Email Notification Template.		Prior To Each Payment Wave	Electronic Format	Email to HHS/HRSA Comms Team
9	Customer Service Help Desk Report. (Refer to PWS Attachment B PWS Assumptions)	Not Applicable	N/A	N/A	N/A
10	Customer Service Open HHS/HRSA Queue. (Case Management/Escalation Report)		As New Items Are Added	Electronic Format	Email to HHS/HRSA Case Mgmt team
11	Quality Assurance Surveillance Plan.		A Draft Is Due 30 days After Award of definitized contract QASP Metrics Should Be Delivered To HRSA monthly after award of definitized contract (by 10 th of month)	Electronic Format	Email to COR.
12	ACH Payment Accounting Detail.		Ad Hoc	Electronic Format	Secure File Transfer Mechanism
13	Provider Attestation Report.		Bi-Weekly	Electronic Format	Secure File Transfer Mechanism
14	Aggregated Attestation Summary. (Refer to PWS Attachment B PWS Assumptions)	Not Applicable	N/A	N/A	N/A
15	Attestation/ Demographic Detail.		Bi-Weekly	Electronic Format	Secure File Transfer Mechanism
16	Unique Specialties. (Refer to PWS Attachment B PWS Assumptions)	Not Applicable	N/A	N/A	N/A

17	Ad Hoc Reports To Support Program Operations.		Within three days unless otherwise stated.	Electronic Format	Email to COR.
18	OIG Request Log.		EDOC	Electronic Format	Email to COR.
19	Payment File Record Change Log. (Refer to PWS Attachment BPWS Assumptions)	Not Applicable	N/A	N/A	N/A
20	Provider Detail Report. (Refer to PWS Attachment BPWS Assumptions)	Not Applicable	N/A	N/A	N/A
21	System Demo Or Screenshots Of Each Provider Facing System.		Before And After Each Change as requested	Electronic Format	Email to COR and HHS/HRSA Portal team
22	FAQs And Or Scripts Developed By The Contractor Call Center. (Refer to PWS Attachment BPWS Assumptions)	Not Applicable	N/A	N/A	N/A
23	Contractor Procedures And Processes In Support Of The Program.		As They Are Developed Or Updated	Electronic Format	Email to COR
24	Records Management Schedule And Disposition Plan.	1	Within Thirty Days After Award	Electronic Format	Email to COR.
25	Records Management Training.	As Needed	Prior To Contractor Performance And Annually Thereafter	Electronic Format	Email to COR.
26	Provider Populations Phase/Wave Report		Daily	Electronic Format	Email to COR. and HHS/HRSA defined distribution
27	PRF Records And Artifacts Produced By The Contractor And Contractor Bank. (Refer to PWS Attachment B PWS Assumptions)	Not Applicable	N/A	N/A	N/A

VII. Payment Schedule

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

Item	Description	Quantity	Unit of Issue	Unit Price	Totals
0001	Claims Processing Services for Provider Relief and Protection Fund (PRF)	1	Lot		(b) (4)
1001	Optional Task 1 – Transition Out Plan	1	Lot		(b) (4)
Total Contract Value:					(b) (4)

PWS ATTACHMENT A – QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Task Area	Evaluation Measure	Performance Standard/Acceptable Quality Level (AQL)	Method Used	Frequency
Pymt	Payment Population Grid Reporting measures timely and accurate reporting of wave payments	Timely reporting of wave payments AQL: Submitted timely 99% of time	Inspection	Daily
Pymt	Optum Bank® Payment Processing Quality Program measures the accuracy of HHS payments processed via OptumBank systems	The target/goal performance and success measure is that 95% of payments are processed in an accurate manner	Inspection	Monthly
Pymt	OptumPay ACH Returns Processing Quality Program measures the accuracy of ACH returns processed	The target/goal performance and success measure is that 95% of ACH returns are processed in an accurate manner	Inspection	Daily
Enrlmt	OptumPay Provider ACH Enrollment Processing Quality Program measures the accuracy of provider ACH enrollments processed to effectuate HHS provider payments	The target/goal performance and success measure is that 95% of enrollments processed are processed in an accurate manner	Inspection	Daily
Pymt	Turn-Around Time validation of payment processing measures the processing time of payments from date of receipt from HHS/HRSA to Payment Distribution	The target/goal performance and success measure is that 95% of payment files are processed are processed within the defined 4-day defined turn-around time.	Inspection	With every payment file

PWS ATTACHMENT B – PWS Assumptions

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

1. Task 6. Security Requirements:

In order to meet the highly dynamic, rapidly evolving circumstances, and significant uncertainty, the Contractor relied on its existing systems, security protocols, record keeping systems and training programs to distribute 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 need.

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 this requirement. Contractor will provide its HITRUST certification to HHS under this Contract. Contractor's robust security practices and protocols are further evidenced by the interim ATO issued by HHS.

2. Task 6. Section 5. Protection of Sensitive Information:

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.

3. Task 6. Section 10. Standard for Encryption:

For items a-e, 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.). Contractor assumes that its security and encryption practices, as documented in its HITRUST and Risk Management Framework is sufficient to meet this requirement.

4. Task 6. Section 11. Contractor Non-Disclosure Agreement (NDA):

Contractor assumes the Non-Disclosure Agreement signed between HRSA and UHC April 6, 2020, satisfies this requirement for this contract.

5. Task 6. Section 13. Training:

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.

6. Task 6. Section 14. Rules of Behavior:

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.

7. Task 6. Section 16. Position Sensitivity Designation:

Contractor assumes its standard background check policies and procedures satisfies the requirements for this task. In addition, Contractor believes that none of its employee have direct access to HRSA systems. Accordingly, it is assumed that this task is not applicable to Contractor.

8. Task 6. Section 17. Homeland Security Presidential Directive (HSPD)-12:

Contractor assumes this task was fulfilled by providing HHS/HRSA the contacts and their information at the start of the program. As the program progresses, any resource changes are discussed in joint meetings. Contractor assumes these disclosures met the requirements of this task.

9. Task 6. Section 21. Protection of Information in a Cloud Environment:

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 incident response system and required notices to the HHS CSIRC to support the work required under this Contract meet this requirement.

10. Task 6. Section 27. 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 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 UHG Records Management processes satisfies this task.

11. Task 6. Section 28. Records Management Training:

Regarding Items #24 and #25, the references to “Award” and “Contractor performance” shall mean the execution date of the definitized contract. 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.

12. VI. Deliverables:

Contractor’s pricing is conditioned upon HRSA’s acceptance of the revised deliverables table as well as HRSA’s concurrence that all deliverables submitted through the effective date of definitization of this contract are deemed accepted by HRSA. Note there are a number of deliverables edited and/or deleted from the deliverables table that have never been required nor are they anticipated to be required during the term of the contract.

Regarding Items #24 and #25, the references to “Award” and “Contractor performance” shall mean the execution date of the definitized contract.

A. In reference to Records Management Schedule and Disposition Plan (#24):

Assumption is that current records retention practices and documentation satisfy this requirement. UHG can provide documentation on maintaining Federal Records to include Records Management Schedule and Disposition Plan.

B. The following deliverables are considered not applicable to this program for the following reasons:

- 1) Customer Service Help Desk Report (#9):
 - a. Not applicable to PRF program.
- 2) Aggregated Attestation Summary (#14):
 - a. Included in #3 deliverable titled Daily Contract HHS CARES Act Update.
- 3) Unique Specialties (#16):
 - a. HRSA initially considered the use of specialties in the attestation file however made the decision to not pursue this data file.
- 4) Payment File Record Log Change (#19):
 - a. UHG does not make changes to the payment file; therefore not applicable to

this program.

- 5) Provider Detail Report (#20):
 - a. Included in #15 Attestation/Demographic Detail.
 - 6) FAQs and/or Scripts Developed by the Contractor Call Center (#22):
 - a. HRSA determines all content.
 - 7) PRF Records and Artifacts Produced by the Contractor and Contractor Bank (#27):
 - a. Covered by other deliverables outlined in the PWS.
- C. 508 Compliance. In order to meet the highly dynamic, rapidly evolving circumstances, and significant uncertainty, the Contractor relied on its existing commercial systems to meet HRSA's needs under the program. These commercial systems include pre-existing websites and portals that are not subject to section 508 compliance. Contractor has no obligation to assure that such commercial functionality complies with section 508 requirements.

CPARS Information Sheet

The Contractor Performance Assessment Reporting System (CPARS) is the Department of Defense (DoD) Enterprise Solution for collection of contractor Past Performance Information (PPI) as required by the Federal Acquisition Regulation (FAR). CPARS is a web-enabled application that collects and manages a library of automated contractor report cards. A report card assesses a contractor's performance and provides a record, both positive and negative, on a given contract for a specific period of time. Each report card is based on objective facts and is supported by program and contract management data. Use of CPARS promotes report card consistency, increases data integrity, and motivates improved contractor performance. For more information, see www.cpars.gov.

CPARS Information Sheet

The Contractor Performance Assessment Reporting System (CPARS) is the Department of Defense (DoD) Enterprise Solution for collection of contractor Past Performance Information (PPI) as required by the Federal Acquisition Regulation (FAR). CPARS is a web-enabled application that collects and manages a library of automated contractor report cards. A report card assesses a contractor's performance and provides a record, both positive and negative, on a given contract for a specific period of time. Each report card is based on objective facts and is supported by program and contract management data. Use of CPARS promotes report card consistency, increases data integrity, and motivates improved contractor performance. For more information, see www.cpars.gov.

NON-DISCLOSURE AGREEMENT

WHEREAS, the United States Department of Health and Human Services, Health Services and Resources Administration (HRSA) will enter into a Contract with United Healthcare Services, Inc., on behalf of itself and its affiliates (UHC);

WHEREAS, in advance of the Contract, HRSA will send a data file containing provider information to UHC to facilitate payments to eligible providers from the Public Health and Social Services Emergency Fund under the Coronavirus Aid, Relief, and Economic Security (CARES) Act;

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.

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.

Signed for and on behalf of
HRSA

by /s/

by /s/

Payman Pezhman, Secretary and
Authorised Signatory

Thomas J. Engels
HRSA, Administrator



NOW THAT I HAVE A GOVERNMENT CONTRACT HOW DO I GET PAID?

A. RECEIVING PAYMENT UNDER ATTACHED AWARD

You must be able to accept electronic payments and you must be registered in the System for Award Management (SAM) database (<http://www.sam.gov>). Your DUNS number and banking information must be current. Keep in mind that you must make changes in SAM if your bank merges with another bank or you change banks. You are responsible for updating the data in the SAM database and for re-registering before your expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

B. SUBMITTING REQUEST FOR PAYMENT

1. The contractor **shall** submit payment requests to hirsainvoices@hrsa.gov using **Standard Form 1034, Public Voucher for Purchases and Services Other Than Personal**. Supporting documentation necessary to substantiate your request may be submitted along with the SF 1034. Attached for your convenience is a SF 1034.
2. Submit the SF 1034 and all supporting documentation in PDF format. An electronic copy of the SF1034 in PDF format may be found at www.gsa.gov/portal/forms/download/115462.
3. Only one SF 1034 may be attached to your submission. An e-mail with more than one voucher will be returned to you.
4. Complete the SF 1034 following the directions below:
 - In block entitled, *Voucher No.*, enter the number of the voucher.
 - In block entitled, *U.S. Department, Bureau or Establishment and Location* enter:

HHS/Health Resources and Services Administration
Office of Acquisition Management and Policy
5600 Fishers Lane, Room 14W26
Rockville, MD 20857
 - In the block entitled, *Date Voucher Prepared*, enter the date the voucher is prepared.
 - In the block entitled, *Contract Number and Date*, enter the contract number under which reimbursement is claimed and the date the contract was signed. If billing for work done under a task order or BPA call, enter the contract number or Blanket Purchase Agreement number against which the order or call was issued. If you are simply billing for deliverables under a Purchase Order, leave this block blank and enter the order number in the block entitled, *Number and Date of Order*.
 - In the block entitled, *Requisition Number and Date*, leave blank.

- In the block entitled, *Payee's Name and Address*, enter the name and address as it appears on the contract. In the case of assignment of claims, also supply the *remit to* address of the organization to which payments are assigned. Enter the DUNS number in this block.
- In the block entitled, *Number and Date of Order*, enter the number and date of the Purchase Order, task order or BPA call number.
- In the block entitled, *Date of Delivery or Service*, if billing monthly, enter the specific month/year that the cost were incurred. If billing for a period other than monthly, enter the beginning and ending dates of the cost incurrence period.
- In the block entitled, *Articles or Services*, enter a description of the articles or service provided. If additional space is needed, provide in an attachment. Include the signed statement, "I certify that all payments requested are for appropriate purposes and in accordance with the contract."
- In blocks entitled, *Amount and Total*, enter the total dollar amount claimed for this billing.

VOUCHERS WITHOUT ALL REQUIRED INFORMATION WILL BE DENIED UNTIL THE PROPER INFORMATION IS SUBMITTED.

5. Inquiries:

Regarding payment, contact the Accounts Payable Section:

PSC/FMP/AS
 U.S. Department of Health and Human Services
 Program Support Center
 7700 Wisconsin Ave., Suite 9000
 Bethesda, MD 20814
 Telephone: 301-492-5233 Fax: 301-480-5089
 Email: pscinvoiceinquiries@psc.hhs.gov

Regarding voucher submission, e-mail your concerns to hrsainvoices@hrsa.gov.

Regarding technical issues, inspection and acceptance, call your Contracting Officer Representative (COR).

Regarding suspension or rejection of costs submitted, call your Contract Specialist.

Note: Your respective COR does not have the authority to (1) solicit proposals, (2) modify the stated terms of the award (i.e. change in price, change in scope of work), (3) issue instructions to the contractor to start or stop work, or (4) approve any action that will result in additional charges to the government. These changes are the sole responsibility of the Contracting Officer. The Government will not be responsible for cost overruns or unauthorized procurements made by the vendor.

Standard Form 1034 Revised October 1987 Department of the Treasury 1 TFM 4-2000 1034-122	PUBLIC VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL	VOUCHER NO.				
U.S. DEPARTMENT, BUREAU, OR ESTABLISHMENT AND LOCATION Health Resources & Services Administration 5600 Fishers Lane, 14W26 Rockville, MD 20857	DATE VOUCHER PREPARED	SCHEDULE NO.				
	CONTRACT NUMBER AND DATE	PAID BY				
	REQUISITION NUMBER AND DATE (Optional)					
PAYEE'S NAME AND ADDRESS	Address as it appears on the Contract/Order: Remit to address (where payment is to be sent) : DUNS No. _____		DATE INVOICE RECEIVED			
			DISCOUNT TERMS			
			PAYEE'S ACCOUNT NUMBER			
			GOVERNMENT B/L NUMBER			
SHIPPED FROM	TO	WEIGHT				
NUMBER AND DATE OF ORDER	DATE OF DELIVERY OR SERVICE	ARTICLES OR SERVICES <i>(Enter description, item number of contract or Federal supply schedule, and other information deemed necessary)</i>	QUANTITY	UNIT PRICE		AMOUNT (¹)
				COST	PER	
Date: (mm/dd/yyyy)	From: (mm/dd/yyyy)	I certify that all payments requested are for appropriate purposes and in accordance with the contract". X _____ (Name of Official) (Title) (Date)				
Order No.: HSH _____	To: (mm/dd/yyyy)					
(Use continuation sheets if necessary) (Payee must NOT use the space below) TOTAL						
PAYMENT: <input type="checkbox"/> PROVISIONAL <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL <input type="checkbox"/> PROGRESS <input type="checkbox"/> ADVANCE	APPROVED FOR	EXCHANGE RATE	DIFFERENCES			
	= \$	= \$1.00				
	BY ²			Amount verified; correct for		
	TITLE	(Signature or initials)				
Pursuant to authority vested in me, I certify that this voucher is correct and proper for payment.						
_____		_____		_____		
(Date)		(Authorized Certifying Officer) ²		(Title)		
ACCOUNTING CLASSIFICATION						
CHECK NUMBER	ON ACCOUNT OF U.S. TREASURY		CHECK NUMBER	ON (Name of bank)		
CASH	DATE	PAYEE ³				
\$						
¹ When stated in foreign currency, insert name of currency. ² If the ability to certify and authority to approve are combined in one person, one signature only is necessary; otherwise the approving officer will sign in the space provided, over his official title. ³ When a voucher is receipted in the name of a company or corporation, the name of the person writing the company or corporate name, as well as the capacity in which he signs, must appear. For example: "John Doe Company, per John Smith, Secretary" or "Treasurer", as the case may be.					PER	
					TITLE	

Previous edition usable

NSN 7650-00-634-4206

PRIVACY ACT STATEMENT

The information requested on this form is required under the provisions of 31 U.S.C. 82b and 82c, for the purpose of disbursing Federal money. The information requested is to identify the particular creditor and the amounts to be paid. Failure to furnish this information will hinder discharge of the payment obligation.



