

 <p>Washington State Department of Social &amp; Health Services</p> <p><i>Transforming lives</i></p>	<h2>INTERLOCAL DATASHARE AGREEMENT</h2> <p><b>Washington Connection</b></p>	DSHS Agreement Number: 2291-37341	
This Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the Contractor identified below, and is issued pursuant to the Interlocal Cooperation Act, chapter 39.34 RCW.		Program Contract Number:  Contractor Contract Number:	
CONTRACTOR NAME  Harborview Medical Center		CONTRACTOR doing business as (DBA)	
CONTRACTOR ADDRESS  325 9th Ave Box 359760 Seattle, WA 98104-2420		WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)  578-037-394	DSHS INDEX NUMBER  1145
CONTRACTOR CONTACT  Sandra Herrera	CONTRACTOR TELEPHONE  (206) 744-4486	CONTRACTOR FAX  (206) 744-8652	CONTRACTOR E-MAIL ADDRESS  sherrera@uw.edu
DSHS ADMINISTRATION  Economic Services Administration	DSHS DIVISION  Community Services Division	DSHS CONTRACT CODE  3067DS-91	
DSHS CONTACT NAME AND TITLE  Jessica Gempler Program Administrator		DSHS CONTACT ADDRESS  712 SE Pear St  Olympia, WA 98504	
DSHS CONTACT TELEPHONE  (509)655-0117	DSHS CONTACT FAX  <a href="#">Click here to enter text.</a>	DSHS CONTACT E-MAIL ADDRESS  Jessica.gempler@dshs.wa.gov	
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT?  No		CFDA NUMBER(S)	
AGREEMENT START DATE  02/01/2022	AGREEMENT END DATE  01/31/2024	MAXIMUM AGREEMENT AMOUNT  No Payment	
<b>EXHIBITS. The following Exhibits are attached and are incorporated into this Agreement by reference:</b> <input checked="" type="checkbox"/> <b>Data Security: Exhibit A – Data Security Requirements</b> <input type="checkbox"/> <b>Exhibits (specify):</b>			
The terms and conditions of this Agreement 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 Agreement, between the parties. The parties signing below represent they have read and understand this Agreement, and have the authority to execute this Agreement. This Agreement shall be binding on DSHS only upon signature by DSHS.			
CONTRACTOR SIGNATURE  <i>Sommer Kleweno-Walley</i>		PRINTED NAME AND TITLE Sommer Kleweno-Walley chief Executive Officer	DATE SIGNED 1/24/2022
DSHS SIGNATURE  <i>Alice Hildebrandt</i>		PRINTED NAME AND TITLE Alice Hildebrandt, Contracts Officer DSHS/ESA/Community Services Division	DATE SIGNED 1/25/2022

## DSHS General Terms and Conditions

1. **Definitions.** The words and phrases listed below, as used in this Contract, shall each have the following definitions:
- a. "Central Contracts and Legal Services" means the DSHS central headquarters contracting office, or successor section or office.
  - b. "Confidential Information" or "Data" means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.
  - c. "Contract" or "Agreement" means the entire written agreement between DSHS and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original.
  - d. "CCLS Chief" means the manager, or successor, of Central Contracts and Legal Services or successor section or office.
  - e. "Contractor" means the individual or entity performing services pursuant to this Contract and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.
  - f. "Debarment" means an action taken by a Federal agency or official to exclude a person or business entity from participating in transactions involving certain federal funds.
  - g. "DSHS" or the "Department" means the state of Washington Department of Social and Health Services and its employees and authorized agents.
  - h. "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.
  - i. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.
  - j. "Physically Secure" means that access is restricted through physical means to authorized individuals only.
  - k. "Program Agreement" means an agreement between the Contractor and DSHS containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by DSHS.
  - l. "RCW" means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at <http://apps.leg.wa.gov/rcw/>.

