



DATASHARE AGREEMENT Washington Connection

DSHS Contract Number:
1392-72387
Resulting From Procurement Number:

This Contract is between the state of Washington Department of Social and Health Services (DSHS) and the Contractor identified below, and is governed by chapter 39.29 RCW.

Program Contract Number:

Contractor Contract Number:

CONTRACTOR NAME Kittitas County		CONTRACTOR doing business as (DBA) Kittitas County Health Department	
CONTRACTOR ADDRESS 507 North Nanum Street, Suite 102 Ellensburg, WA 98926-		WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI) 192-002-673	DSHS INDEX NUMBER 1225
CONTRACTOR CONTACT Mark Larson	CONTRACTOR TELEPHONE (509) 962-7515	CONTRACTOR FAX (509) 962-7581	CONTRACTOR E-MAIL ADDRESS mark.larson@co.kittitas.wa.us
DSHS ADMINISTRATION Economic Services Administration	DSHS DIVISION Community Services Division		DSHS CONTRACT CODE 3067DS-92
DSHS CONTACT NAME AND TITLE Stephanie Hill Program Administrator		DSHS CONTACT ADDRESS PO Box 45440 Olympia, WA 98504-5440	
DSHS CONTACT TELEPHONE (360) 725-4666	DSHS CONTACT FAX (360) 725-4905		DSHS CONTACT E-MAIL ADDRESS hillsr@dshs.wa.gov
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT? No		CFDA NUMBER(S)	
CONTRACT START DATE 04/22/2013	CONTRACT END DATE 04/30/2018		CONTRACT MAXIMUM AMOUNT \$0.00
EXHIBITS. The following Exhibits are attached and are incorporated into this Contract by reference: <input checked="" type="checkbox"/> Exhibits (specify): Exhibit A – Data Security Requirements <input type="checkbox"/> 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.			
CONTRACTOR SIGNATURE 		PRINTED NAME AND TITLE Robin H. Read, Administrator	DATE SIGNED 4/22/13
DSHS SIGNATURE 		PRINTED NAME AND TITLE Ramona Bushnell, Contracts Officer DSHS/ESA/Community Services Division	DATE SIGNED 4-22-13

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 Contract 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. "Contracts Administrator" means the manager, or successor, of Central Contract 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 128 bits.
 - 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/>.
 - 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

General Terms and Conditions

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.

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,

General Terms and Conditions

- (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, 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.

General Terms and Conditions

- 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 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;

General Terms and Conditions

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. **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, 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.
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 DSHS Contracts Administrator or designee has the authority to waive any term or condition of this Contract on behalf of DSHS.

Additional General Terms and Conditions – Datashare Agreements:

17. **Advance Payment.** DSHS shall not make any payments in advance or anticipation of the delivery of services to be provided pursuant to this Contract.
18. **Construction.** The language in this Contract shall be interpreted as to its fair meaning and not strictly for or against any party. Any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in interpreting this Contract.
19. **Indemnification and Hold Harmless.**
 - a. The Contractor shall be responsible for and shall indemnify, defend, and hold DSHS harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines, of whatsoever kind of nature, arising out of or relating to a) the Contractor's or any Subcontractor's performance or failure to perform this Contract, or b) the acts or omissions of the Contractor or any Subcontractor.
 - b. The Contractor's duty to indemnify, defend, and hold DSHS harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include DSHS' personnel-related costs, reasonable attorney's fees, court costs, and all related expenses.
 - c. 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.
 - d. Nothing in this term shall be construed as a modification or limitation on the Contractor's obligation to procure insurance in accordance with this Contract or the scope of said insurance.
20. **Industrial Insurance Coverage.** The Contractor shall comply with the provisions of Title 51 RCW, Industrial Insurance. If the Contractor fails to provide industrial insurance coverage or fails to pay premiums or penalties on behalf of its employees, as may be required by law, Agency may collect from the Contractor the full amount payable to the Industrial Insurance accident fund. The Agency may deduct the amount owed by the Contractor to the accident fund from the amount payable to the Contractor by the Agency under this contract, and transmit the deducted amount to the Department of Labor and Industries, (L&I) Division of Insurance Services. This provision does not waive any of L&I's rights to collect from the Contractor.
21. **Notice of Overpayment.** If the Contractor receives a vendor overpayment notice or a letter communicating the existence of an overpayment from DSHS, the Contractor may protest the

General Terms and Conditions

overpayment determination by requesting an adjudicative proceeding. The Contractor's request for an adjudicative proceeding must:

- a. Be *received* by the Office of Financial Recovery (OFR) at Post Office Box 9501, Olympia, Washington 98507-9501, within twenty-eight (28) calendar days of service of the notice;
- b. Be sent by certified mail (return receipt) or other manner that proves OFR received the request;
- c. Include a statement as to why the Contractor thinks the notice is incorrect; and
- d. Include a copy of the overpayment notice.

