COUNTY PROGRAM AGREEMENT

Refugee Health Screening

DSHS Agreement Number
2363-46782

This Program Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the County identified below, and is issued in conjunction with a County and DSHS Agreement On General Terms and Conditions, which is incorporated by reference.

Administration or Division Agreement Number

County Agreement Number
1783-86629

DSHS ADMINISTRATION	DSHS DIVISION	DSHS INDEX NUMBER	DSHS CONTRACT CODE
Economic Services Administration	Community Services Division	1065	3000CC-63

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Cathy Vue Program Manager	1700 E Cherry Street Seattle, WA 98122

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(206)568-5597	Click here to enter text.	vuec@dshs.wa.gov

COUNTY NAME	COUNTY ADDRESS
Snohomish County Snohomish County Health Department	3020 Rucker Ave Suite 203 Everett, WA 98201
COUNTY FEDERAL EMPLOYER IDENTIFICATION NUMBER	COUNTY CONTACT NAME Katie Curtis

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(425) 339-8711		katie.curtis@co.snohomish.wa.us

IS THE COUNTY A SUBRECIPIENT FOR PURPOSES OF THIS PROGRAM AGREEMENT?	ASSISTANCE LISTING NUMBERS
No	

PROGRAM AGREEMENT START DATE	**PROGRAM AGREEMENT END DATE**	MAXIMUM PROGRAM AGREEMENT AMOUNT
01/01/2023	09/30/2023	$257,000.00

EXHIBITS. When the box below is marked with an X, the following Exhibits are attached and are incorporated into this County Program Agreement by reference:

☒ **Exhibits (specify):** Exhibit A - Data Security Requirements **Exhibit B – Statement of Work (SOW)**

☐ **No Exhibits.**

The terms and conditions of this Contract are an integration and representation of the final, entire and exclusive understanding between the parties superseding and merging all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Contract. The parties signing below represent that they have read and understand this Contract, and have the authority to execute this Contract. This Contract shall be binding on DSHS only upon signature by DSHS.

COUNTY SIGNATURE(S)	PRINTED NAME(S) AND TITLE(S)	DATE(S) SIGNED
Harper, Lacey Digitally signed by Harper, Lacey Date: 2023.06.13 13:00:32 -07'00'	Lacey Harper, Executive Director	06/13/2023
DSHS SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
Doina Dobrin	Doina Dobrin, Contracts Officer DSHS,ESA-Community Services Division	06/20/2023

1. Definitions. The words and phrases listed below, as used in this Contract, shall each have the following definitions:

a. "Class A and B conditions" are medical notifications made by the U.S. Public Health Service regarding refugees arriving in the U.S. with medical conditions. The Class A condition is one needing immediate assessment and follow-up. The Class B condition is one needing assessment/diagnosis and follow-up soon after arrival in the U.S.

b. "Contract" or "Agreement" means the entire written agreement between DSHS and the Contractor, including any Exhibits, documents, or materials incorporated by reference.

c. "ESA" means the DSHS Economic Services Administration.

d. "Refugee" means persons who have entered the United States with refugee status, or persons who have been granted asylum under section 208 of the Immigration and Nationality Act, Cuban-Haitian Entrants with requirements in 45 CFR, Part 401, and victims of trafficking documented by the Federal Office of Refugee Resettlement, certain Amerasians from Vietnam, or Special Immigrant Visa Holders.

e. "ORIA" means the DSHS Office of Refugee and Immigrant Assistance within the Community Services Division.

f. "USCIS" means the U.S. Citizenship and Immigration Services.

2. Purpose.

The purpose of this Contract is to assist refugees in obtaining a domestic refugee health screening outlined by the Center for Disease Prevention and Control and the Office of Refugee Resettlement. The Contractor shall follow the Washington State Guidelines, incorporated by reference.

3. Statement of Work.

The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of work as described in this Contract and the attached Exhibit(s).

4. Consideration.

The total amount payable to the Contractor for satisfactory performance of work completed under this Contract shall not exceed the Contract Maximum Amount shown on page one (1) of this Contract, and shall be paid in accordance with the fees set forth in the attached Exhibit(s).

5. Billing and Payment.

a. Invoice System.

The Contractor must use State Form A19-1A Invoice Voucher when submitting invoices. The Contractor shall submit one invoice for each month of service and each invoice must be received by ORIA no later than thirty (30) days after the last day of each month. Previously denied claims and services not billed in the month actually provided, may be included in a future quarterly invoice.

b. The Contractor may submit one (1) additional final September invoice to ORIA for any previously denied claims or services provided but not billed during the current federal fiscal year of this contract. The final invoice must be received by ORIA by December 31, 2023.

c. Each Invoice Voucher submitted for payment must be accompanied by:

(1) A completed Contract Summary Report, format provided by DSHS;

(2) A completed Monthly Billing Datasheet, format provided by DSHS. Client details include but not limited to: First Name, Last Name, Alien Number, Date of Birth, Sex, Country of Origin, Arrival Date, Date of Service, Status at Time of Entry, Type of Visit, and any other client details requested by DSHS.