## DSHS General Terms and Conditions

- m. "Regulation" means any federal, state, or local regulation, rule, or ordinance.
  - n. "Secured Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
  - o. "Subcontract" means any separate agreement or contract between the Contractor and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract.
  - p. "Tracking" means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.
  - q. "Trusted Systems" include only the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.
  - r. "WAC" means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at <http://apps.leg.wa.gov/wac/>.
- 2. Amendment.** This Contract may only be modified by a written amendment signed by both parties. Only personnel authorized to bind each of the parties may sign an amendment.
- 3. Assignment.** The Contractor shall not assign this Contract or any Program Agreement to a third party without the prior written consent of DSHS.
- 4. Billing Limitations.**
- a. DSHS shall pay the Contractor only for authorized services provided in accordance with this Contract.
  - b. DSHS shall not pay any claims for payment for services submitted more than twelve (12) months after the calendar month in which the services were performed.
  - c. The Contractor shall not bill and DSHS shall not pay for services performed under this Contract, if the Contractor has charged or will charge another agency of the state of Washington or any other party for the same services.
- 5. Compliance with Applicable Law.** At all times during the term of this Contract, the Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to, nondiscrimination laws and regulations.
- a. **COVID-19 Vaccination Requirement.** Contractor shall abide by the vaccination requirements of Governor Jay Inslee's Proclamation 21-14 and all subsequent amendments. After October 18, 2021 Contractor Staff who are reasonably likely or contractually obligated to engage in work while physically present at a building, facility, jobsite, project site, unit, or other defined area owned,

## DSHS General Terms and Conditions

leased, occupied by, or controlled by a State Agency, an operator of an Educational Setting, or an operator of a Health Care Setting as defined in the Proclamation must be fully vaccinated against COVID-19 unless they have been granted a valid disability or religious accommodation by Contractor. Contractor shall obtain a copy of, or visually observe proof of full vaccination against COVID-19 for all Staff who are subject to the vaccination requirement in the Governor's Order. Contractor shall follow the requirements for granting disability and religious accommodations to Contractor's Staff that apply to State Agencies under the Governor's Order. Contractor and Contractor Staff shall provide proof of such vaccination or accommodation upon request by DSHS. Contractor shall cooperate with any investigation or inquiry DSHS makes into the employer's compliance with these requirements, including by providing information and records upon request, except any information or records that the employer is prohibited by law from disclosing.

### 6. Confidentiality.

- a. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:
  - (1) as provided by law; or,
  - (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.
- b. The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the Confidential Information by:
  - (1) Allowing access only to staff that have an authorized business requirement to view the Confidential Information.
  - (2) Physically Securing any computers, documents, or other media containing the Confidential Information.
  - (3) Ensure the security of Confidential Information transmitted via fax (facsimile) by:
    - (a) Verifying the recipient phone number to prevent accidental transmittal of Confidential Information to unauthorized persons.
    - (b) Communicating with the intended recipient before transmission to ensure that the fax will be received only by an authorized person.
    - (c) Verifying after transmittal that the fax was received by the intended recipient.
  - (4) When transporting six (6) or more records containing Confidential Information, outside a Secured Area, do one or more of the following as appropriate:
    - (a) Use a Trusted System.
    - (b) Encrypt the Confidential Information, including:
      - i. Encrypting email and/or email attachments which contain the Confidential Information.
      - ii. Encrypting Confidential Information when it is stored on portable devices or media,

## DSHS General Terms and Conditions

including but not limited to laptop computers and flash memory devices.

**Note: If the DSHS Data Security Requirements Exhibit is attached to this contract, this item, 6.b.(4), is superseded by the language contained in the Exhibit.**

- (5) Send paper documents containing Confidential Information via a Trusted System.
  - (6) Following the requirements of the DSHS Data Security Requirements Exhibit, if attached to this contract.
  - c. Upon request by DSHS, at the end of the Contract term, or when no longer needed, Confidential Information shall be returned to DSHS or Contractor shall certify in writing that they employed a DSHS approved method to destroy the information. Contractor may obtain information regarding approved destruction methods from the DSHS contact identified on the cover page of this Contract.
  - d. Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Confidential Information requiring special handling (e.g. protected health information) must be destroyed on-site through shredding, pulping, or incineration.
  - e. Notification of Compromise or Potential Compromise. The compromise or potential compromise of Confidential Information must be reported to the DSHS Contact designated on the contract within one (1) business day of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.
- 7. Debarment Certification.** The Contractor, by signature to this Contract, certifies that the Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions (Debarred). The Contractor also agrees to include the above requirement in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor becomes Debarred. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor becomes Debarred during the term hereof.
- 8. Governing Law and Venue.** This Contract shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in Superior Court for Thurston County.
- 9. Independent Contractor.** The parties intend that an independent contractor relationship will be created by this Contract. The Contractor and his or her employees or agents performing under this Contract are not employees or agents of the Department. The Contractor, his or her employees, or agents performing under this Contract will not hold himself/herself out as, nor claim to be, an officer or employee of the Department by reason hereof, nor will the Contractor, his or her employees, or agent make any claim of right, privilege or benefit that would accrue to such officer or employee.
- 10. Inspection.** The Contractor shall, at no cost, provide DSHS and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located. These inspection rights are intended to allow DSHS and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.
- 11. Maintenance of Records.** The Contractor shall maintain records relating to this Contract and the