NOW THAT I HAVE A GOVERNMENT CONTRACT HOW DO I GET PAID?

A. RECEIVING PAYMENT UNDER ATTACHED AWARD

You must be able to accept electronic payments and you must be registered in the System for Award Management (SAM) database (<http://www.sam.gov>). Your DUNS number and banking information must be current. Keep in mind that you must make changes in SAM if your bank merges with another bank or you change banks. You are responsible for updating the data in the SAM database and for re-registering before your expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

B. SUBMITTING REQUEST FOR PAYMENT

1. The contractor **shall** submit payment requests to hर्सainvoices@hrsа.gov using **Standard Form 1034, Public Voucher for Purchases and Services Other Than Personal**. Supporting documentation necessary to substantiate your request may be submitted along with the SF 1034. Attached for your convenience is a SF 1034.
2. Submit the SF 1034 and all supporting documentation in PDF format. An electronic copy of the SF1034 in PDF format may be found at www.gsa.gov/portal/forms/download/115462.
3. Only one SF 1034 may be attached to your submission. An e-mail with more than one voucher will be returned to you.
4. Complete the SF 1034 following the directions below:

- In block entitled, *Voucher No.*, enter the number of the voucher.
- In block entitled, *U.S. Department, Bureau or Establishment and Location* enter:

HHS/Health Resources and Services Administration
Office of Acquisition Management and Policy
5600 Fishers Lane, Room 14W26
Rockville, MD 20857

- In the block entitled, *Date Voucher Prepared*, enter the date the voucher is prepared.
- In the block entitled, *Contract Number and Date*, enter the contract number under which reimbursement is claimed and the date the contract was signed. If billing for work done under a task order or BPA call, enter the contract number or Blanket Purchase Agreement number against which the order or call was issued. If you are simply billing for deliverables under a Purchase Order, leave this block blank and enter the order number in the block entitled, *Number and Date of Order*.
- In the block entitled, *Requisition Number and Date*, leave blank.

- In the block entitled, *Payee's Name and Address*, enter the name and address as it appears on the contract. In the case of assignment of claims, also supply the *remit to* address of the organization to which payments are assigned. Enter the DUNS number in this block.
- In the block entitled, *Number and Date of Order*, enter the number and date of the Purchase Order, task order or BPA call number.
- In the block entitled, *Date of Delivery or Service*, if billing monthly, enter the specific month/year that the cost were incurred. If billing for a period other than monthly, enter the beginning and ending dates of the cost incurrence period.
- In the block entitled, *Articles or Services*, enter a description of the articles or service provided. If additional space is needed, provide in an attachment. Include the signed statement, "I certify that all payments requested are for appropriate purposes and in accordance with the contract."
- In blocks entitled, *Amount and Total*, enter the total dollar amount claimed for this billing.

VOUCHERS WITHOUT ALL REQUIRED INFORMATION WILL BE DENIED UNTIL THE PROPER INFORMATION IS SUBMITTED.

5. Inquiries:

Regarding payment, contact the Accounts Payable Section:

PSC/FMP/AS
 U.S. Department of Health and Human Services
 Program Support Center
 7700 Wisconsin Ave., Suite 9000
 Bethesda, MD 20814
 Telephone: 301-492-5233 Fax: 301-480-5089
 Email: pscinvoiceinquiries@psc.hhs.gov

Regarding voucher submission, e-mail your concerns to hrsainvoices@hrsa.gov.

Regarding technical issues, inspection and acceptance, call your Contracting Officer Representative (COR).

Regarding suspension or rejection of costs submitted, call your Contract Specialist.

Note: Your respective COR does not have the authority to (1) solicit proposals, (2) modify the stated terms of the award (i.e. change in price, change in scope of work), (3) issue instructions to the contractor to start or stop work, or (4) approve any action that will result in additional charges to the government. These changes are the sole responsibility of the Contracting Officer. The Government will not be responsible for cost overruns or unauthorized procurements made by the vendor.

Standard Form 1034 Revised October 1987 Department of the Treasury 1 TFM 4-2000 1034-122		PUBLIC VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL				VOUCHER NO.			
U.S. DEPARTMENT, BUREAU, OR ESTABLISHMENT AND LOCATION Health Resources & Services Administration 5600 Fishers Lane, 14W26 Rockville, MD 20857			DATE VOUCHER PREPARED		SCHEDULE NO.				
			CONTRACT NUMBER AND DATE		PAID BY				
			REQUISITION NUMBER AND DATE (Optional)						
PAYEE'S NAME AND ADDRESS		Address as it appears on the Contract/Order: Remit to address (where payment is to be sent) : DUNS No. _____				DATE INVOICE RECEIVED			
		DISCOUNT TERMS		PAYEE'S ACCOUNT NUMBER					
		SHIPPED FROM		TO		WEIGHT		GOVERNMENT B/L NUMBER	
		NUMBER AND DATE OF ORDER		DATE OF DELIVERY OR SERVICE		ARTICLES OR SERVICES <i>(Enter description, item number of contract or Federal supply schedule, and other information deemed necessary)</i>		QUAN-TITY	UNIT PRICE COST PER
Date: (mm/dd/yyyy) Order No.: HSH _____		From: (mm/dd/yyyy) To: (mm/dd/yyyy)		I certify that all payments requested are for appropriate purposes and in accordance with the contract". X _____ (Name of Official) (Title) (Date)					
(Use continuation sheets if necessary)			(Payee must NOT use the space below)			TOTAL			
PAYMENT: <input type="checkbox"/> PROVISIONAL <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL <input type="checkbox"/> PROGRESS <input type="checkbox"/> ADVANCE		APPROVED FOR =\$ _____		EXCHANGE RATE =\$1.00		DIFFERENCES _____			
		BY ² _____				Amount verified; correct for			
		TITLE _____				(Signature or initials)			
Pursuant to authority vested in me, I certify that this voucher is correct and proper for payment.									
_____ (Date)			_____ (Authorized Certifying Officer) ²				_____ (Title)		
ACCOUNTING CLASSIFICATION									
	CHECK NUMBER		ON ACCOUNT OF U.S. TREASURY			CHECK NUMBER		ON (Name of bank)	
	CASH \$		DATE			PAYEE ³			
¹ When stated in foreign currency, insert name of currency. ² If the ability to certify and authority to approve are combined in one person, one signature only is necessary; otherwise the approving officer will sign in the space provided, over his official title. ³ When a voucher is receipted in the name of a company or corporation, the name of the person writing the company or corporate name, as well as the capacity in which he signs, must appear. For example: "John Doe Company, per John Smith, Secretary" or "Treasurer", as the case may be.							PER		
							TITLE		

Previous edition usable

NSN 7650-00-634-4206

PRIVACY ACT STATEMENT

The information requested on this form is required under the provisions of 31 U.S.C. 82b and 82c, for the purpose of disbursing Federal money. The information requested is to identify the particular creditor and the amounts to be paid. Failure to furnish this information will hinder discharge of the payment obligation.

Contractor Non-Disclosure Agreement (NDA)

This NDA is to be completed by a contractor upon award of contract.

The following statement is to be completed by all contractor employees who may be involved in the performance of contract work.

Access to privileged information obtain under the performance under contract 75R60221C00003 between the Department of Health and Human Services (HHS) and my employer United HealthCare Services, Inc., will not be disclosed or used for any benefit of myself or my employer.

I, _____, ON THIS ____ DAY _____ OF _____, hereby agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with the provision of *18 U.S.C. 641, 18 U.S.C. 1905, 18 U.S.C. 2071, Public Law 96-511*, and other pertinent laws and regulations governing the confidentiality of privileged information.

I understand the provision of *18 U.S. C. 641, 18 U. S. C. 1905, 18 U. S. C. 2071 and Public law 96-511*, and that I am subject to criminal penalties prescribed by law for any violations thereof.

Signed: _____

Date: _____

Witnessed by: _____

Date: _____

Cc:
Contracting Officer Representative (COR)
Contract Specialist (CS)

**TRI-PARTITE BANK AGREEMENT FOR PAYMENT PROCESSING SERVICES FOR
COVID-19 PROVIDER RELIEF AND PROTECTION FUND**

This TRI-PARTITE BANK AGREEMENT FOR PAYMENT PROCESSING SERVICES FOR COVID-19 Provider Relief and Protection Fund (this “Tri-Partite Agreement”) is effective starting on 7 April 2020, or whatever date the Contractor (as hereinafter defined) actually begins to use the banking contractor discussed herein, and is between the Health Resources and Services Administration (HRSA), represented by the HRSA Administrator or his/her designee executing this Tri-Partite Agreement; United HealthCare Services, Inc. (hereinafter called the Contractor); and Optum Bank, Inc. (hereinafter called the Bank).

RECITALS

- (1) HRSA and the Contractor are parties to 75R60220C00006, referred to herein as the “Agreement,” providing for the disbursement of funds (the “Funds”) for payments to providers under the program established by the Health Resources and Services Administration (HRSA), Payment Processing Services for COVID-19 Provider Relief and Protection Fund.
- (2) The Agreement requires that the Funds be used solely for making payments to medical service providers who are participating in the HRSA Payment Processing program and approved to receive these funds. The Funds will be deposited in a HRSA Providers Relief and Protection Fund Account (further described below) at a member bank or banks of the Federal Reserve System or any “insured” bank within the meaning of the Act creating the Federal Deposit Insurance Corporation (“FDIC”) (Act of August 23, 1935; 49 Stat. 684, as amended; 12 U.S.C. § 264), separate from the Contractor's general or other funds; and, the Bank being such a bank, the parties are agreeable to so depositing said amounts with the Bank.
- (3) The HRSA Provider Relief and Protection Fund Account (the “HRSAPRPF”), which account includes one or more of a controlled disbursement account, a deposit account, and/or a funding account shall be in the Bank's name.

COVENANTS

In consideration of the foregoing, and for other good and valuable consideration, it is agreed that:

- (1) The Bank shall have a lien upon the credit balances in the HRSAPRPF to secure the repayment of any and all amounts due the Bank hereunder, which lien shall be superior to any lien or claim of HRSA or the Contractor.
- (2) The Bank shall not be responsible for (a) the application of Funds withdrawn from the HRSAPRPF, or (b) determining whether any person or entity is entitled to receive Funds ordered or directed to be paid by the Contractor. Provided that the Bank exercises ordinary care, after receipt by the Bank of written directions from the duly authorized representative of HRSA or the Contractor, the Bank shall act thereon and shall be under no liability to any party hereto or any

third party for any action taken or not taken in accordance with such written directions, including without limitation any directions in the form of electronic transmission, file, mail or other electronic instruction or transaction, including automated clearing house entry, or for the breach of any warranty or representation by HRSA or the Contractor, as the case may be. Any such written directions or instructions received by the Bank from or at the direction of the Administrator, HRSA, or from the duly authorized representative of same may, in so far as the rights, duties and liabilities of the Bank are concerned, be considered as having been properly issued and filed with the Bank by HRSA.

(3) HRSA or its authorized representatives may request copies of the establishment and maintenance of, and transactions in the HRSAPRPF at HRSA's expense. Such copies shall be available within a reasonable time. Such records shall be preserved by the Bank for a period of six (6) years following the close of the calendar year in which the records were created unless prior to that time, the Bank has been notified in writing by HRSA that preservation of such records for a longer period of time is necessary for purposes of litigation or dispute.

(4) In the event of the service of any writ of attachment, levy of execution, or commencement of garnishment proceedings with respect to the HRSAPRPF, the Bank will promptly notify HRSA and the Contractor.

(5) The Bank's release of electronic Automated Clearing House Payments ("ACH") to medical service providers is dependent upon full HRSA funding. Advance notice of daily funding requirements will be provided by the Bank to HRSA. HRSA will fund the HRSAPRPF through the United States Treasury by means of an electronic funds transfer, including ACH or wire transfer in an amount sufficient to cover the amount of: (a) items issued by or in the name of the Bank, (individually, "Item" and collectively, the "Items"); and (b) any withdrawals or debits to the FQHCA in accordance with ordinary procedures for processing any Items, including, without limitation, any adjustments and charge backs in connection with any Items (the "Adjustments"). In conjunction with any transfers of funds, the parties agree to be bound by the then current Operating Rules and Guidelines of the National Automated Clearinghouse Association (the "NACHA Rules"), except that with respect to the Government, as such NACHA Rules are modified by Department of the Treasury Regulations. Notwithstanding anything to the contrary herein, the Bank shall be under no obligation to follow the instructions or directions of HRSA or the Contractor to reverse any entries or Items unless such reversal is in accordance with the NACHA Rules or Department of Treasury Regulations. The Bank agrees to service the HRSAPRPF in the manner set forth herein and based on the specifications and other information contained in Addenda A and B, incorporated herein.

In the event Items or other withdrawals presented or projected to be presented against the HRSAPRPF exceed the available Funds in the account, the Bank will use commercially reasonable efforts to notify HRSA before 12:00 p.m. Eastern Time, and HRSA shall, increase the Funds in the HRSAPRPF as necessary, to cover the excess amount. In the event that HRSA fails to timely respond, the Bank will hold such Items exceeding the amount of the available funds until good Funds become available to the Bank by HRSA.

Each party to this Tri-Partite Agreement agrees to notify all other parties to this Tri-Partite Agreement within 15 days after learning of the occurrence of any actions or omissions of which the first party becomes aware that may be in violation of the Tri-Partite Agreement or which may be otherwise fraudulent or unauthorized.

The Bank, the Contractor and HRSA agree that no person other than the parties to the Agreement are intended to be the beneficiaries of this Tri-Partite Agreement or the Agreement nor shall any other person have rights arising under same.

(6) This Tri-Partite Agreement, with all its provisions and covenants, shall commence on 7 April 2020 and end on 6 April 2021.

(7) Notwithstanding Covenant 6, in the event the Agreement referenced in Recital (1) is not renewed or is terminated, this Tri-Partite Agreement among HRSA, the Contractor, and the Bank will automatically be terminated upon the delivery of written notice to the other parties. This Tri-Partite Agreement will terminate automatically at the conclusion of the term listed in (6), above.

(8) The Bank agrees that it shall not enter into any agreement with any other party to carry out the primary responsibilities of this Tri-Partite Agreement without the prior written approval of HRSA.

(9) Pricing and payment terms for the banking services provided hereunder are set forth in that certain Contract 75R60220C00006 with an effective date of April 7, 2020 by and between the Contractor and HRSA (as the same may be amended from time to time), the terms of which are incorporated herein by reference.

(10) .

The Bank, the Contractor, and HRSA agree to comply with the provisions set forth in Addenda A and B, which are attached hereto and incorporated herein.