(3) Other additional receipts or backup documentation that provides clarification or gives detail regarding the A19-1A Invoice Voucher submitted for payment.

d. Payment.

Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and acceptance of properly completed forms. Payment shall be sent to the address designated by the Contractor on page one of this Contract. DSHS may, at its sole discretion, withhold payment claimed by the Contractor for services rendered if Contractor fails to satisfactorily comply with any term or condition of this Contract.

6. Data Sharing. DSHS will provide the Contractor access to client information on an as needed basis.

a. Purpose.

(1) Activity for which the Data is needed: To provide services to eligible clients.
(2) How Data Recipient will use Data: Contractor will use client information to administer this Contract. This includes but is not limited to the following:

(a) Billing;
(b) Reporting; and
(c) Client information updates.

b. Description of Data.

(1) Data elements. Client's personal information including but not limited to:

(a) Date of Birth;
(b) Gender;
(c) Date of Arrival or Asylum Granted;
(d) Alien Number;
(e) Immigration Status; and
(f) DSHS Client ID.
(g) Domestic screening data (sent directly to DOH, covered by DSHS DOH data share agreement)

(2) Time frame(s) for Data disclosure or exchange: Duration of Contract.

(3) Conditions under which, if any, that Data disclosed or exchanged can be linked to other data:

The Contractor shall not link the data with Personal Information or individually identifiable data from any other source nor re-disclose or duplicate the data unless specifically authorized to do so in this Contract or by the prior written consent of DSHS.

c. Data Access or Transfer.

(1) Staff Access to Data.

(a) Access to Data shall be limited to staff that are assigned to provide services under this Contract.

(b) The Contractor shall provide the DSHS Contact listed of their staff that are providing services under this Contract that have been granted access to the DSHS client information.

(c) The Contractor shall contact the DSHS Contact whenever they need to change the staff that are granted access to the DSHS client information.

(2) Method. DSHS will provide the Contractor DSHS client information via Secure e-mail and/or secure file transfer.

(3) Requirements for Access.

(a) Prior to making Data available to its staff, the Contractor shall notify all such staff of the Use and Disclosure requirements.

(b) Staff that are authorized to have access to DSHS data must annually review and sign a DSHS ESA Nondisclosure of Confidential Information Agreement-Non Employee form (DSHS 03-374D).

i. The Contractor shall retain the original signed copies of the forms for their records.
ii. Upon DSHS request, the Contractor shall provide DSHS with copies of the signed forms.

(4) Frequency of Exchange: Daily access.

d. Limitations on Use of Data.

If the Data and analyses generated by Data Recipient contain personal information about DSHS clients, then any and all reports utilizing these Data shall be subject to review and approval by the Data Provider prior to publication in any medium or presentation in any forum.

e. Security of Data.

Data Protection. The Data Recipient shall exercise due care to protect Data from unauthorized physical and electronic access. Due care includes establishing and maintaining security policies, standards, and procedures which detail:

(a) Access security, identification, and authentication;
(b) Network and workstation security;
(c) Premise security; and
(d) Sanctions for unauthorized use or disclosure of Data.

(2) Data Disposition.

(a) The Data provided will remain the property of the Data Provider and will be promptly destroyed by the Data Recipient, or returned to the Data Provider, when the work for which the Data was required, as fully described herein, is completed. This includes removal of the Data from hard drives upon which the Data may have been stored, in a way that prevents

the Data from being retrieved (such as by using a “wipe” utility).

(b) DSHS shall not process the Contractor’s final invoice for payment until such time that the Contractor has taken action to properly dispose of the Data and has signed a Disposition of Data form provided by DSHS and provided the completed form to the DSHS Contact or designee listed on page one (1) of this Contract.

f. Confidentiality and Nondisclosure.

(1) The Data Recipient may use Personal Information and other information or Data gained by reason of this Contract only for the purposes of this Contract.

(2) The Data Recipient shall not disclose, transfer, or sell any such information to any party, except as provided by law or, in the case of Personal Information, without the prior written consent of the person to whom the Personal Information pertains.

(a) The Contractor shall use an Authorization to Release Information form and file the signed release forms in each participant’s file.