## DSHS General Terms and Conditions

performance of the services described herein. The records include, but are not limited to, accounting procedures and practices, which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. All records and other material relevant to this Contract shall be retained for six (6) years after expiration or termination of this Contract.

Without agreeing that litigation or claims are legally authorized, if any litigation, claim, or audit is started before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

- 12. Order of Precedence.** In the event of any inconsistency or conflict between the General Terms and Conditions and the Special Terms and Conditions of this Contract or any Program Agreement, the inconsistency or conflict shall be resolved by giving precedence to these General Terms and Conditions. Terms or conditions that are more restrictive, specific, or particular than those contained in the General Terms and Conditions shall not be construed as being inconsistent or in conflict.
- 13. Severability.** If any term or condition of this Contract is held invalid by any court, the remainder of the Contract remains valid and in full force and effect.
- 14. Survivability.** The terms and conditions contained in this Contract or any Program Agreement which, by their sense and context, are intended to survive the expiration or termination of the particular agreement shall survive. Surviving terms include, but are not limited to: Billing Limitations; Confidentiality, Disputes; Indemnification and Hold Harmless, Inspection, Maintenance of Records, Notice of Overpayment, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of Property.
- 15. Contract Renegotiation, Suspension, or Termination Due to Change in Funding.**

If the funds DSHS relied upon to establish this Contract or Program Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, after the effective date of this contract but prior to the normal completion of this Contract or Program Agreement:

- a. At DSHS's discretion, the Contract or Program Agreement may be renegotiated under the revised funding conditions.
- b. At DSHS's discretion, DSHS may give notice to Contractor to suspend performance when DSHS determines that there is reasonable likelihood that the funding insufficiency may be resolved in a timeframe that would allow Contractor's performance to be resumed prior to the normal completion date of this contract.
  - (1) During the period of suspension of performance, each party will inform the other of any conditions that may reasonably affect the potential for resumption of performance.
  - (2) When DSHS determines that the funding insufficiency is resolved, it will give Contractor written notice to resume performance. Upon the receipt of this notice, Contractor will provide written notice to DSHS informing DSHS whether it can resume performance and, if so, the date of resumption. For purposes of this subsection, "written notice" may include email.
  - (3) If the Contractor's proposed resumption date is not acceptable to DSHS and an acceptable date cannot be negotiated, DSHS may terminate the contract by giving written notice to Contractor. The parties agree that the Contract will be terminated retroactive to the date of the notice of suspension. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the retroactive date of termination.

## DSHS General Terms and Conditions

c. DSHS may immediately terminate this Contract by providing written notice to the Contractor. The termination shall be effective on the date specified in the termination notice. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination. No penalty shall accrue to DSHS in the event the termination option in this section is exercised.

**16. Waiver.** Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Contract. Only the CCLS Chief or designee has the authority to waive any term or condition of this Contract on behalf of DSHS.

### Additional General Terms and Conditions – Interlocal Agreements:

**17. Disputes.** Both DSHS and the Contractor (“Parties”) agree to work in good faith to resolve all conflicts at the lowest level possible. However, if the Parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either Party may reduce its description of the dispute in writing, and deliver it to the other Party for consideration. Once received, the assigned managers or designees of each Party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency’s respective operational protocols, to the Secretary of DSHS (“Secretary”) and the Contractor’s Agency Head (“Agency Head”) or their deputies or designated delegates. Both Parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the Secretary and Agency Head.