(11) Each party to this Tri-Partite Agreement represents and warrants to the other parties that it: (i) has the power and legal right and authority to enter into, deliver and perform this Tri-Partite Agreement, and that neither this Tri-Partite Agreement, nor the agreements contained in this Tri-Partite Agreement, contravenes any provision of or constitutes a default under any agreement, instrument or indenture to which such party is a party or signatory or any provision of such party's constituent documents or any other agreement or requirement of law; (ii) this Tri-Partite Agreement has been duly executed and delivered by such party and constitutes the legal, valid and binding obligation of such party, enforceable against it in accordance with its terms, except as such enforceability may be limited by applicable bankruptcy, insolvency, reorganization, moratorium or similar laws affecting creditors' rights generally and by general principles of equity; and (iii) no consent, approval or authorization of or registration or declaration with any party, including but not limited to any governmental authority, is required (except for those which such party has obtained or provided) in connection with the execution

and delivery by such party of this Tri-Partite Agreement, or the performance of the obligations of such party described in this Tri-Partite Agreement.

[SIGNATURES ON NEXT PAGE]

IN WITNESS WHEREOF, the parties hereto have caused this Tri-Partite Agreement, including the signature pages, to be executed as of the day and year first above written.

THE UNITED STATES OF AMERICA
Department of Health and Human Services
Health Resources and Services Administration

CONTRACTOR
United Healthcare Services, Inc.

/s/

/s/

By: Thomas J. Engels

By: Brian R. Thompson

Its: Administrator

Its: CEO, UHC Government Programs

Date: April 7, 2020

Date: April 7, 2020

BANK
Optum Bank, Inc.

/s/

By: Jonathan Willey

Its: CFO, Optum Bank

Date: April 7, 2020

ADDENDUM A

CONTRACTOR'S BANKING SERVICES

The list of approved banking services is provided below and will be subject to change based on definitization of Contract 75R60220C00006 between Contractor and HRSA. Any additional services requested must be approved by HRSA.

MEASURED ACCOUNT SERVICES		
1	PAYMENT	
	a)	EFTs
	b)	Checks
2		
	MAJOR COST ITEMS	
	a)	(b) (4)
	b)	(b) (4)
	c)	(b) (4)
3		
	ALL OTHER ITEMS	
	a)	Account Maintenance
	b)	Reconciliations
	c)	HRSA Mandated Reconciliations and Reports (per funding account)
	d)	CD ROM Disks
	e)	Controlled Distribution Maintenance (Controlled Disbursement & ARP)
	f)	Wire Transfers
	g)	Mail Credit Advice/Express Courier Deposit
	h)	Online Payable Services - paid check retention
	i)	Online Stop Payments
	j)	Online Information Reporting - subscription fee (per user, per module)
	k)	Online Payable Services -Maintenance
	l)	Data Transmission - ACH (per transmission)
	m)	Data Transmission - Issue File
	n)	Data Transmission/Pay File (per transmission)
	o)	Deposit Ticket/Credits Posted
	p)	EFT Monthly Maintenance
	q)	EFT Return Notification Fax
	r)	ACH Debit Block Maintenance
	s)	ACH returns/NOCs
	t)	ACH reversals

u)	ACH return via transmission (per item)
v)	Positive Pay Maintenance
w)	Positive Pay Exception (per item)
x)	Positive Pay Exception Return (per return)
y)	Same Day Positive Pay
z)	Onsite Electronic Deposit - Deposited Items
aa)	Onsite Electronic Deposit- Credit
bb)	Onsite Electronic Deposit - Check Scanner
cc)	Onsite Electronic Deposit - Email Notification of Returns
dd)	Web Service -Ext paid check Retention 84 months (per item)
ee)	Image Deposited Checks maintenance (monthly)
ff)	Image Deposited Checks - per item
gg)	Image Deposit - Credit posted
hh)	Image Deposit - Return Deposited Item (per item)
ii)	Image Deposited Checks Maintenance (Monthly)
jj)	Image Deposit - Credit posted (per credit)
kk)	Lockbox- Item Processing
ll)	Lockbox- Photocopy- (per Item)
mm)	Lockbox- Checks Deposited
nn)	Lockbox- Account Changes
oo)	Lockbox - Image File Transmission (per item)
pp)	Lockbox- Data Entry
qq)	Lockbox- Document Sorting/matching
rr)	Lockbox- Returned deposits/envelopes
ss)	Lockbox- Credit Ticket
tt)	Lockbox- Monthly Maintenance
vv)	Lockbox - Deposit Item Image CD (per item)
ww)	Payee Positive Pay
4	New Accounts Setup/Service Changes/All Testing Support
a)	(b) (4)
b)	
c)	

ADDENDUM B

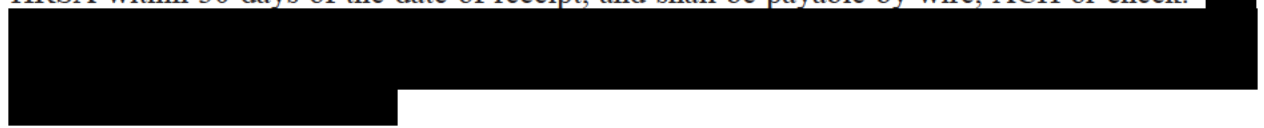
(All capitalized terms used herein and not otherwise defined shall have the meaning as set forth in this Tri-Partite Agreement.)

ADDITIONAL PROCEDURES APPLICABLE TO HRSAPRPF FUNDING

1. The Bank will confirm the availability of funds in the HRSAPRPF prior to accessing the Bank's system to release HRSAPRPF electronic payments to medical service providers.

2. RESERVED

3. The Bank will provide its charge for each of the requested services, including any FDIC fee or charge required to be paid by the Bank from time to time as such fee or charge may change, as reflected in the Specifications to Provide Required Banking Services (Addendum A) and will receive monthly reimbursement for servicing the HRSAPRPF. All such fees and charges shall be sent monthly to the HRSA Chief Financial Officer are due and payable by HRSA within 30 days of the date of receipt, and shall be payable by wire, ACH or check. ^{(b) (4)}



4. The Bank will be required to prepare a monthly reconciliation of the HRSAPRPF. The Contractor will furnish the Bank with a record of checks/EFTs issued (numerically identified) to be matched against those checks/EFTs which have cleared through the HRSAPRPF. The results of the Bank reconciliation will be given to the Contractor.

5. The Bank will be required to submit to the Contractor each month:

(a) A bank statement reflecting the daily total checks/EFTs debited, daily total deposits credited, any Adjustments, and daily HRSAPRPF balance. All deposits will be shown separately on the statement.

(b) An analysis of the HRSAPRPF, reflecting the Contractor's actual account activity for the month.

6. TERMINATION PROCEDURES

In the event of termination, the Bank agrees to retain the HRSAPRPF for an additional 30-day period beyond the termination, to allow for clearance of return and re-routing of potentially mis-directed ACH payments. During this period, the Contractor and HRSA agree to strictly comply with the Covenant 5 of this Tri-Partite Agreement. Moreover, all terms and

conditions of this Tri-Partite Agreement, other than Covenant 6 and Covenant 7 which may be modified by such additional term, will remain in effect.

During the entire period, it is further understood that all Bank FDIC fees or charges will be consistent with and paid in accordance with this Tri-Partite Agreement.

7. LIMITATION OF LIABILITY

Provided that the Bank acts in good faith and with ordinary care, the Bank's liability under this Tri-Partite Agreement shall be limited to actual direct costs incurred by the Contractor and/or HRSA due to the Bank's gross negligence, or refusal to materially comply with this Tri-Partite Agreement as are required to be performed or completed by the Bank.



NOW THAT I HAVE A GOVERNMENT CONTRACT HOW DO I GET PAID?

A. RECEIVING PAYMENT UNDER ATTACHED AWARD

You must be able to accept electronic payments and you must be registered in the System for Award Management (SAM) database (<http://www.sam.gov>). Your DUNS number and banking information must be current. Keep in mind that you must make changes in SAM if your bank merges with another bank or you change banks. You are responsible for updating the data in the SAM database and for re-registering before your expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

B. SUBMITTING REQUEST FOR PAYMENT

1. The contractor **shall** submit payment requests to hrsainvoices@hrsa.gov using Standard Form 1034, Public Voucher for Purchases and Services Other Than Personal. Supporting documentation necessary to substantiate your request may be submitted along with the SF 1034. Attached for your convenience is a SF 1034.
2. Submit the SF 1034 and all supporting documentation in PDF format. An electronic copy of the SF1034 in PDF format may be found at www.gsa.gov/portal/forms/download/115462.
3. Only one SF 1034 may be attached to your submission. An e-mail with more than one voucher will be returned to you.
4. Complete the SF 1034 following the directions below:

- In block entitled, *Voucher No.*, enter the number of the voucher.
- In block entitled, *U.S. Department, Bureau or Establishment and Location* enter:

HHS/Health Resources and Services Administration
Office of Acquisition Management and Policy
5600 Fishers Lane, Room 14W26
Rockville, MD 20857

- In the block entitled, *Date Voucher Prepared*, enter the date the voucher is prepared.
- In the block entitled, *Contract Number and Date*, enter the contract number under which reimbursement is claimed and the date the contract was signed. If billing for work done under a task order or BPA call, enter the contract number or Blanket Purchase Agreement number against which the order or call was issued. If you are simply billing for deliverables under a Purchase Order, leave this block blank and enter the order number in the block entitled, *Number and Date of Order*.

- In the block entitled, *Requisition Number and Date*, leave blank.
- In the block entitled, *Payee's Name and Address*, enter the name and address as it appears on the contract. In the case of assignment of claims, also supply the *remit to* address of the organization to which payments are assigned. Enter the DUNS number in this block.
- In the block entitled, *Number and Date of Order*, enter the number and date of the Purchase Order, task order or BPA call number.
- In the block entitled, *Date of Delivery or Service*, if billing monthly, enter the specific month/year that the cost were incurred. If billing for a period other than monthly, enter the beginning and ending dates of the cost incurrence period.
- In the block entitled, *Articles or Services*, enter a description of the articles or service provided. If additional space is needed, provide in an attachment. Include the signed statement, "I certify that all payments requested are for appropriate purposes and in accordance with the contract."
- In blocks entitled, *Amount and Total*, enter the total dollar amount claimed for this billing.

VOUCHERS WITHOUT ALL REQUIRED INFORMATION WILL BE DENIED UNTIL THE PROPER INFORMATION IS SUBMITTED.

5. Inquiries:

Regarding payment, contact the Accounts Payable Section:

PSC/FMP/AS
 U.S. Department of Health and Human Services
 Program Support Center
 7700 Wisconsin Ave., Suite 9000
 Bethesda, MD 20814
 Telephone: 301-492-5233 Fax: 301-480-5089
 Email: pscinvoiceinquiries@psc.hhs.gov

Regarding voucher submission, e-mail your concerns to hrsainvoices@hrsa.gov.

Regarding technical issues, inspection and acceptance, call your Contracting Officer Representative (COR).

Regarding suspension or rejection of costs submitted, call your Contract Specialist.

Note: Your respective COR does not have the authority to (1) solicit proposals, (2) modify the stated terms of the award (i.e. change in price, change in scope of work), (3) issue instructions to the contractor to start or stop work, or (4) approve any action that will result in additional charges to the government. These changes are the sole responsibility of the Contracting Officer. The Government will not be responsible for cost overruns or unauthorized procurements made by the vendor.

Standard Form 1034 Revised October 1987 Department of the Treasury 1 TFM 4-2000 1034-122		PUBLIC VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL				VOUCHER NO.	
U.S. DEPARTMENT, BUREAU, OR ESTABLISHMENT AND LOCATION Health Resources & Services Administration 5600 Fishers Lane, 14W26 Rockville, MD 20857			DATE VOUCHER PREPARED		SCHEDULE NO.		
			CONTRACT NUMBER AND DATE		PAID BY		
			REQUISITION NUMBER AND DATE (Optional)				
PAYEE'S NAME AND ADDRESS		Address as it appears on the Contract/Order:				DATE INVOICE RECEIVED	
		Remit to address (where payment is to be sent) :				DISCOUNT TERMS	
		DUNS No. _____				PAYEE'S ACCOUNT NUMBER	
		SHIPPED FROM		TO		WEIGHT	
NUMBER AND DATE OF ORDER	DATE OF DELIVERY OR SERVICE	ARTICLES OR SERVICES <i>(Enter description, item number of contract or Federal supply schedule, and other information deemed necessary)</i>	QUANTITY	UNIT PRICE		AMOUNT	
				COST	PER	(¹)	
Date: (mm/dd/yyyy) Order No.: HSH _____	From: (mm/dd/yyyy) To: (mm/dd/yyyy)	I certify that all payments requested are for appropriate purposes and in accordance with the contract". X _____ (Name of Official) (Title) (Date)					
(Use continuation sheets if necessary) (Payee must NOT use the space below) TOTAL							
PAYMENT: <input type="checkbox"/> PROVISIONAL <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL <input type="checkbox"/> PROGRESS <input type="checkbox"/> ADVANCE		APPROVED FOR =\$ _____	EXCHANGE RATE =\$1.00	DIFFERENCES _____			
		BY ² _____	Amount verified; correct for				
		TITLE _____	(Signature or initials)				
Pursuant to authority vested in me, I certify that this voucher is correct and proper for payment.							
_____ (Date)		_____ (Authorized Certifying Officer) ²			_____ (Title)		
ACCOUNTING CLASSIFICATION							
CHECK NUMBER		ON ACCOUNT OF U.S. TREASURY		CHECK NUMBER		ON (Name of bank)	
CASH \$ _____		DATE _____		PAYEE ³ _____			
¹ When stated in foreign currency, insert name of currency. ² If the ability to certify and authority to approve are combined in one person, one signature only is necessary; otherwise the approving officer will sign in the space provided, over his official title. ³ When a voucher is receipted in the name of a company or corporation, the name of the person writing the company or corporate name, as well as the capacity in which he signs, must appear. For example: "John Doe Company, per John Smith, Secretary" or "Treasurer", as the case may be.					PER		
					TITLE		

Previous edition usable

NSN 7650-00-634-4206

PRIVACY ACT STATEMENT

The information requested on this form is required under the provisions of 31 U.S.C. 82b and 82c, for the purpose of disbursing Federal money. The information requested is to identify the particular creditor and the amounts to be paid. Failure to furnish this information will hinder discharge of the payment obligation.

SECTION A – STANDARD FORM (SF) 33

This page intentionally left blank.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Purpose of Contract

The purpose of this requirement 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 and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Program (Uninsured Program).

B.2 Consideration and Payment

This is a Firm Fixed Price (FFP) contract. In consideration for satisfactory performance of the services outlined in the Performance Work Statement located at Section J (Attachment A), the following payment schedule will be utilized.

Base Period

The maximum reimbursement that may be dispersed during the Base Period is 42,862,928 for submitted (billed) claims and 29,488.437 for paid claims.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0001	Management and Administration Fees	12	Month	\$(b) (4)	\$(b) (4)
0002	Fee per submitted (billed) claim	42,862,928	Each	\$(b) (4)	(b) (4)
0003	Fee per paid claim	29,488,437	Each	(b) (4)	(b) (4)
Total Value Base Period (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

Option Period One

The maximum reimbursement that may be dispersed during the Option Period One is 7,000,000 for submitted (billed) claims and 3,000,000 for paid claims.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1001	Management and Administration Fees	12	Month	(b) (4)	(b) (4)
1002	Fee per submitted (billed) claim	7,000,000	Each	(b) (4)	(b) (4)
1003	Fee per paid claim	3,000,000	Each	(b) (4)	(b) (4)
Total Value Option Period One (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4)

Option Period Two

The maximum reimbursement that may be dispersed during the Option Period Two is 4,000,000 for submitted (billed) claims and 1,000,000 for paid claims.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2001	Management and Administration Fees	12	Month	(b) (4)	(b) (4)
2002	Fee per submitted (billed) claim	4,000,000	Each	(b) (4)	(b) (4)
2003	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
Total Value Option Period Two (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4)

B.2.1 Allowable Costs

Costs shall be determined by the Contracting Officer to be allowable in accordance with FAR Subpart 31 in effect on the date of this Contract and the terms of this Contract.