(b) The Data Recipient shall maintain the confidentiality of all Personal Information and other information gained by reason of this Contract. Further, the Data Recipient shall not link the Data with Personal Information or individually identifiable data from any other source nor re-disclose or duplicate the Data unless specifically authorized to do so in this Contract or by the prior written consent of DSHS.

g. Portable Devices or Media.

(1) The Contractor must obtain written permission from the DSHS Contact listed on page one (1) of Contract prior to using portable devices or portable media for purposes related to providing services under this Contract. The Contractor shall provide DSHS with information about the type of portable devices or portable media that will be used.

(1) The use of portable devices or portable media is subject to requirements of Exhibit A, Data Security Requirements.

(2) The Contractor shall provide training about the Exhibit A, Data Security Requirements to all of their staff that will be using portable devices or portable media that contain DSHS Data. The Contractor shall keep a copy of the training materials, a record which contains the dates of the training and the names of the staff who attended the training.

(3) The Contractor shall keep the following records about their use of portable devices or media:

(a) Type of portable devices or portable media used;
(b) Serial Numbers;
(c) Proof of encryption of DSHS Data; and
(d) Check-in and check-out system which identifies which of the Contractors staff is using the portable devices or media that contains DSHS Data.

(4) The Contractor must have a process in place that will ensure that they on a weekly basis download all DSHS Data from portable device or portable media to a secure storage method as described in Exhibit A, Data Security Requirements. The Contractor shall keep a record of dates of the weekly storage download and the storage method.

The Contractor shall upon the request of DSHS make the records required in this section

available to DSHS.

h. Data Recipient Change of Circumstance and Contact Information.

(1) The Data Recipient shall notify Data Provider within ten (10) business days when staff no longer need access to secure information related to this Contract.

(2) The Data Recipient shall notify Data Provider within ten (10) business days any information concerning a change of circumstances. For the purposes of this Agreement, changes in circumstances include but are not limited to: contact information, address, telephone number, fax number, e-mail address; Location or practice.

i. **Breach or Potential Compromise of DSHS Information**. As provided in Exhibit A of this Agreement, the compromise or potential compromise of Confidential Information must be reported to the DSHS contact on page one (1) of this agreement within one (1) business day of discovery. The notifying party shall take immediate action to mitigate the risk of loss and comply with any notification or other requirements imposed by law. The Contractor shall report any lost or stolen portable devices or media to the DSHS contact within one (1) calendar day of discovery.

7. Child Abuse and Health and Safety Concerns.

In the delivery of services under this Contract, children's health and safety shall always be the first concern of the Contractor. The Contractor shall immediately report all instances of suspected child abuse to Child Protective Services at 1-866-END HARM (1-866-363-4276).

8. Contract Suspension.

DSHS may take certain actions in the event the Contractor, or any of its partners, officers, directors, or employees, is investigated by a local, county, state or federal agency, for a matter which DSHS determines may adversely affect the delivery of services provided under this Contract. DSHS may, without prior notice, either suspend the delivery of services or disallow the person(s) involved in the allegation(s) from providing services or having contact with clients pending final resolution of the investigation.

9. Contractor Information.

The Contractor shall forward to DSHS within ten (10) working days, any information concerning the Contractor's change of circumstances. Changes in the Contractor's circumstances include change of business name, address, telephone number, fax number, e-mail address, business status, and names of staff that are current state employees.

10. Culturally Relevant Services.

The Contractor shall ensure all services are provided in the cultural context of the client and/or the client's family.

11. Dispute Resolution.

Either party may submit a request for resolution of a contract dispute (rates set by law, regulation, or DSHS policy are not disputable). The requesting party shall submit a written statement identifying the issue(s) in dispute and the relative positions of the parties. A request for a dispute resolution must include the Contractor's name, address, and Contract number, and be mailed to the address listed below within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue in dispute.

DSHS/ESA/Community Services Division
Attn: Contracts Administrator
P.O. Box 45470
Olympia, WA 98504-5470

12. Fraud Reporting.

The Contractor shall report any knowledge of welfare fraud to DSHS by calling 1-800-562-6906 or on-line.

13. Insurance.

a. DSHS certifies that it is self-insured under the State's self-insurance liability program, as provided by RCW 4.92.130, and shall pay for losses for which it is found liable.

b. The Contractor certifies, by checking the appropriate box below, initialing to the left of the box selected, and signing this Agreement, that:

LH ☒ The Contractor is self-insured or insured through a risk pool and shall pay for losses for which it is found liable; or

_____ ☐ The Contractor maintains the types and amounts of insurance identified below and shall, prior to the execution of this Agreement by DSHS, provide certificates of insurance to that effect to the DSHS contact on page one of this Agreement.