Upon receipt of the referral and relevant documentation, the Secretary and Agency Head will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Secretary and Agency Head may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Secretary and Agency Head are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

The final decision will be put in writing, and will be signed by both the Secretary and Agency Head. If the Agreement is active at the time of resolution, the Parties will execute an amendment or change order to incorporate the final decision into the Agreement. The decision will be final and binding as to the matter reviewed and the dispute shall be settled in accordance with the terms of the decision.

If the Secretary and Agency Head are unable to come to a mutually acceptable decision, the Parties will request intervention by the Governor, per RCW 43.17.330, in which case the governor shall employ whatever dispute resolution methods that the governor deems appropriate in resolving the dispute.

Both Parties agree that, the existence of a dispute notwithstanding, the Parties will continue without delay to carry out all respective responsibilities under this Agreement that are not affected by the dispute.

**18. Hold Harmless.**

a. The Contractor shall be responsible for and shall hold DSHS harmless from all claims, loss, liability, damages, or fines arising out of or relating to the Contractor’s, or any Subcontractor’s, performance or failure to perform this Agreement, or the acts or omissions of the Contractor or any

## DSHS General Terms and Conditions

Subcontractor. DSHS shall be responsible for and shall hold the Contractor harmless from all claims, loss, liability, damages, or fines arising out of or relating to DSHS' performance or failure to perform this Agreement.

- b. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.

**19. Ownership of Material.** Material created by the Contractor and paid for by DSHS as a part of this Contract shall be owned by DSHS and shall be "work made for hire" as defined by Title 17 USCA, Section 101. This material includes, but is not limited to: books; computer programs; documents; films; pamphlets; reports; sound reproductions; studies; surveys; tapes; and/or training materials. Material which the Contractor uses to perform the Contract but is not created for or paid for by DSHS is owned by the Contractor and is not "work made for hire"; however, DSHS shall have a perpetual license to use this material for DSHS internal purposes at no charge to DSHS, provided that such license shall be limited to the extent which the Contractor has a right to grant such a license.

**20. Subrecipients.**

- a. General. If the Contractor is a subrecipient of federal awards as defined by 2 CFR Part 200 and this Agreement, the Contractor shall:
  - (1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Catalog of Federal Domestic Assistance (CFDA) title and number, award number and year, name of the federal agency, and name of the pass-through entity;
  - (2) Maintain internal controls that provide reasonable assurance that the Contractor is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;
  - (3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;
  - (4) Incorporate 2 CFR Part 200, Subpart F audit requirements into all agreements between the Contractor and its Subcontractors who are subrecipients;
  - (5) Comply with the applicable requirements of 2 CFR Part 200, including any future amendments to 2 CFR Part 200, and any successor or replacement Office of Management and Budget (OMB) Circular or regulation; and
  - (6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to <https://oip.gov/about/offices/ocr.htm> for additional information and access to the aforementioned Federal laws and regulations.)
- b. Single Audit Act Compliance. If the Contractor is a subrecipient and expends \$750,000 or more in federal awards from any and/or all sources in any fiscal year, the Contractor shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Contractor shall:



## DSHS General Terms and Conditions

- (1) Submit to the DSHS contact person the data collection form and reporting package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;
  - (2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a "Summary Schedule of Prior Audit Findings" reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.
- c. Overpayments. If it is determined by DSHS, or during the course of a required audit, that the Contractor has been paid unallowable costs under this or any Program Agreement, DSHS may require the Contractor to reimburse DSHS in accordance with 2 CFR Part 200.

### 21. Termination.

- a. Default. If for any cause, either party fails to fulfill its obligations under this Agreement in a timely and proper manner, or if either party violates any of the terms and conditions contained in this Agreement, then the aggrieved party will give the other party written notice of such failure or violation. The responsible party will be given 15 working days to correct the violation or failure. If the failure or violation is not corrected, this Agreement may be terminated immediately by written notice from the aggrieved party to the other party.
- b. Convenience. Either party may terminate this Interlocal Agreement for any other reason by providing 30 calendar days' written notice to the other party.
- c. Payment for Performance. If this Interlocal Agreement is terminated for any reason, DSHS shall only pay for performance rendered or costs incurred in accordance with the terms of this Agreement and prior to the effective date of termination.