B.2.2 Prior Authorization of Certain Direct Costs

1. Requirements for purchase orders and subcontracts are governed by FAR 52.244-2, Subcontracts (JUN 2020) of the General Provisions except as may be indicated herein.
2. The Contractor shall not incur any of the following costs without the prior written approval of the Contracting Officer. Incurrence of such costs with the intent of claiming reimbursement as direct costs under this contract shall be at the Contractor's own risk:
 - a. Purchase of any item of equipment, including furniture or office equipment, regardless of cost;
 - b. Any rental agreement for real or personal property, or any term contract for maintenance;
 - c. Travel for general scientific meetings; and
 - d. Rearrangement, alternation or relocation of facilities.

B.2.3 Requirement to notify Government and Limitation of Government's Obligation

1. By the 15th day of each month, the Contractor shall advise the Government of the number of reimbursement.

If the number of reimbursement is likely to exceed the maximum specified in B.2 for the applicable contract period, the contractor shall notify the Government as soon as practicable. The notification shall advise the Contracting Officer of the estimated increase in number of reimbursement.

2. The Government’s payment obligation under the per claim is limited to payment for the actual number of claims, up to the maximum number of claims specified for the applicable contract period. Under no event shall the Government be obligated to pay for more than the actual number of claims.

B.3 Optional Item and Quantity Pricing

1. During the base period of performance, CLIN 0009 may be exercised once.
2. During the respective period of performance, each of these CLIN 0004, 1004 and 2004 may be exercised once per period.
3. The unit pricing for the Fee per Submitted (billed) Claims, Fee per Paid Claims, OIG Interviews and TIN Investigations CLINs will be determined by the number of reimbursements dispersed during each period of performance, as set forth below.

Base Period

CLIN 0005 may be exercised for up to 9,000,000 units in the Base Period.

CLIN 0006 may be exercised for up to 3,000,000 units in the Base Period.

CLIN 0007 may be exercised for up to 25 units in the Base Period.

CLIN 0008 may be exercised for up to 70 units in the Base Period.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0004	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
0005	Fee per submitted (billed) claim	9,000,000	Each	(b) (4)	(b) (4)
0006	Fee per paid claim	3,000,000	Each	(b) (4)	(b) (4)
0007	OIG Interview	25	Each	(b) (4)	(b) (4)
0008	TIN Investigation	70	Each	(b) (4)	(b) (4)
0009	Optional Task 2 – Fraud Detection	1	Lot	To Be Negotiated Prior To Exercising	To Be Negotiated Prior To Exercising
Total Value Base Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

Option Period One

CLIN 1005 may be exercised for up to 4,000,000 units in Option Period One.
 CLIN 1006 may be exercised for up to 1,000,000 units in Option Period One.
 CLIN 1007 may be exercised for up to 25 units in the Option Period One.
 CLIN 1008 may be exercised for up to 60 units in the Option Period One.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1004	Optional Task 1 – Transition Out Plan	1	Lot	\$(b) (4)	(b) (4)
1005	Fee per submitted (billed) claim	4,000,000	Each	(b) (4)	(b) (4)
1006	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
1007	OIG Interview	25	Each	(b) (4)	(b) (4)
1008	TIN Investigation	60	Each	(b) (4)	(b) (4)
Total Value Option Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

Option Period Two

CLIN 2005 may be exercised for up to 3,000,000 units in Option Period Two.
 CLIN 2006 may be exercised for up to 1,000,000 units in Option Period Two.
 CLIN 2007 may be exercised for up to 25 units in the Option Period Two.
 CLIN 2008 may be exercised for up to 60 units in the Option Period Two.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2004	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
2005	Fee per submitted (billed) claim	3,000,000	Each	(b) (4)	(b) (4)
2006	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
2007	OIG Interview	25	Each	(b) (4)	(b) (4)
2008	TIN Investigation	60	Each	(b) (4)	(b) (4)
Total Value Option Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

B.4 Total Estimated Contract Value is: (b) (4)

SECTION C – DESCRIPTION/SPECIFICATIONS/ STATEMENT OF WORK

C.1 Performance Work Statement

Independently and not as an agent of the Government, the Contractor shall furnish all personnel, material, facilities, services, and equipment as needed to perform the Performance Work Statement located at Section J (Attachment A), attached hereto and made part of this document.

SECTION D – PACKAGING AND MARKING

D.1 Packaging and Marking

All reports and documents shall have, at a minimum, in the document header, the contract number, and the Contracting Officer Representative (COR) name. All reports and documents shall have, at a minimum in the document footer, the author in the lower left corner, the page # of total # of pages in the center bottom of the page, and the date and /or version of the document (not the auto date) in the lower right corner.

The Contractor shall deliver all items at the time indicated in the Deliverables Schedule.

All deliverable reports are to carry at the top of the first page the following information:

Contract number
Deliverable item number
Deliverable item delivery due date
Date of submission

SECTION E – INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

The Contracting Officer's Representative (COR), as a duly authorized representative of the Contracting Officer, shall assume the responsibilities for monitoring the Contractor's performance, evaluating the quality of services provided by the Contractor and performing final inspection and acceptance of all deliverables.

E.2 Inspection

FAR 52.246-4 Inspection of Services – Fixed-Price (Aug 1996)

- (a) Definition. "Services," as used in this clause, includes services performed, workmanship, and material furnished or utilized in the performance of services.
- (b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires.
- (c) The Government has the right to inspect and test all services called for by the contract, to the extent practicable at all times and places during the term of the contract. The Government shall perform inspections and tests in a manner that will not unduly delay the work.
- (d) If the Government performs inspections or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties.
- (e) If any of the services do not conform with contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by reperformance, the Government may –
 - (1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and
 - (2) Reduce the contract price to reflect the reduced value of the services performed.
- (f) If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with contract requirements, the Government may –

(1) By contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Government that is directly related to the performance of such service; or

(2) Terminate the contract for default.

E.3 Quality Assurance Surveillance Plan (QASP)

The Government will monitor the Contractor's performance under this contract in accordance with the QASP. The following is a sample Quality Assurance Surveillance Plan (QASP):

Task Area	Evaluation Measure	Performance Standard/Acceptable Quality Level (AQL)	Method Used	Frequency
All Tasks	Status Reporting	Timely information on project status AQL: Submitted timely 97% of time	Inspection	Monthly
	Fraudulent Report	Report within 1 calendar day of detection	Time (days/hours) of report from detection	When Fraudulent request detected
	Payment Filing and Processing	Payment filing and processing AQL: Within 4 days	Inspection	Monthly
	Successful Payment Rate	Clean-payment rate AQL: 90% payment rate	Inspection	Monthly
	Documentation Deliverable	Secure and confidential patient information AQL: 100% patient information is secured and confidential	Inspection	Monthly
	Defined Processes	Call center and payment return processes AQL: Reduce by 50%	Inspection	Monthly
	Funding Request Accuracy	Status of payments AQL: No more than 1 revision per week	Report	Monthly
	Reconciled Payment	Reconciled successful and returned ACH and check payment AQL:	Report	Monthly
	Call Center Resolution	Call center call issues AQL: Resolves 95% of calls	Report	Weekly
	Call Center Response Rates	Increase adjudication rates AQL: Within 5 minutes	Inspection	Monthly

SECTION F – DELIVERIES OR PERFORMANCE

F.1 Period of Performance

The period of performance will be for one (1) 12 month base period with two (2) 12 month option periods. The option periods under this contract may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). The base period of performance will start on April 17, 2021, through April 16, 2022.

F.2 Place of Performance

Work shall be performed under this contract off-site, primarily at the contractor's facilities, which includes work performed by staff that telecommute.

F.3 Observance of Federal Holidays

New Year's Day	January 1st
Martin Luther King, Jr. Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4th
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	November 11th
Thanksgiving Day	Fourth Thursdays in November
Christmas Day	December 25th
Inauguration Day	Every fourth year after 1965, January 20th, Washington, DC

No on-site services shall be performed, nor shall HRSA reimburse a contractor for work performed on Federal legal holidays, holidays set forth by Presidential Executive Order and any other Government closures, including closures for inclement weather, unless otherwise provided for in the terms of the contract. The contractor may not bill for hours not worked.

F.4 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
1	Records Management Schedule and Disposition Plan	1	Within Thirty (30) Days After Award.	Electronic Format	Email to COR.
2	Records Management Training.	As Needed	Within Thirty (30) days after contract award and Fourteen (14) days after new staff onboarding	Electronic Format	Email to COR.
3	Program and Project Management Plan.	1	Within Thirty (30) Days After Award	Electronic Format	Email to COR

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
9	Biweekly COR Meeting Agendas	26	One (1) Time Every Two (2) Weeks	Electronic Format	Email to COR
10	Project Updates.		As requested	Electronic Format	Email to COR
11	Monthly Status Reports.	12	Monthly	Electronic Format	Email to COR
12	Weekly Reports.	52	Each Wednesday by 6PM EST,	Electronic Format	Email to COR
13	Daily Executive Email.	262	Daily (weekdays)	Electronic Format	Email to COR
14	Daily Financial Report.	262	Daily (weekdays)	Electronic Format	Email to COR and the Chief, Budget Execution and Management Branch
15	Ad hoc Reports.	12	As Requested	Electronic Format	Email to COR
16	Final Report.	1	Thirty (30) Days Prior to the End of the Period of Performance	Electronic Format	Email to COR
17	Risk Management Plan.	1	Within fourteen (14) Days After Award	Electronic Format	Email to COR
18	Website Content.		Within Fifteen (15) days After Award of	Electronic Format	COR

			Contract and as Requested		
19	Consumer Education Materials.	4	As Requested	Electronic Format	COR
20	Social Media Plan.	1	Within Thirty (30) Days After Award of Contract.	Electronic Format	Email to COR
21	Data Reports Within Federal Government.		As Requested	Electronic Format	Email to COR
22	Urgent Data Reports Within Federal Government.		As Requested	Electronic Format	Email to COR
23	Routine Data Reports Outside Federal Government.	60	Up to 5 Each Month	Electronic Format	Email to COR
24	Routine Data Reports Outside Federal Government Tracking Report.	4	Quarterly	Electronic Format	Email to COR
25	Provider Portal Data Reports.	12	Monthly	Electronic Format	Email to COR
26	Encrypted Approved Claims File.	52	Weekly	Electronic Format	Email to Chief Data Officer
27	Claims Verification Process.	1	Within 5 Days of After Award of Contract	Electronic Format	Email to COR
28	Claims Held Report	12	Monthly	Electronic format	Email to COR
29	Record of Claims Reimbursement for Testing and Treatment to Eligible Providers.	24	Two (2) Times a Month	Electronic Format	Email to COR
30	Reimbursement Submissions	262	Daily (weekdays)	Electronic Format	Email to COR and HRSA Office of Budget and Finance
31	Reimbursement Return Payments - Process Report.	1	Prior to Contract Kickoff Meeting	Electronic Format	Email to COR

32	Approved Bank Account Monthly Utilization Reports.	12	Monthly	Electronic Format	Email to COR
33	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
34	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
35	Financial Management and Reporting Documentation.	1	Annually	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
36	Monthly Daily Extract of Financial Data Report.	262	Daily (weekdays)	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
37	Daily Incremental Extract File.	262	Daily (weekdays)	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
38	Specifics of the file structure, data elements, data dictionary.	1	Prior to Contract Kickoff Meeting	Electronic Format	Email to COR and Director, Division of Financial Policy and Analysis
39	Claims Reimbursement File formats.	1	Prior to Kickoff Meeting	Electronic Format	Email to COR and Director, Division of Financial

					Policy and Analysis
40	Claims Reimbursement Files, returned funds. Reports.	1			COR and Director, Division of Financial Policy and Analysis
41	Reimbursement Requests.	262	Daily/weekdays	Electronic Format	Email to COR
42	Process to identify and offset an overpayment to a provider.	1	Within Five (5) Days After Award of Contract	Electronic Format	Email to COR
43	Funds Exhausted Submissions.		When Funding is Exhausted	Electronic Format	Email to COR
44	FPLP Withholding to Payments Submissions.	1	Annually	Electronic Format	Email to Treasury
45	Internal Escalation and Issue Tracking Submissions.	1	Within 30 days of EDOC	Electronic Format	Email to COR
46	Log of All Reports and Data Requests.	12	Monthly	Electronic Format	Email to COR
47	Contractor Non-Disclosure Agreements.	1	Prior To Contractor Performance	Electronic Format	Email to COR
48	Incident Response.		As Required	Electronic Format	Email to HRSA Security Operations (SOC), CO, COR, HRSA SOP (or His or Her Designee) and Other Stakeholders
49	Roster.		As Required	Electronic Format	Email to COR
50	IT Required Reporting and Continuous Monitoring: a. Operating system, database, Web	12	Monthly	Electronic Format	Email to COR

	<p>application, and network vulnerability scan results;</p> <p>b. Updated POA&Ms;</p> <p>c. Any updated authorization package documentation as required by the annual attestation / assessment / review or as requested by the HRSA System Owner or AO; and,</p> <p>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.</p>				
51	SORN	1	Once completed	Electronic Format	HRSA Privacy Act Officer
52	ATO	1	Prior to system operation	Electronic format	HRSA Chief Information Officer
53	Transition Out Plan.	1	120 Days Prior to the End of Contract Performance	Electronic Format	Email to COR

F.5 Reporting Requirements and Deliverables

The Contractor shall submit the items in quantities and during the time periods indicated above to the following address or electronically as mutually agreed:

Health Resources and Services Administration
5600 Fishers Lane
Rockville, MD. 20857

The Contractor shall submit each deliverable items individually per the deliverable schedule.

F.6 Stop Work or Delay of Work

52.242-15 Stop-Work Order (Aug 1989)

52.242-15 Stop-Work Order (APR 1984)

52.242-17 Government Delay of Work (APR 1984)

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 Designation of Contracting Officer Representative (COR)

The person identified below is hereby designated as the Contracting Officer Representative (COR) for this contract. The responsibility of the COR is to assist in the technical monitoring and administration of the contract. To this end, the COR may provide technical direction to the contractor as described in Sections G.2 and G.3.

Daniel Bietz
5600 Fishers Lane
Rockville, MD. 20857
Phone: 301-443-0967
Email: dbietz@hrsa.gov

G.2 Contracting Officer's Representative's Authority

Technical Direction – The COR is authorized to provide the contractor with information, direction, and coordination within the confines of the contractual work description.

This includes providing technical direction to the Contractor to guide the contract effort in order to accomplish the contractual performance work statement. This may include the interpretation of specifications or technical portions of the work description, and where required by the contract, review and approval of product deliverables of the Contractor to the Government under the contract.

G.3 Restrictions on the Contracting Officer's Representative's Authority

The COR has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract nor in any way direct the contractor or its subcontractors to operate in conflict with the contract terms and conditions.

The COR is not authorized to provide technical direction outside the parameters of the performance work statement as stated in the Contract.

The COR may not issue any direction to the Contractor that:

1. Solicits a proposal, or
2. Constitutes an assignment of additional work outside the performance work statement of this Contract, or
3. In any manner causes an increase in the total contract cost or the time required for contract performance, or
4. Changes any of the express terms, conditions, or specifications of the Contract (e.g., changes in the price or scope of work, instructions to start or stop work, approval of any actions that will result in additional charges to the government).

If the contractor is unclear whether a technical direction is within the parameters of the performance work statement, then the contractor must contact the Contracting Officer, who is the only individual authorized to determine whether a technical direction is within the parameters of the performance work statement.