Commercial General Liability Insurance (CGL) – to include coverage for bodily injury, property damage, and contractual liability, with the following minimum limits: Each Occurrence - $1,000,000; General Aggregate - $2,000,000. The policy shall include liability arising out of premises, operations, independent contractors, products-completed operations, personal injury, advertising injury, and liability assumed under an insured contract. The State of Washington, DSHS, its elected and appointed officials, agents, and employees shall be named as additional insureds

14. Record Keeping.

The Contractor shall maintain client records and shall make the client files available to ORIA for monitoring purposes**.**

Exhibit A – Data Security Requirements

1. Definitions. The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:

a. "AES" means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf).

b. "Authorized Users(s)" means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.

c. "Business Associate Agreement" means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.

d. "Category 4 Data" is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.

e. "Cloud" means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

f. "Encrypt" means to encode Confidential Information into a format that can only be read by those possessing a "key"; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

g. "FedRAMP" means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.

h. "Hardened Password" means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

i. "Mobile Device" means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

j. "Multi-factor Authentication" means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. "PIN" means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

k. "Portable Device" means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.

l. "Portable Media" means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.

m. "Secure Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.

n. "Trusted Network" means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.

o. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

2. **Authority**. The security requirements described in this document reflect the applicable requirements of Standard 141.10 (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: https://www.dshs.wa.gov/ffa/keeping-dshs-client-information-private-and-secure, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.

3. **Administrative Controls.** The Contractor must have the following controls in place:

a. A documented security policy governing the secure use of its computer network and systems, and

which defines sanctions that may be applied to Contractor staff for violating that policy.

b. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

c. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

4. Authorization, Authentication, and Access. In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

a. Have documented policies and procedures governing access to systems with the shared Data.

b. Restrict access through administrative, physical, and technical controls to authorized staff.

c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.

d. Ensure that only authorized users are capable of accessing the Data.

e. Ensure that an employee's access to the Data is removed immediately:

(1) Upon suspected compromise of the user credentials.

(2) When their employment, or the contract under which the Data is made available to them, is terminated.

(3) When they no longer need access to the Data to fulfill the requirements of the contract.

f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.

g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:

(1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.

(2) That a password does not contain a user's name, logon ID, or any form of their full name.

(3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.

(4) That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk and enforce password and logon requirements for users by employing measures including:

(1) Ensuring mitigations applied to the system don't allow end-user modification.

(2) Not allowing the use of dial-up connections.

(3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

(4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.

(5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point.

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

(1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor

(2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)

(3) Must not contain a "run" of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

(1) Be a minimum of six alphanumeric characters.

(2) Contain at least three unique character classes (upper case, lower case, letter, number).

(3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

k. Render the device unusable after a maximum of 10 failed logon attempts.

5. Protection of Data. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives**. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network server disks**. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other

authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives**. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents**. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.

f. **Remote Access**. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

g. **Data storage on portable devices or media**.

(1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:

(a) Encrypt the Data.

(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

(d) Apply administrative and physical security controls to Portable Devices and Portable Media by:

i. Keeping them in a Secure Area when not in use,

ii. Using check-in/check-out procedures when they are shared, and

iii. Taking frequent inventories.

(2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.

h. **Data stored for backup purposes**.

(1) DSHS Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

(2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

i. **Cloud storage**. DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Contractor has control of the environment in which the Data is stored. For this reason:

(1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

(a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the Contractor network.

(c) The Data will remain Encrypted during transmission to the Cloud.

(d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.

(e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DSHS.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Contractor's network.

(2) Data will not be stored on an Enterprise Cloud storage solution unless either:

(a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,

(b) The Cloud storage solution used is FedRAMP certified.

(3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. System Protection. To prevent compromise of systems which contain DSHS Data or through which that Data passes:

a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.

b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.

c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.

d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. Data Segregation.

a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

(1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,

(2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,

(3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,

(4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.

(5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.

b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

8. Data Disposition. When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

9. **Notification of Compromise or Potential Compromise**. The compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

10. **Data shared with Subcontractors**. If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this contract for review and approval.

Exhibit B – Statement of Work (SOW)

REFUGEE HEALTH SCREENING
STATEMENT OF WORK

1. **Purpose.** The purpose of this Contract is to provide health screening, outreach, access and follow-up to health assessment services with primary care, community health clinics, or specialty care for newly arrived refugees.

2. **Reference.** The following information is available for the Contractor's use and incorporated by reference under this Contract.

a. The Domestic Medical Screening Guidelines Checklist for Newly Arriving Refugees which provides guidance around screening asymptomatic refugees.

b. The Washington State Plan Refugee Screening Guidelines- Attachment A which provides guidance as to what activities are funded through RMA.