- 22. Treatment of Client Property.** Unless otherwise provided, the Contractor shall ensure that any adult client receiving services from the Contractor has unrestricted access to the client's personal property. The Contractor shall not interfere with any adult client's ownership, possession, or use of the client's property. The Contractor shall provide clients under age eighteen (18) with reasonable access to their personal property that is appropriate to the client's age, development, and needs. Upon termination of the Contract, the Contractor shall immediately release to the client and/or the client's guardian or custodian all of the client's personal property.

## Special Terms and Conditions

1. **Definitions Specific to Special Terms:** The words and phrases listed below, as used in this Contract, shall each have the following definitions:
  - a. "Applicant(s)" means individuals submitting an application, a renewal or reporting a change for benefits or services.
  - b. "Assisting Agency" means community or faith based organizations, tribal, city, or county municipalities who provide trained employees or volunteers to help applicants complete and submit online applications through Washington Connection. These agencies must sign a Data Share Agreement with DSHS and each employee and volunteer of the agency with access to Applicant information must complete a DSHS non-disclosure form. Any reference to Assisting Agency includes the Assisting Agency's employees, agents, officers, subcontractors, third party contractors, volunteers, or directors.
  - c. "Authorized Representative" means someone designated by the Applicant to talk with DSHS about his/her benefits. This individual is authorized to act on the Applicant's behalf for eligibility purposes.
  - d. "Contractor Contact", referenced on page one of this agreement, means the person who handles the day-to-day duties related to this agreement. This person may or may not be the one who signs this agreement on behalf of the Contractor.
  - e. "Data" means the information that is exchanged as described by this Agreement that is specifically protected by law which may impose penalties for wrongful disclosure. This includes protected health information under the HIPAA Privacy Rule.
  - f. "ESA" means Economic Services Administration.
  - g. "SAW" means SecureAccess Washington. SAW is a single sign-on application gateway created by Washington State's Department of Information Services to access government services accessible via the Internet.
  - h. "Washington Connection" means the web-based benefit portal that provides access to a broad array of federal, state and local services and benefits to address basic needs.
  
2. **Purpose** – To allow an Assisting Agency to help Washington residents complete an online application to provide more effective access to available federal, state and local services through the Washington Connection benefit portal and carry out other activities designed to help them maintain eligibility. This agreement also includes contractors that submit paper applications to DSHS.
  
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 set forth below:
  - a. The Assisting Agency listed on page one of this Data Share Agreement is the Contractor, and DSHS is the Data Provider in this agreement. In exchange for the receipt of information, the Contractor agrees to abide by the terms and conditions in this agreement.
    - (1) Anyone at the Contractor agency with access to Data will be required to read and complete a non-disclosure agreement annually. The Contractor must maintain these forms and make them available for inspection.
    - (2) When Contractors use Washington Connection for applications, DSHS will work with them to:
      - (a) Establish access to the DSHS Washington Connection and online application.

## Special Terms and Conditions

- (b) Establish a Washington Connection SAW account with either an Employee or a Supervisor access level:
  - i. *Employee Access* allows the individual to view, edit and submit applications when the employee has provided direct access with the application through Washington Connection as part of their work at the Assisting Agency.
  - ii. *Supervisor Access* includes all functions of the Employee Access plus the ability to: view, edit and submit all applications associated with employees assigned to the supervisor in the Washington Connection profile; add, modify, and delete employees; reassign applications between employees under the same supervisor, and request a summary page of all application status (submitted or incomplete) associated with the Assisting Agency.