G.4 Key Personnel

Pursuant to the Key Personnel clause (HHSAR 352.242-70) referenced in Section I of this contract, the following individual(s) is (are) designated as Key Personnel and considered to be essential to the work being performed under this contract:

Program Manager
Denise Gillson
Phone: (952) 202-0381
Email: denise_gillson@uhg.com
PO Box 9472
Minneapolis, MN 55440

The person identified as the Program Manager shall direct the necessary work and services toward fulfillment of the contractual requirements. Prior to removing, replacing, or diverting the specified individual(s), the Contractor shall notify the Contracting Officer in writing and reasonably in advance, and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the contract. No diversion shall be made by the Contractor without the written consent of the Contracting Officer, provided that the Contracting Officer may ratify in writing changes made due to events beyond the control of the Contractor, and such ratification shall constitute the consent of the Contracting Officer required by this clause. Examples of events beyond the control of the Contractor are: (1) prolonged sickness, (2) termination of employment, and (3) death. Key personnel, with the consent of the Contracting Officer, may be amended from time to time during the course of the contract to either add or delete personnel, as appropriate.

G.5 Staffing Requirements

The general responsibilities of all contract personnel are as follows:

1. Consistently exhibit teamwork and provides best value for customers by improving the quality of customer interaction and communication, and internally improving communication to increase the quality and value of service provided.
2. Demonstrate proactive behavior, provides timely responsiveness, and exhibits a sense of ownership and commitment in all dealings.
3. Consistently perform timely follow through to ensure quality completion of customer actions. Actively engages in customer partnering sessions and lessons learned sessions. On a regular basis, shows initiative in problem identification and resolution.

4. Maintain the integrity and security of federally-owned property, including equipment, supplies, and information technology related hardware, software and data.
5. Effectively plan, organize, and prioritize work to accommodate agreed to dates/timelines as noted in the task order, and produce clear and effective results of acceptable quality.
6. Refer new or unusual circumstances in a timely manner to the COR for guidance.

G.6 Electronic Funds Transfer

The Contractor shall designate a financial institution for receipt of electronic funds transfer payments. Contractors are encouraged to periodically review their file for accuracy and are required to re-register before their expiration date, which is the same date as their CCR expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

G.7 Evaluation of Contractor's Performance

Interim and final evaluation of Contractor performance (including options) on this contract shall be conducted in accordance with FAR Subpart 42.15 and HHSAR 342.7001(d) and entered into the Contractors Performance Assessment Reporting System (CPARS) (located at Section J (Attachment B)).

The Government will conduct an evaluation of Contractor's performance based on the completion of the tasks stated in the PWS. HRSA documents contractor performance using the Contractor Performance Assessment Rating System (CPARS) (www.cpars.gov). The evaluation shall be conducted by the COR and be comprised of an evaluation of contractor performance completed by the Contractor and Federal staff, and a review of progress reports and financial reports.

G.8 Billing Instructions

Located at Section J (Attachment C).

G.9 Subcontracting Plan Provisions (Applies to Large Businesses)

1. Small Business and Small Disadvantaged Business Subcontracting Plan
 - a. The Small Business and Small Disadvantaged Business Subcontracting Plan, dated is attached hereto and made a part of this contract.
 - b. The failure of any contractor or subcontractor to comply in good faith with the Clause entitled "Utilization of Small Business Concerns and Small Disadvantaged Business Concerns" incorporated in this contract and the attached Subcontracting Plan, will be a material breach of such Contract or Subcontract.

2. Small Disadvantaged Business (SDB) Participation Plan

- a. The Small Disadvantaged Business (SDB) Participation Plan, dated [Insert Date] is attached hereto and made a part of this contract.
- b. In compliance with FAR 19, Small Disadvantaged Business Participation Program – Disadvantaged Status and Reporting, if this contract contains SDB participation targets, the Contractor shall report on the participation of SDB concerns. Reporting shall be on Optional Form 312, Small Disadvantaged Business Participation Report, or in the Contractor's own format providing the same information and shall be submitted on an annual basis and upon completion of the contract. In no event shall the targets identified in the attached SDB Participation Plan be revised without the prior written authorization of the Contracting Officer.
- c. The failure of any Contractor or subcontractor to comply in good faith with FAR Clause 19, entitled "Small Disadvantaged Business Participation Program -- Disadvantaged Status and Reporting" incorporated in this contract and the attached SDB Participation Plan, will be a material breach of such contract or subcontract and subject to the remedies reserved to the Government under FAR Clause 52.219-16 entitled, "Liquidated Damages-Subcontracting Plan."

3. Subcontracting Reports

- a. The Contractor shall submit the Individual Subcontract Report and the Summary Subcontract Report using the web-based Electronic Subcontracting Reporting System (eSRS at <http://www.esrs.gov>) following the instructions in eSRS as supplemented by agency regulations;
 - 1) Ensure that its subcontractors with subcontracting plans agree to submit the Individual Subcontract Report and/or the Summary Subcontract Report using eSRS;
 - 2) Provide the prime contract number, the order number, if applicable, and the prime contractor's DUNS number to all first-tier subcontractors with subcontracting plans so they can enter this information into eSRS with their reports; and
 - 3) Ensure that all subcontractors with subcontracting plans under the flow-down requirements of subparagraph (a)(9) above, at every tier, provide the prime contract number, the order number, if applicable and their own DUNS number to all of their subcontractors with subcontracting plans.
- b. Regardless of the effective date of this contract, the report shall be submitted on the following dates for the entire life of this contract:

April 25th and October 25th.

G.10 Limitation on Subcontracting (Applies to Small Businesses)

FAR 52.219-14 Limitations of Subcontracting (MAR 2020) is applicable to this contract and stated below in full text:

- (a) This clause does not apply to the unrestricted portion of a partial set-aside.
- (b) By submission of an offer and execution of a contract, the Offeror/Contractor agrees that in performance of the contract in the case of a contract for –
 - (1) Services (except construction). At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.
 - (2) Supplies (other than procurement from regular dealer in such supplies). The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.
 - (3) General construction. The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.
 - (4) Construction by special trade contractors. The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 Food

Food (including but not limited to meals, light refreshments, and beverages) is not to be provided and is an unallowable cost.

H.2 Equipment

The Contractor shall not use federal funding available through this contract for costs incurred for services or equipment which are reimbursable as part of another government contract. The federal funding available through this contract shall not be used to reimburse the contractor for the purchase of computer hardware and/or software without prior Contracting Officer approval.

H.3 Confidentiality Agreement Requirement

The Contractor shall implement a confidentiality agreement related to all data provided by the Government staff. All Contractor staff that work with the Federal Government and are provided information and access to databases shall sign such an agreement and a copy of the signed agreement for each relevant staff member shall be submitted to the COR prior to receipt of relevant documents.

H.4 Travel Reimbursement

Any travel reimbursement under this contract shall be performed in accordance with Federal Travel Regulations.

H.5 Prohibition Against Personal Services

The Contractor shall not perform personal services as defined under FAR 2.101 under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently governmental functions under this contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

H.6 Equal Employment Opportunity Posters

In order to comply with the notice posting requirements of FAR clause 52.222-26 Equal Opportunity as incorporated into the contract, the contractor shall obtain the posters from the following link: <https://www.eeoc.gov/employers/eo-law-poster>.

H.7 Post Award Organizational Conflict of Interest

General: The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.

Disclosure: The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contract or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.

Resolution: In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.

H.8 Government Ownership and Control of Contract-Related Data

All data furnished by the Government to the Contractor under this contract is deemed to be furnished to the Contractor under this contract by or on behalf of the Government under FAR 52.227-17, Rights in Data-Special Works, which is hereby incorporated by reference in this contract, solely with respect to such data.

For the avoidance of doubt, the Parties agree that all information previously held by the Contractor related to providers and all provider-related information that Contractor obtains outside of this contract, including through enrollment in the Optum Pay system, (collectively, "contractor's previously held information") may continue to be used by the Contractor in the normal course of its operations and that any data collected from providers that was not previously held by the Contractor or that was obtained outside of this contract shall be subject to the terms of the HRSA COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Website Privacy Policy, Terms of Use and the Optum Pay Enrollment Agreement (collectively "Terms") and may be used by the contractor as permitted by the Terms (<https://coviduninsuredclaim.linkhealth.com/>). Except as described in the previous sentence, any data provided by the Government in the performance of this contract shall not be used for any other purposes than the performance of this contract.

The contractor's previously held information includes:

*Provider demographic and bank account information captured by Contractor from providers enrolled in Optum Pay including bank routing and account numbers used to effectuate electronic funds transfers.

*All provider information held by Contractor relating to its provider networks or claims systems.

*Contractor's claims adjudication, claims payment and Optum Pay systems and processes.

*All systems, processes and information held or used by the Contractor that were developed or obtained by Contractor outside of the scope of this contract.

For the avoidance of doubt, the Parties further agree that none of Contractor's previously held information, systems or processes, including its payment processing and adjudication systems, will be delivered to the Government during the performance of this Contract, and that the Government has no right, title or interest in or to such payment processing and adjudication systems and processes.

H.9 Expectation of Confidentiality on all Submitted Data

Except to the extent such information has already been publicly disclosed or if disclosure is permitted in accordance with Section H.8 above, the Government's expectation is that all information in possession of Contractor that was submitted by providers as part of the HRSA COVID-19 Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Website, which consists of data related to testing, treatment or vaccination services rendered by providers to patients that is submitted to Contractor by providers in order to receive payment of uninsured claims (Collectively "Uninsured Provider Submission Data"), or provided to the Contractor by the Government (such as: Office of Inspector General's List of Excluded Individuals/Entities (LEIE), CMS Medicare Revocation List, CMS Medicaid Termination List, CMS Compliance Holds, Death Master File, Flagged Providers list / HRSA do not pay list) during the performance of this contract to process claims to eligible providers, as determined by the Government, will be kept confidential and not released to any third party unless required by a valid court order or otherwise required by law. Furthermore, upon completion of the contract, except as prohibited by law, the contractor is to provide the Government all the Uninsured Provider Submission Data used and collected during the performance of the contract. For the avoidance of doubt, Uninsured Provider Submission Data does not include any of contractor's previously held information.

H.10 Legal Process.

With respect to any legal process (including, but not limited to, subpoenas discovery requests) seeking disclosure of any contractor's previously held information or any data collected via the Optum Pay systems, Contractor is solely responsible for responding to any such request, and the costs associated with any such response.

With respect to any legal process from third-parties (including, but not limited to, subpoenas or discovery requests) seeking disclosure of the Uninsured Provider Submission Data, Contractor will oppose such legal process seeking discovery on the ground that the U.S. government is the real party in interest and has the sole legal right to possess, control, release, disclose or utilize such Data. Should the United States be substituted as a party in interest, the United States will

subsequently defend each such discovery request and legal action at no charge or expense to the Contractor. In each case, unless and until the United States Department of Justice successfully moves to substitute the United States Government as the real party in interest and is able to remove any such action that is in a state court to Federal Court, the Contractor will defend such legal action. Any responses to adverse legal process or defense of such litigation from third-parties in response by Contractor will be treated as within the scope of work under this contract, and such reasonable costs treated in accordance with FAR 31.205-47 Costs related to legal and other proceedings.

SECTION I – CONTRACT CLAUSES

I.1 Federal Acquisition Regulation (FAR) Contract Clauses

FAR 52.252-2 Clauses Incorporated by Reference (FEB 1998)

This contract incorporated one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at <https://www.acquisition.gov>.

Clause No.	Title	Date
52.202-1	Definitions	JUN 2020
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	JUN 2020
52.203-7	Anti-Kickback Procedures	JUN 2020
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	SEP 2007
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	JUN 2020
52.203-13	Contractor Code of Business Ethics and Conduct	JUN 2020
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	JUN 2020
52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation	JAN 2017
52.204-4	Printing/Copying Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-7	System for Award Management Maintenance	OCT 2018
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUN 2020
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance	AUG 2020
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2014
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-22	Alternative Line Item Proposal	JAN 2017

52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	OCT 2020
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	JUN 2020
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	OCT 2018
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
52.209-12	Certification Regarding Tax Matters	(FEB 2016)
52.210-1	Market Research	JUN 2020
52.212-4	Contract Terms and Conditions-Commercial Items	OCT 2018
52.212-5	Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items	JAN 2021
52.215-2	Audit and Records-Negotiation Alternate II	AUG 2016 (JUN 2020)
52.215-8	Order of Precedence - Uniform Contract Format	OCT 1997
52.215-10	Price Reductions for Defective Cost or Pricing Data	AUG 2011
52.215-11	Price Reduction for Defective Cost or Pricing Data – Modifications	JUN 2020
52.215-12	Subcontractor Certified Cost or Pricing Data	JUN 2020
52.215-13	Subcontractor Certified Cost of Pricing Data–Modifications	JUN 2020
52.215-14	Integrity of Unit Prices	JUN 2020
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	JULY 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost of Pricing Data or Information Other Than Cost or Pricing Data – Modifications	JUN 2020
52.215-23	Limitation on Pass-Through Charges	JUN 2020
52.216-7	Allowable Cost and Payment	AUG 2018
52.216-8	Fixed Fee	JUN 2011
52.217-8	Option to Extend Services	NOV 1999
52.219-8	Utilization of Small Business Concerns	OCT 2018
52.223-6	Drug-Free Workplace	(MAY 2001)
52.224-1	Privacy Act Notification	(APR 1984)
52.224-2	Privacy Act	(APR 1984)
52.225-25	Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran Representation and Certification	(JUN 2020)
52.232-1	Payments	(APR 1984)
52.232-9	Limitation on Withholding of Payments	(APR 1984)
52.232-39	Unenforceability of Unauthorized Obligations	(JUN 2013)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	(Dec 2013)

52.233-2	Service of Protest	(SEPT 2006)
52.237-3	Continuity of Services	(JAN 1991)
52.242-13	Bankruptcy	(JUL 1995)
52.244-5	Competition in Subcontracting	(DEC 1996)
52.244-6	Subcontracts for Commercial Items	(AUG 2019)
52.245-1	Government Property	(JAN 2017)
52.246-25	Limitation of Liability-Services	(FEB 1997)
52.252-6	Authorized Deviations in Clauses	(APR 1984)
52.253-1	Computer Generated Forms	(JAN 1991)

FAR Clauses in Full Text:

FAR 52.244-2 Subcontracts (JUN 2020).

(a) Definitions. As used in this clause -

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

Subcontract means any contract, as defined in FAR subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that -

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds -

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold, as defined in FAR 2.101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold, as defined in FAR 2.101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

- (i) A description of the supplies or services to be subcontracted.
- (ii) Identification of the type of subcontract to be used.
- (iii) Identification of the proposed subcontractor.
- (iv) The proposed subcontract price.
- (v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.
- (vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.
- (vii) A negotiation memorandum reflecting –
 - (A) The principal elements of the subcontract price negotiations;
 - (B) The most significant considerations controlling establishment of initial or revised prices;
 - (C) The reason certified cost or pricing data were or were not required;
 - (D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;
 - (E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;
 - (F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and
 - (G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to

quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (b), (c), or (d) of this clause.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination -

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

FAR 52.217-7 Option for Increased Quantity-Separately Priced Line Item (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

FAR 52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days.

FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within sixty days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

FAR 52.252-6 Authorized Deviations in Clauses (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any Department of Health and Human Services Acquisition Regulation (HHSAR) (48 CFR Chapter 3) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

I.2 Department of Health and Human Services Acquisition Regulation (HHSAR) Contract Clauses

Clause No.	Title	Date
HHSAR 352.203-70	Anti-Lobbying	(DEC 2015)
HHSAR 352.208-70	Printing and Duplication	(DEC 2015)
HHSAR 352.211-1	Public Accommodations and Commercial Facilities	(DEC 2015)
HHSAR 352.211-3	Paperwork Reduction Act	(DEC 2015)
HHSAR 352.219-70	Mentor Protégé Program	(DEC 2015)
HHSAR 352.219-71	Mentor Protégé Program Reporting	(JAN 2010)
HHSAR 352.224-70	Privacy Act	(DEC 2015)
HHSAR 352.227-70	Publications and Publicity	(DEC 2015)
HHSAR 352.231-70	Salary Rate Limitation	(DEC 2015)
HHSAR 352.233-71	Litigation and Claims	(DEC 2015)
HHSAR 352.239-74	Electronic and Information Technology Accessibility	(DEC 2015)

HHSAR Clauses in Full Text:

352.224-71 Confidential Information (DEC 2015)

- (a) Confidential Information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.
- (b) Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this contract. The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.
- (c) Confidential Information or records shall not be disclosed by the Contractor until:
- (1) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.
 - (2) For information provided by or on behalf of the government,
 - (i) The publication or dissemination of the following types of information are restricted under this contract: personally identifiable information about patients and donors.
 - (ii) The reason(s) for restricting the types of information identified in subparagraph (i) is/are: maintain patient and donor confidentiality and safety.
 - (iii) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.
- (d) Whenever the Contractor is uncertain with regard to the confidentiality of or a property interest in information under this contract, the Contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication.