3. **Refugee Client Eligibility.** The Contractor shall provide refugee health screening services to refugee participants who meet the following specific criteria:

a. Persons have entered the United States and have status as a refugee, Cuban-Haitian entrant, Special Immigrant Visa holders, those granted asylum, or Humanitarian Parolees eligible for ORR-benefits. Eligibility also includes certain Amerasians from Vietnam who are admitted to the U.S. as immigrants, victims of a severe form of torture who receive certified or eligibility letters from the Office of Refugee Resettlement, or clients eligible for ORR-funded programs and services.

b. Have an I-94 or other verifiable documentation indicating refugee or eligible status.

c. Have completed the health screening process within the first 90 days of their date of arrival in the United States and are resettling in the Contractor's service area.

d. Secondary arrivals who did not complete the health screening process in another state and resettle in the Contractor's service area within 90 days of their arrival to the United States.

4. **Contractor Obligations.**

Per the ORR State Letter 13-10 and our Washington State Plan for providing Refugee Services and the State Plan Refugee Screening Guidelines – Attachment A document, all Refugee Health Screening activities billable to Medicaid shall be billed to Medicaid. If services billed to Medicaid are denied, payment shall be made by DSHS. The Contractor must obtain documentation or proof of Medicaid denial.

The Contractor shall provide or subcontract for the following services:

a. **Coordination.** Coordinate with the Voluntary Agencies (VOLAGs) serving the Contractor's service area, to provide information and education to VOLAG staff and newly arrived refugees about health screening and adjustment of status. In accordance with HIPPA regulations, assure that VOLAG staff are informed of any needed information that will assist the refugee in their resettlement process. Assure that priority is given to referrals for newly arriving refugees who have a Class A or B medical condition. This may include the following:

(1) Coordinate with the refugee or VOLAG case manager to schedule a health screening appointment.

(2) Coordinate with the refugee's primary care provider regarding necessary follow-up.

b. **Physical (or Clinical) Screening.** Perform health screening based on the Washington State Domestic Screening Guidelines Checklist, including physical exam, laboratory tests, diagnostic tests and immunizations. Screening activities must be completed within the first 90 days of client's ORR-eligibility date.

c. **Interpreter Services.** Coordinate all necessary interpreter services needed to provide refugee health care. To qualify for reimbursement, interpreters used must be tested and certified/qualified through the DSHS Medical Interpreter testing process or through a DSHS approved medical interpreter testing process.

d. **Civil Surgeon Certification.** The Contractor should maintain "Civil Surgeon" status through USCIS and may provide Civil Surgeon Certification of immunizations on the United States Citizenship and Immigration Services (USCIS) immunization record (I-693) within 18 months of the refugee's arrival in the United States. If desired by the client, provide a certified immunization record (I-693) to indicate immunizations are complete.

e. **Client follow-up and referral as needed to assure access to on-going medical care:** Make initial referrals to community medical/dental/mental health professionals as indicated from the health screening.

f. **Service Coordination.** Attend relevant refugee meetings and trainings, including but not limited to:

(1) Quarterly WA Health Coalition Meetings and Trainings;

(2) Quarterly Local Refugee Community Consultation Meetings;

(3) DSHS ORIA Provider Meetings and Trainings;

(4) DOH Annual Screening Meetings; and,

(5) Other meetings as requested by DOH or DSHS.

5. **Reporting.** The Contractor shall submit:

a. To Washington State Department of Health a completed Refugee Health Domestic Screening form for each refugee screened. Forms must be submitted as soon as a screening is completed and no later than 30 days from screening completion.

b. To DSHS ORIA with request for payment, a completed Monthly Client Billing Datasheet, format provided by DSHS. Client details include but not limited to: First Name, Last Name, Alien Number, Date of Birth, Sex, Country of Origin, Arrival Date, Date of Service, Status at Time of Entry, Type of Visit, and any other client details requested by DSHS.

6. **Consideration.** The Contractor shall receive payment up to **$257,000.00** during the contract period based on the following:

Payment Point 1: Indirect costs for clinic operation for actual time spent providing services as outlined in Section 4, above to the refugee population.

Payment Point 2: Direct actual costs for all activities related to providing the direct client services as outlined on the Washington State Domestic Medical Screening Guidelines for Public Health Care Based Screening and the Civil Surgeon Certification.

Payment Point 3: Interpreter services shall be paid at actual cost with receipt(s) for services. Supporting documentation shall be submitted.

Payment Point 4: Medicaid denials reimbursed by DSHS at billable costs. Supporting documentation shall be submitted.