### (3) Consent Form and Use Limitation

- (a) The Contractor must obtain a Consent form via Washington Connection with an e-signature from the Applicant before accessing any Applicant Information. The Contractor must keep any written DSHS consent form obtained from the Applicant onsite and provide them for inspection upon request.
  - i. DSHS and the Contractor may need to share additional information to provide services, but at no time should the Consent be interpreted to:
    - (A) Designate the Contractor as an “Authorized Representative”
    - (B) Allow DSHS to share Applicant information not needed for the purposes under this agreement
    - (C) Allow DSHS to disclose documents or information from the Applicant’s files or records for other purposes outside the scope of this agreement

### b. Description of Data

Data is limited to:

- (a) application data
- (b) defined display of household benefit information available through the Washington Connection query system

### c. Data Access or Transfer

- (1) If applications are received through Washington Connection and the Applicant has indicated consent to share application data, a Contractor may view and print applications, reviews and change of circumstances forms saved or submitted through Washington Connection for 90 calendar days from the last activity day. Application statuses, “submitted” or “not submitted”, are also available for 90 calendar days from the last activity day. Contractors submitting paper applications have no ability to view them online.
- (2) If the correct client identification number or negative client identification number (includes a minus sign before the number) is entered into the Washington Connection query system, the successful query will result in the display of the following information for the listed head of

## Special Terms and Conditions

household if that person is not registered in the Address Confidentiality Program (ACP):

(a) Application Status

A = approved

P = Pending

D = Denied

M = Pending Spenddown (with base period and remaining amount)

(b) Eligibility history (3 month rolling) from DSHS and/or HCA

(c) Benefit amount for cash and food assistance programs only

(d) Number in the household associated with cash, food and medical benefits

(e) Benefit end date for each certification period (cash, food, medical, and childcare)

(f) Child's name receiving childcare services

(g) Childcare provider name for each child

(h) Copayment amount for each child

(i) Gross earned income

(3) Requirements for Access

(a) Access to Data shall be limited to staff (including employees and volunteers) whose duties specifically require access to such Data in the performance of their assigned duties. Prior to making Data available to its staff, Contractor shall notify all such staff of the Use and Disclosure requirements.

(b) All staff accessing the data shall sign a Nondisclosure of Confidential Information form, or its replacement, each year and agree to adhere to the use and disclosure requirements. The signed, original form and a regularly updated list of staff with access to the Data shall be maintained by the Contractor and submitted to the Data Provider upon request.

(c) The Contractor must remind staff annually of nondisclosure requirements and make available to DSHS upon request evidence that they have reminded all staff with access to Applicant data of the limitations, use or publishing of data.

(d) The Contractor must immediately notify the DSHS contact person listed on page one when any staff with access to the Data is terminated from employment or when his or her job duties no longer require access to Data.

d. Limitations on Use of Data

If the Data and analyses generated by the Contractor contain Confidential Information about DSHS Applicants, 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.

## Special Terms and Conditions

### 4. Data Security

- a. Violations of the Nondisclosure provisions of this agreement may result in criminal or civil penalties. Violation is a gross misdemeanor under RCW 7A.04.060, punishable by imprisonment of not more than one year and/or a fine not to exceed five thousand dollars. Sanctions also may apply under other state and federal law, including civil and criminal penalties for violations of the HIPAA Privacy and Security rules.
- b. The Contractor shall take reasonable precautions to secure against unauthorized physical and electronic access to Applicant Information. Data shall be protected in a manner that prevents unauthorized persons, including the general public, from access by computer, remote terminal, or other means.
- c. Contractor shall notify the DSHS contact designated on the contract verbally and in writing of the compromise or suspected compromise of the security or privacy of data within one (1) business day and to work with DSHS to assess additional steps to be taken. The Contractor shall be responsible to comply with legal requirements, provide notification of clients as needed and for any costs associated mitigating the breach.

### 5. Insurance.

The Contractor shall at all times comply with the following insurance requirements.

#### a. Professional Liability Insurance (PL)

If the Contractor provides professional services, either directly or indirectly, the Contractor shall maintain Professional Liability Insurance, including coverage for losses caused by errors and omissions, with the following minimum limits: Each Occurrence - \$1,000,000; General Aggregate - \$2,000,000.

#### b. Evidence of Coverage

The Contractor shall submit Certificates of Insurance to DSHS for each coverage required of the Contractor under the Contract. The Contractor shall submit the Certificates of Coverage to Central Contract Services, Post Office Box 45811, Olympia, Washington 98504-5811, or via email to [CCSContractsCounsel@dshs.wa.gov](mailto:CCSContractsCounsel@dshs.wa.gov). Each Certificate of Insurance shall be executed by a duly authorized representative of each insurer, showing compliance with the insurance requirements specified in this Contract. The Certificate of Insurance for each required policy shall reference the DSHS Contract Number for the Contract. Material Changes

The insurer shall give DSHS Central Contract Services forty-five (45) days advance notice of cancellation or non-renewal. If cancellation is due to non-payment of premium, the insurer shall give DSHS Central Contract Services 10 days advance notice of cancellation.