SECTION J – LIST OF ATTACHMENTS

J.1 Solicitation Attachments

Attachment Letter	Title
A	Performance Work Statement
B	CPARs Information Sheet
C	Billing Instructions
D	Non-Disclosure Agreement

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 Designation of Contracting Officer Representative (COR)

The person identified below is hereby designated as the Contracting Officer Representative (COR) for this contract. The responsibility of the COR is to assist in the technical monitoring and administration of the contract. To this end, the COR may provide technical direction to the contractor as described in Sections G.2 and G.3.

Dina Passman
5600 Fishers Lane
Rockville, MD. 20857
Phone: 301-443-2337
Email: dpassman@hrsa.gov

G.2 Contracting Officer's Representative's Authority

Technical Direction – The COR is authorized to provide the contractor with information, direction, and coordination within the confines of the contractual work description.

This includes providing technical direction to the Contractor to guide the contract effort in order to accomplish the contractual performance work statement. This may include the interpretation of specifications or technical portions of the work description, and where required by the contract, review and approval of product deliverables of the Contractor to the Government under the contract.

G.3 Restrictions on the Contracting Officer's Representative's Authority

The COR has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract nor in any way direct the contractor or its subcontractors to operate in conflict with the contract terms and conditions.

The COR is not authorized to provide technical direction outside the parameters of the performance work statement as stated in the Contract.

The COR may not issue any direction to the Contractor that:

1. Solicits a proposal, or
2. Constitutes an assignment of additional work outside the performance work statement of this Contract, or
3. In any manner causes an increase in the total contract cost or the time required for contract performance, or
4. Changes any of the express terms, conditions, or specifications of the Contract (e.g., changes in the price or scope of work, instructions to start or stop work, approval of any actions that will result in additional charges to the government).

If the contractor is unclear whether a technical direction is within the parameters of the performance work statement, then the contractor must contact the Contracting Officer, who is the only individual authorized to determine whether a technical direction is within the parameters of the performance work statement.

G.4 Key Personnel

Pursuant to the Key Personnel clause (HHSAR 352.242-70) referenced in Section I of this contract, the following individual(s) is (are) designated as Key Personnel and considered to be essential to the work being performed under this contract:

Program Manager
Aditya Mutalik
Phone: (201) 647-1820
Email: aditya.mutalik@optum.com
10480 Little Patuxent Pkwy
Columbia, MD 21044

The person identified as the Program Manager shall direct the necessary work and services toward fulfillment of the contractual requirements. Prior to removing, replacing, or diverting the specified individual(s), the Contractor shall notify the Contracting Officer in writing and reasonably in advance, and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the contract. No diversion shall be made by the Contractor without the written consent of the Contracting Officer, provided that the Contracting Officer may ratify in writing changes made due to events beyond the control of the Contractor, and such ratification shall constitute the consent of the Contracting Officer required by this clause. Examples of events beyond the control of the Contractor are: (1) prolonged sickness, (2) termination of employment, and (3) death. Key personnel, with the consent of the Contracting Officer, may be amended from time to time during the course of the contract to either add or delete personnel, as appropriate.

G.5 Staffing Requirements

The general responsibilities of all contract personnel are as follows:

1. Consistently exhibit teamwork and provides best value for customers by improving the quality of customer interaction and communication, and internally improving communication to increase the quality and value of service provided.
2. Demonstrate proactive behavior, provides timely responsiveness, and exhibits a sense of ownership and commitment in all dealings.
3. Consistently perform timely follow through to ensure quality completion of customer actions. Actively engages in customer partnering sessions and lessons learned sessions. On a regular basis, shows initiative in problem identification and resolution.

4. Maintain the integrity and security of federally-owned property, including equipment, supplies, and information technology related hardware, software and data.
5. Effectively plan, organize, and prioritize work to accommodate agreed to dates/timelines as noted in the task order, and produce clear and effective results of acceptable quality.
6. Refer new or unusual circumstances in a timely manner to the COR for guidance.

G.6 Electronic Funds Transfer

The Contractor shall designate a financial institution for receipt of electronic funds transfer payments. Contractors are encouraged to periodically review their file for accuracy and are required to re-register before their expiration date, which is the same date as their CCR expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

G.7 Evaluation of Contractor's Performance

Interim and final evaluation of Contractor performance (including options) on this contract shall be conducted in accordance with FAR Subpart 42.15 and HHSAR 342.7001(d) and entered into the Contractors Performance Assessment Reporting System (CPARS) (located at Section J (Attachment B)).

The Government will conduct an evaluation of Contractor's performance based on the completion of the tasks stated in the PWS. HRSA documents contractor performance using the Contractor Performance Assessment Rating System (CPARS) (www.cpars.gov). The evaluation shall be conducted by the COR and be comprised of an evaluation of contractor performance completed by the Contractor and Federal staff, and a review of progress reports and financial reports.

G.8 Billing Instructions

Located at Section J (Attachment C).

G.9 Subcontracting Plan Provisions (Applies to Large Businesses)

1. Small Business and Small Disadvantaged Business Subcontracting Plan
 - a. The Small Business and Small Disadvantaged Business Subcontracting Plan, dated is attached hereto and made a part of this contract.
 - b. The failure of any contractor or subcontractor to comply in good faith with the Clause entitled "Utilization of Small Business Concerns and Small Disadvantaged Business Concerns" incorporated in this contract and the attached Subcontracting Plan, will be a material breach of such Contract or Subcontract.

2. Small Disadvantaged Business (SDB) Participation Plan

- a. The Small Disadvantaged Business (SDB) Participation Plan, dated [Insert Date] is attached hereto and made a part of this contract.
- b. In compliance with FAR 19, Small Disadvantaged Business Participation Program – Disadvantaged Status and Reporting, if this contract contains SDB participation targets, the Contractor shall report on the participation of SDB concerns. Reporting shall be on Optional Form 312, Small Disadvantaged Business Participation Report, or in the Contractor's own format providing the same information and shall be submitted on an annual basis and upon completion of the contract. In no event shall the targets identified in the attached SDB Participation Plan be revised without the prior written authorization of the Contracting Officer.
- c. The failure of any Contractor or subcontractor to comply in good faith with FAR Clause 19, entitled "Small Disadvantaged Business Participation Program -- Disadvantaged Status and Reporting" incorporated in this contract and the attached SDB Participation Plan, will be a material breach of such contract or subcontract and subject to the remedies reserved to the Government under FAR Clause 52.219-16 entitled, "Liquidated Damages-Subcontracting Plan."

3. Subcontracting Reports

- a. The Contractor shall submit the Individual Subcontract Report and the Summary Subcontract Report using the web-based Electronic Subcontracting Reporting System (eSRS at <http://www.esrs.gov>) following the instructions in eSRS as supplemented by agency regulations;
 - 1) Ensure that its subcontractors with subcontracting plans agree to submit the Individual Subcontract Report and/or the Summary Subcontract Report using eSRS;
 - 2) Provide the prime contract number, the order number, if applicable, and the prime contractor's DUNS number to all first-tier subcontractors with subcontracting plans so they can enter this information into eSRS with their reports; and
 - 3) Ensure that all subcontractors with subcontracting plans under the flow-down requirements of subparagraph (a)(9) above, at every tier, provide the prime contract number, the order number, if applicable and their own DUNS number to all of their subcontractors with subcontracting plans.
- b. Regardless of the effective date of this contract, the report shall be submitted on the following dates for the entire life of this contract:

April 25th and October 25th.

G.10 Limitation on Subcontracting (Applies to Small Businesses)

FAR 52.219-14 Limitations of Subcontracting (MAR 2020) is applicable to this contract and stated below in full text:

- (a) This clause does not apply to the unrestricted portion of a partial set-aside.
- (b) By submission of an offer and execution of a contract, the Offeror/Contractor agrees that in performance of the contract in the case of a contract for –
 - (1) Services (except construction). At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.
 - (2) Supplies (other than procurement from regular dealer in such supplies). The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.
 - (3) General construction. The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.
 - (4) Construction by special trade contractors. The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Purpose of Contract

The purpose of this requirement 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 and Facilities for Testing, Treatment, and Vaccine Administration for the Uninsured Program (Uninsured Program).

B.2 Consideration and Payment

This is a Firm Fixed Price (FFP) contract. In consideration for satisfactory performance of the services outlined in the Performance Work Statement located at Section J (Attachment A), the following payment schedule will be utilized.

Base Period

The maximum reimbursement that may be dispersed during the Base Period is 42,862,928 submitted (billed) claims, 29,488,437 paid claims, 90,137,072 submitted (billed) claims, and 85,511,563 paid claims for CLINs 0002, 0003, 0010, and 0011, respectively.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0001	Management and Administration Fees	12	Month	(b) (4)	(b) (4)
0002	Fee per submitted (billed) claim	42,862,928	Each	(b) (4)	(b) (4)
0003	Fee per paid claim	29,488,437	Each	(b) (4)	(b) (4)
0010	Add-on to Fee per Submitted (billed) claim.	90,137,072	Each	(b) (4)	(b) (4)
0011	Add-on to Fee per Paid Claim	85,511,563	Each	(b) (4)	(b) (4)
Total Value Base Period (Not to Exceed):					(b) (4)

Note: The pricing for CLINs 0001, 0002, and 0003 reflects an overall (b) (4).

Option Period One

The maximum reimbursement that may be dispersed during the Option Period One is 7,000,000 for submitted (billed) claims and 3,000,000 for paid claims.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1001	Management and Administration Fees	12	Month	(b) (4)	(b) (4)
1002	Fee per submitted (billed) claim	7,000,000	Each	(b) (4)	(b) (4)
1003	Fee per paid claim	3,000,000	Each	(b) (4)	(b) (4)
Total Value Option Period One (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

Option Period Two

The maximum reimbursement that may be dispersed during the Option Period Two is 4,000,000 for submitted (billed) claims and 1,000,000 for paid claims.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2001	Management and Administration Fees	12	Month	(b) (4)	(b) (4)
2002	Fee per submitted (billed) claim	4,000,000	Each	(b) (4)	(b) (4)
2003	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
Total Value Option Period Two (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

B.2.1 Allowable Costs

Costs shall be determined by the Contracting Officer to be allowable in accordance with FAR Subpart 31 in effect on the date of this Contract and the terms of this Contract.

B.2.2 Prior Authorization of Certain Direct Costs

1. Requirements for purchase orders and subcontracts are governed by FAR 52.244-2, Subcontracts (JUN 2020) of the General Provisions except as may be indicated herein.
2. The Contractor shall not incur any of the following costs without the prior written approval of the Contracting Officer. Incurrence of such costs with the intent of claiming reimbursement as direct costs under this contract shall be at the Contractor's own risk:

- a. Purchase of any item of equipment, including furniture or office equipment, regardless of cost;
- b. Any rental agreement for real or personal property, or any term contract for maintenance;
- c. Travel for general scientific meetings; and
- d. Rearrangement, alternation or relocation of facilities.

B.2.3 Requirement to notify Government and Limitation of Government's Obligation

1. By the 15th day of each month, the Contractor shall advise the Government of the number of reimbursement.

If the number of reimbursement is likely to exceed the maximum specified in B.2 for the applicable contract period, the contractor shall notify the Government as soon as practicable. The notification shall advise the Contracting Officer of the estimated increase in number of reimbursement.

2. The Government's payment obligation under the per claim is limited to payment for the actual number of claims, up to the maximum number of claims specified for the applicable contract period. Under no event shall the Government be obligated to pay for more than the actual number of claims.

B.3 Optional Item and Quantity Pricing

1. During the base period of performance, CLIN 0009 may be exercised once.
2. During the respective period of performance, each of these CLIN 0004, 1004 and 2004 may be exercised once per period.
3. The unit pricing for the Fee per Submitted (billed) Claims, Fee per Paid Claims, OIG Interviews and TIN Investigations CLINs will be determined by the number of reimbursements dispersed during each period of performance, as set forth below.

Base Period

CLIN 0005 may be exercised for up to 9,000,000 units in the Base Period.

CLIN 0006 may be exercised for up to 3,000,000 units in the Base Period.

CLIN 0007 may be exercised for up to 25 units in the Base Period.

CLIN 0008 may be exercised for up to 70 units in the Base Period.

CLIN 0012 may be exercised for up to 9,000,000 units in the Base Period.

CLIN 0013 may be exercised for up to 3,000,000 units in the Base Period.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0004	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
0005	Fee per submitted (billed) claim	9,000,000	Each	(b) (4)	(b) (4)
0006	Fee per paid claim	3,000,000	Each	(b) (4)	(b) (4)
0007	OIG Interview	25	Each	(b) (4)	(b) (4)
0008	TIN Investigation	70	Each	(b) (4)	(b) (4)
0009	Optional Task 2 – Fraud Detection	1	Lot	To Be Negotiated Prior To Exercising	To Be Negotiated Prior To Exercising
0012	Fee per submitted (billed) claim	9,000,000	Each	(b) (4)	(b) (4)
0013	Fee per paid claim	3,000,000	Each	(b) (4)	(b) (4)
Total Value Base Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing for CLINs 0004, 0005, 0006, 0007, and 0008 reflects an overall (b) (4)

(b) (4)

Option Period One

CLIN 1005 may be exercised for up to 4,000,000 units in Option Period One.
 CLIN 1006 may be exercised for up to 1,000,000 units in Option Period One.
 CLIN 1007 may be exercised for up to 25 units in the Option Period One.
 CLIN 1008 may be exercised for up to 60 units in the Option Period One.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1004	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
1005	Fee per submitted (billed) claim	4,000,000	Each	(b) (4)	(b) (4)
1006	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
1007	OIG Interview	25	Each	(b) (4)	(b) (4)
1008	TIN Investigation	60	Each	(b) (4)	(b) (4)
Total Value Option Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

Option Period Two

CLIN 2005 may be exercised for up to 3,000,000 units in Option Period Two.
 CLIN 2006 may be exercised for up to 1,000,000 units in Option Period Two.
 CLIN 2007 may be exercised for up to 25 units in the Option Period Two.
 CLIN 2008 may be exercised for up to 60 units in the Option Period Two.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2004	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
2005	Fee per submitted (billed) claim	3,000,000	Each	(b) (4)	(b) (4)
2006	Fee per paid claim	1,000,000	Each	(b) (4)	(b) (4)
2007	OIG Interview	25	Each	(b) (4)	(b) (4)
2008	TIN Investigation	60	Each	(b) (4)	(b) (4)
Total Value Option Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Note: The pricing above reflects an overall (b) (4).

B.4 Total Estimated Contract Value is: (b) (4)

SECTION A – STANDARD FORM (SF) 33

This page intentionally left blank.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Purpose of Contract

The purpose of this requirement is to provide disbursement of payments to eligible health care providers for health care related expenses and/or lost revenues that are attributable to COVID-19.

B.2 Consideration and Payment

This is a Firm Fixed Price (FFP) contract. In consideration for satisfactory performance of the services outlined in the Performance Work Statement located at Section J (Attachment A), the following payment schedule will be utilized.

Base Period

The maximum reimbursement that may be dispersed during the Base Period is 700,000 unless the optional quantities under B.3 are exercised, if any.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0001	Infrastructure, Management and Operation Fees	12	Month	(b) (4)	(b) (4)
0002	Fee per PRF Reimbursement	700,000	Each	(b) (4)	(b) (4)
Total Value Base Period (Not to Exceed):					(b) (4)

(b) (4)

Option Period One

The maximum reimbursement that may be dispersed during the Option Period One is 150,000 unless the optional quantities under B.3 are exercised, if any.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1001	Infrastructure, Management and Operations Fees	12	Month	\$(b) (4)	\$(b) (4)
1002	Fee per PRF Reimbursement	150,000	Each	(b) (4)	(b) (4)
Total Value Option Period One (Not to Exceed):					(b) (4)

Note: (b) (4)

Option Period Two

The maximum reimbursement that may be dispersed during the Option Period Two is 50,000 unless the optional quantities under B.3 are exercised, if any.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2001	Infrastructure, Management and Operations Fees	12	Month	(b) (4)	(b) (4)
2002	Fee per PRF Reimbursement	50,000	Each	(b) (4)	(b) (4)
Total Value Option Period Two (Not to Exceed):					(b) (4)

Note: (b) (4)

B.2.1 Allowable Costs

Costs shall be determined by the Contracting Officer to be allowable in accordance with FAR Subpart 31 in effect on the date of this Contract and the terms of this Contract.

B.2.2 Prior Authorization of Certain Direct Costs

1. Requirements for purchase orders and subcontracts are governed by FAR 52.244-2, Subcontracts (JUN 2020) of the General Provisions except as may be indicated herein.
2. The Contractor shall not incur any of the following costs without the prior written approval of the Contracting Officer. Incurrence of such costs with the intent of claiming reimbursement as direct costs under this contract shall be at the Contractor's own risk:
 - a. Purchase of any item of equipment, including furniture or office equipment, regardless of cost;
 - b. Any rental agreement for real or personal property, or any term contract for maintenance;
 - c. Travel for general scientific meetings; and
 - d. Rearrangement, alternation or relocation of facilities.

B.2.3 Requirement to notify Government and Limitation of Government's Obligation

1. By the 15th day of each month, the Contractor shall advise the Government of the number of reimbursement.

If the number of reimbursement is likely to exceed the maximum specified in B.2 for the applicable contract period, the contractor shall notify the Government as soon as

practicable. The notification shall advise the Contracting Officer of the estimated increase in number of reimbursement.

2. The Government’s payment obligation under the per reimbursement is limited to payment for the actual number of reimbursements, up to the maximum number of reimbursements specified for the applicable contract period. Under no event shall the Government be obligated to pay for more than the actual number of reimbursements.

B.3 Optional Item and Quantity Pricing

1. During the respective period of performance, each of these CLIN 0003, 1003 and 2003 may be exercised once per period.
2. The unit pricing for the Fee per PRF Reimbursement CLINs will be determined by the number of reimbursements dispersed during each period of performance, as set forth below.

Base Period

CLIN 0004 may be exercised for up to 300,000 units in the Base Period.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
0003	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
0004	Fee per PRF Reimbursement	300,000	Each	(b) (4)	(b) (4)
Total Value Base Period Optional Item and Quantities (Not to Exceed):					(b) (4)

Option Period One

CLIN 1004 may be exercised for up to 500,000 units in Option Period One.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
1003	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
1004	Fee per PRF Reimbursement	500,000	Each	(b) (4)	(b) (4)
Total Value Option Period One Optional Item and Quantities (Not to Exceed):					(b) (4)

Option Period Two

CLIN 2004 may be exercised for up to 500,000 units in the Base Period.

CLIN	Description	Quantity	Unit of Issue	Unit Price	Totals
2003	Optional Task 1 – Transition Out Plan	1	Lot	(b) (4)	(b) (4)
2004	Fee per PRF Reimbursement	500,000	Each	(b) (4)	(b) (4)
Total Value Option Period Two Optional Item and Quantities (Not to Exceed):					(b) (4)

B.4 Total Estimated Contract Value is: (b) (4)

SECTION C – DESCRIPTION/SPECIFICATIONS/ STATEMENT OF WORK

C.1 Performance Work Statement

Independently and not as an agent of the Government, the Contractor shall furnish all personnel, material, facilities, services, and equipment as needed to perform the Performance Work Statement located at Section J (Attachment A), attached hereto and made part of this document.

SECTION D – PACKAGING AND MARKING

D.1 Packaging and Marking

All reports and documents shall have, at a minimum, in the document header, the contract number, and the Contracting Officer Representative (COR) name. All reports and documents shall have, at a minimum in the document footer, the author in the lower left corner, the page # of total # of pages in the center bottom of the page, and the date and /or version of the document (not the auto date) in the lower right corner.

The Contractor shall deliver all items at the time indicated in the Deliverables Schedule.

All deliverable reports are to carry at the top of the first page the following information:

Contract number
Deliverable item number
Deliverable item delivery due date
Date of submission

SECTION E – INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

The Contracting Officer's Representative (COR), as a duly authorized representative of the Contracting Officer, shall assume the responsibilities for monitoring the Contractor's performance, evaluating the quality of services provided by the Contractor and performing final inspection and acceptance of all deliverables.

E.2 Inspection

FAR 52.246-4 Inspection of Services – Fixed-Price (Aug 1996)

- (a) Definition. "Services," as used in this clause, includes services performed, workmanship, and material furnished or utilized in the performance of services.
- (b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires.
- (c) The Government has the right to inspect and test all services called for by the contract, to the extent practicable at all times and places during the term of the contract. The Government shall perform inspections and tests in a manner that will not unduly delay the work.
- (d) If the Government performs inspections or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties.
- (e) If any of the services do not conform with contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by reperformance, the Government may –
 - (1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and
 - (2) Reduce the contract price to reflect the reduced value of the services performed.
- (f) If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with contract requirements, the Government may –

(1) By contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Government that is directly related to the performance of such service; or

(2) Terminate the contract for default.

E.3 Quality Assurance Surveillance Plan (QASP)

The Government will monitor the Contractor's performance under this contract in accordance with the QASP. The following is a sample Quality Assurance Surveillance Plan (QASP):

Task Area	Evaluation Measure	Performance Standard/Acceptable Quality Level (AQL)	Method Used	Frequency
All Tasks	Status Reporting	Timely information on project status AQL: Submitted timely 97% of time	Inspection	Monthly
	Fraudulent Report	Report within 1-hour of detection.	Time (days/hours) of report from detection	When Fraudulent request detected
	Payment Filing and Processing	Payment filing and processing AQL: Within 4 days	Inspection	Monthly
	Successful Payment Rate	Clean-payment rate AQL: 90% payment rate	Inspection	Monthly
	Documentation Deliverable	Secure and confidential patient information AQL: 100% patient information is secured and confidential	Inspection	Monthly
	Defined Processes	Call center and payment return processes AQL: Reduce by 50%	Inspection	Monthly
	Funding Request Accuracy	Status of payments AQL: No more than 1 revision per week	Report	Monthly
	Reconciled Payment	Reconciled successful and returned ACH and check payment AQL:	Report	Monthly
	Call Center Resolution	Call center call issues AQL: Resolves 95% of calls	Report	Weekly
	Call Center Response Rates	Increase adjudication rates AQL: Within 5 minutes	Inspection	Monthly

SECTION F – DELIVERIES OR PERFORMANCE

F.1 Period of Performance

The period of performance will be for one (1) 12 month base period with two (2) 12 month option periods. The option periods under this contract may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). The base period of performance will start date on April 7, 2021, through April 6, 2022.

F.2 Place of Performance

Work shall be performed under this contract off-site, primarily at the contractor's facilities, which includes work performed by staff that telecommute.

F.3 Observance of Federal Holidays

New Year's Day	January 1st
Martin Luther King, Jr. Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4th
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	November 11th
Thanksgiving Day	Fourth Thursdays in November
Christmas Day	December 25th
Inauguration Day	Every fourth year after 1965, January 20th, Washington, DC

No on-site services shall be performed, nor shall HRSA reimburse a contractor for work performed on Federal legal holidays, holidays set forth by Presidential Executive Order and any other Government closures, including closures for inclement weather, unless otherwise provided for in the terms of the contract. The contractor may not bill for hours not worked.

F.4 Schedule of Deliverables

The contractor shall ensure all products and services delivered under this contract are compliant with HHS Section 508 requirements 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 Standard 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 HHS 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 identified in the HHS Section 508 checklists;

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
1	Secure File Transfer Mechanism.		Two Weeks After EDOC	Electronic Format	Email to COR.
2	Program/ Project Plan.		Two Weeks After EDOC	Electronic Format	Email to COR.
3	Program Status Report.		Daily	Electronic Format	Email to COR.
4	Accounting Extract File Format.		Two Weeks After EDOC	Electronic Format	Email to COR.
5	Payment File Integrity Validation.		Each Payment File	Electronic Format	Email to COR.
6	Funding Request.		Prior To An Approved Payment Disbursement Or Upon Check Clearance	Electronic Format	Email to COR.

7	Payment Data File.		Daily	Electronic Format	Email to COR.
8	Provider Payment Email Notification Template.		Prior To Each Payment Wave	Electronic Format	Email to COR.
9	Customer Service Help Desk Report.		As requested, not more than 4 times per year.	Electronic Format	Email to COR.
10	Customer Service Open HHS/HRSA Queue.		As New Items Are Added	Electronic Format	Email to COR.
11	Quality Assurance Surveillance Plan.		A Draft Is Due 2 Weeks After Award With Quarterly Updates. Updates Due By The 5th Day Of Each Quarter. QASP Metrics Should Be Delivered To HRSA Along With The Monthly Contract Status Report.	Electronic Format	Email to COR.
12	ACH Payment Accounting Detail.		Ad Hoc	Electronic Format	Email to COR.
13	Provider Attestation Report.		Bi-Weekly	Electronic Format	Email to COR.
14	Attestation / Demographic Detail.		Bi-Weekly	Electronic Format	Email to COR.
15	Ad Hoc Reports To Support Program Operations.		Within three days unless otherwise stated.	Electronic Format	Email to COR.

16	Report Request Log.		Monthly	Electronic Format	Email to COR.
17	System Demo And Screenshots Of Each Provider Facing System.		Before And After Each Change	Electronic Format	Email to COR.
18	FAQs And Or Scripts Developed By The Contractor Call Center.		As requested, no more than 6 times per year	Electronic Format	Email to COR.
19	Contractor Procedures And Processes In Support Of The Program.		As They Are Developed Or Updated	Electronic Format	Email to COR.
20	Final Report.		30 Days Before The Contract End Date	Electronic Format	Email to COR.
21	PRF Records And Artifacts Produced By The Contractor And Contractor Bank.		15 Days Before The Contract End Date.	Electronic Format	Email to COR.
22	Records Management - Provide documentation on maintaining Federal Records to include Records Management Schedule and Disposition Plan		30 Days after Award	Electronic Format	Email to COR.
23	Records Management Training - Provide Records Management training completion certificates		Within 30 days after contract award and 14 days after new fulltime staff onboarding.	Electronic Format	Email to COR.

F.5 Reporting Requirements and Deliverables

The Contractor shall submit the items in quantities and during the time periods indicated above to the following address or electronically as mutually agreed:

Health Resources and Services Administration
5600 Fishers Lane
Rockville, MD. 20857

The Contractor shall submit each deliverable items individually per the deliverable schedule.

F.6 Stop Work or Delay of Work

52.242-15 Stop-Work Order (Aug 1989)

52.242-15 Stop-Work Order (APR 1984)

52.242-17 Government Delay of Work (APR 1984)

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 Designation of Contracting Officer Representative (COR)

The person identified below is hereby designated as the Contracting Officer Representative (COR) for this contract. The responsibility of the COR is to assist in the technical monitoring and administration of the contract. To this end, the COR may provide technical direction to the contractor as described in Sections G.2 and G.3.

Daniel Bietz
5600 Fishers Lane
Rockville, MD. 20857
Phone: 301-443-0967
Email: dbietz@hrsa.gov

G.2 Contracting Officer's Representative's Authority

Technical Direction – The COR is authorized to provide the contractor with information, direction, and coordination within the confines of the contractual work description.

This includes providing technical direction to the Contractor to guide the contract effort in order to accomplish the contractual performance work statement. This may include the interpretation of specifications or technical portions of the work description, and where required by the contract, review and approval of product deliverables of the Contractor to the Government under the contract.

G.3 Restrictions on the Contracting Officer's Representative's Authority

The COR has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract nor in any way direct the contractor or its subcontractors to operate in conflict with the contract terms and conditions.

The COR is not authorized to provide technical direction outside the parameters of the performance work statement as stated in the Contract.

The COR may not issue any direction to the Contractor that:

1. Solicits a proposal, or
2. Constitutes an assignment of additional work outside the performance work statement of this Contract, or
3. In any manner causes an increase in the total contract cost or the time required for contract performance, or
4. Changes any of the express terms, conditions, or specifications of the Contract (e.g., changes in the price or scope of work, instructions to start or stop work, approval of any actions that will result in additional charges to the government).

If the contractor is unclear whether a technical direction is within the parameters of the performance work statement, then the contractor must contact the Contracting Officer, who is the only individual authorized to determine whether a technical direction is within the parameters of the performance work statement.

G.4 Key Personnel

Pursuant to the Key Personnel clause (HHSAR 352.242-70) referenced in Section I of this contract, the following individual(s) is (are) designated as Key Personnel and considered to be essential to the work being performed under this contract:

The person identified as the Program Manager shall direct the necessary work and services toward fulfillment of the contractual requirements. Prior to removing, replacing, or diverting the specified individual(s), the Contractor shall notify the Contracting Officer in writing and reasonably in advance, and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the contract. No diversion shall be made by the Contractor without the written consent of the Contracting Officer, provided that the Contracting Officer may ratify in writing changes made due to events beyond the control of the Contractor, and such ratification shall constitute the consent of the Contracting Officer required by this clause. Examples of events beyond the control of the Contractor are: (1) prolonged sickness, (2) termination of employment, and (3) death. Key personnel, with the consent of the Contracting Officer, may be amended from time to time during the course of the contract to either add or delete personnel, as appropriate.

G.5 Staffing Requirements

The general responsibilities of all contract personnel are as follows:

1. Consistently exhibit teamwork and provides best value for customers by improving the quality of customer interaction and communication, and internally improving communication to increase the quality and value of service provided.
2. Demonstrate proactive behavior, provides timely responsiveness, and exhibits a sense of ownership and commitment in all dealings.
3. Consistently perform timely follow through to ensure quality completion of customer actions. Actively engages in customer partnering sessions and lessons learned sessions. On a regular basis, shows initiative in problem identification and resolution.
4. Maintain the integrity and security of federally-owned property, including equipment, supplies, and information technology related hardware, software and data.
5. Effectively plan, organize, and prioritize work to accommodate agreed to dates/timelines as noted in the task order, and produce clear and effective results of acceptable quality.
6. Refer new or unusual circumstances in a timely manner to the COR for guidance.

G.6 Electronic Funds Transfer

The Contractor shall designate a financial institution for receipt of electronic funds transfer payments. Contractors are encouraged to periodically review their file for accuracy and are required to re-register before their expiration date, which is the same date as their CCR expiration date. SAM will notify users by e-mail that their file is due to expire beginning 60 days prior to expiration, then 30 days and finally 15 days before expiration.

G.7 Evaluation of Contractor's Performance

Interim and final evaluation of Contractor performance (including options) on this contract shall be conducted in accordance with FAR Subpart 42.15 and HHSAR 342.7001(d) and entered into the Contractors Performance Assessment Reporting System (CPARS) (located at Section J (Attachment B)).