#### c. General

By requiring insurance, the State of Washington and DSHS do not represent that the coverage and limits specified will be adequate to protect the Contractor. Such coverage and limits shall not be construed to relieve the Contractor from liability in excess of the required coverage and limits and shall not limit the Contractor's liability under the indemnities and reimbursements granted to the State and DSHS in this Contract. All insurance provided in compliance with this Contract shall be

## Special Terms and Conditions

primary as to any other insurance or self-insurance programs afforded to or maintained by the State. The Contractor waives all rights against the State of Washington and DSHS for the recovery of damages to the extent they are covered by insurance.

### 6. Inspection.

- a. These inspection rights supersede the general terms and conditions of this agreement. The Contractor shall, at no cost, provide DSHS and the Community Services Division Washington Connection Community Partnership Program with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located, as they relate to this agreement. These inspection rights are intended to allow the Program to monitor, audit, and evaluate the Contractor's compliance regarding these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.
- b. The Contractor will receive a self-assessment via email no less than once every four (4) years. The self-assessment and other supporting documents will be provided by the DSHS contact listed on page one (1,) or their designee. The self-assessment is meant to ensure compliance with:
  - (a) Annual review, signing, and retention of Nondisclosure Agreements;
  - (b) Proof of current liability insurance;
  - (c) Review of active Washington Connection Partner Account users, access, and privileges;
  - (d) Confidentiality and Nondisclosure through Client Search and internal consent
- c. The Contractor shall complete and return the self-assessment within the timeframe provided by the DSHS contact listed on page one (1,) or their designee (not to exceed 30 calendar days.)

### 7. Confidentiality and Nondisclosure

- a. Both parties may use Personal Information and other information or Data gained by reason of this Agreement only for the purposes of this Agreement.
- b. The data to be shared under this agreement is confidential in nature and is subject to state and federal confidentiality requirement that bind the Contractor, its employees, and its subcontractors to protect the confidentiality of the personal information contained in ESA data. Contractors may use personal data and other data gained by reason of this agreement only for the purpose of this agreement.
- c. The Contractor shall maintain the confidentiality of personal data in accordance with state and federal laws, and shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements, including restrictions on re-disclosure.
- d. Neither party shall 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 Agreement.

### 8. Consideration

There is no cost to either party as each will pay for its own costs to perform this contract.

## Special Terms and Conditions

### 9. Payment

- a. The Contractor will receive the information provided under this agreement at no charge. Each party shall be responsible for any expenses incurred in providing or receiving information.
- b. The Contractor is responsible for any costs associated with accessing Applicant data. This includes any costs for hardware/software upgrades, and costs to improve any systems or processors that will enable the Contractor to access the data.

### 10. Compensation

- a. The Contractor shall not charge the applicant for services or time rendered while assisting with application, renewal, or reporting changes to the Department of Social and Health Services
- b. If the applicant requests additional services not included herewith, these services may be subject to fees and should be authorized in writing and signed by the applicant and Contractor under the auspice of separate agreement.

### 11. Disputes

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 Contractors name, address, and Contract number, and be mailed to the address listed below within 30 calendar days after the party could reasonably be expected to have knowledge of the issue in dispute.

DSHS/Community Services Division  
PO Box 45470  
Olympia, WA 98504-5470  
Attn. Contracts Unit

### 12. Contractor Information

The Contractor shall forward to the DSHS Contact person named on page one (1) of this contract (or successor) within ten (10) working days, any information concerning the Contractor's contact person. This would be the person who handles the daily operations regarding this contract. Changes include a change of contractor business name, contractor contact name, address, telephone number, fax number, e-mail address, business status and/or names of staff who are current state employees.

## 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](http://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:

<b>Data stored on:</b>	<b>Will be destroyed by:</b>
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](mailto: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 subcontractor must be submitted to the DSHS Contact specified for this contract for review and approval.