The Government will conduct an evaluation of Contractor's performance based on the completion of the tasks stated in the PWS. HRSA documents contractor performance using the Contractor Performance Assessment Rating System (CPARS) (www.cpars.gov). The evaluation shall be conducted by the COR and be comprised of an evaluation of contractor performance completed by the Contractor and Federal staff, and a review of progress reports and financial reports.

G.8 Billing Instructions

Located at Section J (Attachment C).

G.9 Subcontracting Plan Provisions (Applies to Large Businesses)

1. Small Business and Small Disadvantaged Business Subcontracting Plan
 - a. The Small Business and Small Disadvantaged Business Subcontracting Plan, dated is attached hereto and made a part of this contract.
 - b. The failure of any contractor or subcontractor to comply in good faith with the Clause entitled "Utilization of Small Business Concerns and Small Disadvantaged Business Concerns" incorporated in this contract and the attached Subcontracting Plan, will be a material breach of such Contract or Subcontract.
2. Small Disadvantaged Business (SDB) Participation Plan
 - a. The Small Disadvantaged Business (SDB) Participation Plan, dated [Insert Date] is attached hereto and made a part of this contract.
 - b. In compliance with FAR 19, Small Disadvantaged Business Participation Program – Disadvantaged Status and Reporting, if this contract contains SDB participation

targets, the Contractor shall report on the participation of SDB concerns. Reporting shall be on Optional Form 312, Small Disadvantaged Business Participation Report, or in the Contractor's own format providing the same information and shall be submitted on an annual basis and upon completion of the contract. In no event shall the targets identified in the attached SDB Participation Plan be revised without the prior written authorization of the Contracting Officer.

- c. The failure of any Contractor or subcontractor to comply in good faith with FAR 19, entitled "Small Disadvantaged Business Participation Program -- Disadvantaged Status and Reporting" incorporated in this contract and the attached SDB Participation Plan, will be a material breach of such contract or subcontract and subject to the remedies reserved to the Government under FAR 52.219-16 entitled, "Liquidated Damages-Subcontracting Plan."

3. Subcontracting Reports

- a. The Contractor shall submit the Individual Subcontract Report and the Summary Subcontract Report using the web-based Electronic Subcontracting Reporting System (eSRS at <http://www.esrs.gov>) following the instructions in eSRS as supplemented by agency regulations;
 - 1) Ensure that its subcontractors with subcontracting plans agree to submit the Individual Subcontract Report and/or the Summary Subcontract Report using eSRS;
 - 2) Provide the prime contract number, the order number, if applicable, and the prime contractor's DUNS number to all first-tier subcontractors with subcontracting plans so they can enter this information into eSRS with their reports; and
 - 3) Ensure that all subcontractors with subcontracting plans under the flow-down requirements of subparagraph (a)(9) above, at every tier, provide the prime contract number, the order number, if applicable and their own DUNS number to all of their subcontractors with subcontracting plans.
- b. Regardless of the effective date of this contract, the report shall be submitted on the following dates for the entire life of this contract:

April 25th and October 25th.

G.10 Limitation on Subcontracting (Applies to Small Businesses)

FAR 52.219-14 Limitations of Subcontracting (MAR 2020) is applicable to this contract and stated below in full text:

- (a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) By submission of an offer and execution of a contract, the Offeror/Contractor agrees that in performance of the contract in the case of a contract for –

- (1) Services (except construction). At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.
- (2) Supplies (other than procurement from regular dealer in such supplies). The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.
- (3) General construction. The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.
- (4) Construction by special trade contractors. The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 Food

Food (including but not limited to meals, light refreshments, and beverages) is not to be provided and is an unallowable cost.

H.2 Equipment

The Contractor shall not use federal funding available through this contract for costs incurred for services or equipment which are reimbursable as part of another government contract. The federal funding available through this contract shall not be used to reimburse the contractor for the purchase of computer hardware and/or software without prior Contracting Officer approval.

H.3 Confidentiality Agreement Requirement

The Contractor shall implement a confidentiality agreement related to all data provided by the Government staff. All Contractor staff that work with the Federal Government and are provided information and access to databases shall sign such an agreement and a copy of the signed agreement for each relevant staff member shall be submitted to the COR. All contractor personnel that will be provided Federal Government information and access to databases and who are dedicated to the Program shall execute a confidentiality agreement that will be submitted to the COR within 14 days of the effective date of the contract. Thereafter any dedicated personnel coming onto the Program shall execute a confidentiality agreement, and the confidentiality agreement will be provided to the COR, prior to receiving access to Federal Government information and databases. Non-dedicated Contractor personnel brought onto the Program to meet volume demands will execute a confidentiality agreement that will be submitted to the COR within 14 days after the end of the calendar month in which they first receive access to Federal Government information and databases.

H.4 Travel Reimbursement

Any travel reimbursement under this contract shall be performed in accordance with Federal Travel Regulations.

H.5 Prohibition Against Personal Services

The Contractor shall not perform personal services as defined under FAR 2.101 under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently governmental functions under this

contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

H.6 Equal Employment Opportunity Posters

In order to comply with the notice posting requirements of FAR clause 52.222-26 Equal Opportunity as incorporated into the contract, the contractor shall obtain the posters from the following link: <https://www.eeoc.gov/employers/eo-law-poster>.

H.8 Organizational Conflict of Interest

General: The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.

Disclosure: The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contract or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.

Resolution: In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.

H.9 Government Ownership and Control of Contract-Related Data

All data furnished by the Government to the Contractor under this contract is deemed to be furnished to the Contractor under this contract by or on behalf of the Government under FAR 52.227-17, Rights in Data-Special Works, which is hereby incorporated by reference in this contract, solely with respect to such data.

For the avoidance of doubt, the Parties agree that all information previously held by the Contractor related to providers and all provider-related information that Contractor obtains outside of this contract, including through enrollment in the Optum Pay system, (collectively, "contractor's previously held information") may continue to be used by the Contractor in the normal course of its operations and that any data collected from providers that was not previously held by the Contractor or that was obtained outside of this contract shall be subject to the terms of the CARES Provider Relief Fund (PRF) Website Privacy Policy, Terms of Use and the Optum Pay Enrollment Agreement (collectively "Terms") and may be used by the contractor

as permitted by the Terms (<https://cares.linkhealth.com/#/ms>), and that any data provided by the Government in the performance of this contract shall not be used for any other purposes than the performance of this contract. For the purposes of this clause, all data furnished by the Government refers to payment files sent to the Contractor by the Government. Payment files sent to the contractor by the Government include the following information: TIN, Telephone Number, Email address, Line 1 Street Address, Line 2 Street Address, City Name, State code, ZIP code, COVID Payment, Company Name, Tax Payer ID, Provider Name, Bank Account Number, Routing Number.

The contractor's previously held information includes:

*Provider demographic and bank account information captured by Contractor from providers enrolled in Optum Pay including bank routing and account numbers used to effectuate electronic funds transfers.

*All provider information held by Contractor relating to its provider networks or claims systems.

*The Contractor's previously held information is considered proprietary to the contractor and will not be delivered to, used by or released to the Government under this contract.

For the avoidance of doubt, the Parties further agree that none of Contractor's systems or processes, including its payment processing and adjudication systems, will be delivered to the Government during the performance of this Contract, and that the Government has no right, title or interest in or to such payment processing and adjudication systems and processes.

H.10 Expectation of Confidentiality on all Submitted Data

Except to the extent such information has already been publicly disclosed, the Government's expectation is that all information in possession of Contractor that was submitted by providers as part of the CARES Provider Relief Fund (PRF) Application and Attestation Portal ("PRF Attestation and Payment Data") or provided to the Contractor by the Government during performance of this contract to direct contractor payments to eligible providers, as determined by the Government, will be kept confidential and not released to any third party unless required by a valid court order or otherwise required by law. Furthermore, upon completion of the contract, except as prohibited by law, the contractor is to provide the Government all the PRF Attestation and Payment Data used and collected during the performance of the contract. For the avoidance of doubt, PRF Attestation and Payment Data does not include any of contractor's previously held information or PRF application data because PRF application data is not collected by the Contractor.

H.11 Legal Process.

With respect to any legal process (including, but not limited to, subpoenas discovery requests) seeking disclosure of any contractor previously held information or any data collected via the Optum Pay systems, Contractor is solely responsible for responding to any such request, and the costs associated with any such response.

With respect to any legal process from third-parties (including, but not limited to, subpoenas or discovery requests) seeking disclosure of the PRF Attestation and Payment Data, Contractor will oppose such legal process seeking discovery on the ground that the U.S. government is the real party in interest and has the sole legal right to possess, control, release, disclose or utilize such Data. Should the United States be substituted as a party in interest, the United States will subsequently defend each such discovery request and legal action at no charge or expense to the Contractor. In each case, unless and until the United States Department of Justice successfully moves to substitute the United States Government as the real party in interest and is able to remove any such action that is in a state court to Federal Court, the Contractor will defend such legal action. Any responses to adverse legal process or defense of such litigation from third-parties in response by Contractor will be treated as within the scope of work under this contract, and such reasonable costs treated in accordance with FAR 31.205-47 Costs related to legal and other proceedings.

SECTION I – CONTRACT CLAUSES

I.1 Federal Acquisition Regulation (FAR) Contract Clauses

FAR 52.252-2 Clauses Incorporated by Reference (FEB 1998)

This contract incorporated one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at <https://www.acquisition.gov>.

Clause No.	Title	Date
52.202-1	Definitions	JUN 2020
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	JUN 2020
52.203-7	Anti-Kickback Procedures	JUN 2020
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	SEP 2007
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	JUN 2020
52.203-13	Contractor Code of Business Ethics and Conduct	JUN 2020
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	JUN 2020
52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation	JAN 2017
52.204-4	Printing/Copying Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-7	System for Award Management Maintenance	OCT 2018
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUN 2020
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance	AUG 2020
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2014
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-22	Alternative Line Item Proposal	JAN 2017
52.209-6	Protecting the Government's Interest When Subcontracting	

	with Contractors Debarred, Suspended, or Proposed for Debarment	JUN 2020
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	OCT 2018
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
52.209-12	Certification Regarding Tax Matters	(FEB 2016)
52.210-1	Market Research	JUN 2020
52.212-4	Contract Terms and Conditions-Commercial Items	OCT 2018
52.212-5	Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items	JAN 2021
52.215-2	Audit and Records-Negotiation Alternate II	AUG 2016 (JUN 2020)
52.215-8	Order of Precedence - Uniform Contract Format	OCT 1997
52.215-10	Price Reductions for Defective Cost or Pricing Data	AUG 2011
52.215-11	Price Reduction for Defective Cost or Pricing Data – Modifications	JUN 2020
52.215-12	Subcontractor Certified Cost or Pricing Data	JUN 2020
52.215-13	Subcontractor Certified Cost of Pricing Data–Modifications	JUN 2020
52.215-14	Integrity of Unit Prices	JUN 2020
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-17	Wavier of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	JULY 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost of Pricing Data or Information Other Than Cost or Pricing Data – Modifications	JUN 2020
52.215-23	Limitation on Pass-Through Charges	JUN 2020
52.216-7	Allowable Cost and Payment	AUG 2018
52.216-8	Fixed Fee	JUN 2011
52.219-8	Utilization of Small Business Concerns	OCT 2019
52.223-6	Drug-Free Workplace	(MAY 2001)
52.224-1	Privacy Act Notification	(APR 1984)
52.224-2	Privacy Act	(APR 1984)
52.225-25	Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran Representation and Certification	(JUN 2020)
52.232-1	Payments	(APR 1984)
52.232-9	Limitation on Withholding of Payments	(APR 1984)
52.232-39	Unenforceability of Unauthorized Obligations	(JUN 2013)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	(Dec 2013)
52.233-2	Service of Protest	(SEPT 2006)
52.237-3	Continuity of Services	(JAN 1991)
52.242-13	Bankruptcy	(JUL 1995)
52.244-5	Competition in Subcontracting	(DEC 1996)

52.244-6	Subcontracts for Commercial Items	(AUG 2019)
52.245-1	Government Property	(JAN 2017)
52.246-25	Limitation of Liability-Services	(FEB 1997)
52.252-6	Authorized Deviations in Clauses	(APR 1984)
52.253-1	Computer Generated Forms	(JAN 1991)

FAR Clauses in Full Text:

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (DEC 2019).

The Offeror shall not complete the representation in this provision if the Offeror has represented that it “does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument” in the provision at 52.204-26, Covered Telecommunications Equipment or Services-Representation, or in paragraph (v) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Items.

(a) Definitions. As used in this provision - “Covered telecommunications equipment or services”, “critical technology”, and “substantial or essential component” have the meanings provided in clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. Section 889(a) (1) (A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing -

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(d) Representation. The Offeror represents that it ___ will, ___ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

(e) Disclosures. If the Offeror has represented in paragraph (d) of this provision that it “will” provide covered telecommunications equipment or services”, the Offeror shall provide the following information as part of the offer -

(1) A description of all covered telecommunications equipment and services offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

FAR 52.244-2 Subcontracts (JUN 2020).

(a) Definitions. As used in this clause -

"Approved purchasing system" means a Contractor’s purchasing system that has been reviewed and approved in accordance with part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer’s written consent for the Contractor to enter into a particular subcontract.

Subcontract means any contract, as defined in FAR subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that -

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds -

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold, as defined in FAR 2.101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold, as defined in FAR 2.101 on the date of subcontract award, or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting –

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason certified cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (b), (c), or (d) of this clause.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination -

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

FAR 52.217-7 Option for Increased Quantity-Separately Priced Line Item (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

FAR 52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days.

FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within sixty days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

FAR 52.252-6 Authorized Deviations in Clauses (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any Department of Health and Human Services Acquisition Regulation (HHSAR) (48 CFR Chapter 3) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

I.2 Department of Health and Human Services Acquisition Regulation (HHSAR) Contract Clauses

Clause No.	Title	Date
HHSAR 352.203-70	Anti-Lobbying	(DEC 2015)
HHSAR 352.208-70	Printing and Duplication	(DEC 2015)

HHSAR 352.211-1	Public Accommodations and Commercial Facilities	(DEC 2015)
HHSAR 352.211-3	Paperwork Reduction Act	(DEC 2015)
HHSAR 352.219-70	Mentor Protégé Program	(DEC 2015)
HHSAR 352.219-71	Mentor Protégé Program Reporting	(JAN 2010)
HHSAR 352.224-70	Privacy Act	(DEC 2015)
HHSAR 352.227-70	Publications and Publicity	(DEC 2015)
HHSAR 352.231-70	Salary Rate Limitation	(DEC 2015)
HHSAR 352.233-71	Litigation and Claims	(DEC 2015)
HHSAR 352.239-74	Electronic and Information Technology Accessibility	(DEC 2015)

HHSAR Clauses in Full Text:

352.224-71 Confidential Information (DEC 2015)

(a) Confidential Information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this contract. The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.

(c) Confidential Information or records shall not be disclosed by the Contractor until:

(1) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.

(2) For information provided by or on behalf of the government,

(i) The publication or dissemination of the following types of information are restricted under this contract: personally identifiable information about patients and donors.

(ii) The reason(s) for restricting the types of information identified in subparagraph (i) is/are: maintain patient and donor confidentiality and safety.

(iii) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

(d) Whenever the Contractor is uncertain with regard to the confidentiality of or a property interest in information under this contract, the Contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication.

352.239-73 Electronic and Information Technology Accessibility Notice (DEC 2015)

(a) Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 and the Architectural and Transportation Barriers Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at <http://www.hhs.gov/web/508>. The complete text of the Section 508 Final Provisions can be accessed at <http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards>.

(c) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-74, Electronic and Information Technology Accessibility.

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document - in detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS website <http://www.hhs.gov/web/508>.

In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

SECTION J – LIST OF ATTACHMENTS

J.1 Solicitation Attachments

Attachment Letter	Title
A	Performance Work Statement
B	CPARs Information Sheet
C	Billing Instructions
D	Non-Disclosure Agreement