Timely and complete requests will be scheduled for a formal hearing by the Office of Administrative Hearings. The Contractor may be offered a pre-hearing or alternative dispute resolution conference in an attempt to resolve the overpayment dispute prior to the hearing.

Failure to provide OFR with a written request for a hearing within twenty-eight (28) days of service of a vendor overpayment notice or other overpayment letter will result in an overpayment debt against the Contractor. DSHS may charge the Contractor interest and any costs associated with the collection of this overpayment. DSHS may collect an overpayment debt through lien, foreclosure, seizure and sale of the Contractor's real or personal property; order to withhold and deliver; or any other collection action available to DSHS to satisfy the overpayment debt.

22. **DES Filing Requirement.** Under RCW 39.26, sole source contracts and amendments must be filed with the State of Washington Department of Enterprise Services (DES). If this Contract is one that must be filed, it shall not be effective nor shall work commence or payment be made until it has been approved by DES. In the event DES fails to approve the Contract or any amendment hereto, the Contract or amendment shall be null and void.
23. **Subcontracting.** Except as otherwise provided in this Contract, the Contractor shall not Subcontract any of the contracted services without the prior written approval of DSHS. Contractor is responsible to ensure that all terms, conditions, assurances and certifications set forth in this Contract are included in any and all Subcontracts. Any failure of Contractor or its Subcontractors to perform the obligations of this Contract shall not discharge the Contractor from its obligations hereunder or diminish DSHS' rights or remedies available under this Contract.
24. **Termination for Convenience.** DSHS may terminate this Contract in whole or in part when it is in the best interest of DSHS by giving the Contractor at least thirty (30) calendar days' written notice.
25. **Termination for Default.** The Contracts Administrator may immediately terminate this Contract for default, in whole or in part, by written notice to the Contractor if DSHS has a reasonable basis to believe that the Contractor has:
 - a. Failed to meet or maintain any requirement for contracting with DSHS;
 - b. Failed to protect the health or safety of any DSHS client;
 - c. Failed to perform under, or otherwise breached, any term or condition of this Contract; and/or
 - d. Violated any applicable law or regulation.
 - e. If it is later determined that the Contractor was not in default, the termination shall be considered a termination for convenience.

General Terms and Conditions

- 26. Termination or Expiration Procedure.** The following terms and conditions apply upon Contract termination or expiration:
- a. The Contractor shall cease to perform any services required by this Contract as of the effective date of termination or expiration.
 - b. If the Contract is terminated, the Contractor shall comply with all instructions contained in the termination notice.
 - c. The Contractor shall immediately deliver to the DSHS contact named on page one of this Contract, or to his or her successor, all DSHS property in the Contractor's possession. The Contractor grants DSHS the right to enter upon the Contractor's premises for the sole purpose of recovering any DSHS property that the Contractor fails to return within ten (10) calendar days of the effective date of termination or expiration of this Contract. Upon failure to return DSHS property within ten (10) calendar days, the Contractor shall be charged with all reasonable costs of recovery, including transportation.
 - d. DSHS shall be liable only for payment required under the terms of this Contract for service rendered up to the effective date of termination or expiration.
 - e. DSHS may withhold a sum from the final payment to the Contractor that DSHS determines necessary to protect DSHS against loss or additional liability.
 - f. The rights and remedies provided to DSHS in this Section are in addition to any other rights and remedies provided at law, in equity, and/or under this Contract, including consequential and incidental damages.
- 27. Treatment of Property.** All property purchased or furnished by DSHS for use by the Contractor during this Contract term shall remain with DSHS. Title to all property purchased or furnished by the Contractor for which the Contractor is entitled to reimbursement by DSHS under this Contract shall pass to and vest in DSHS. The Contractor shall protect, maintain, and insure all DSHS property in its possession against loss or damage and shall return DSHS property to DSHS upon Contract termination or expiration.
- 28. Taxes.**
- a. Where required by statute or regulation, Contractor shall pay for and maintain in current status all taxes that are necessary for Contract performance. DSHS will pay sales or use taxes, if any, imposed on the services and materials acquired hereunder. Contractor must pay all other taxes including without limitation Washington Business and Occupation Tax, other taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. DSHS, as an agency of Washington State government, is exempt from property tax.
 - b. Contractor shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this Contract in accordance with the requirements of Title 82 RCW and Title 458 WAC. Out-of-state Contractors must contact the Department of Revenue to determine whether they meet criteria to register and establish an account with the Department of Revenue. Refer to WAC 458-20-93 and call the Department of Revenue at 800-647-7706 for additional information. When out-of-state Contractors are not required to collect and remit sales tax, DSHS shall be responsible for paying use tax, if applicable, directly to the Department of Revenue.
 - c. All payments accrued on account of payroll taxes, unemployment contributions, any other taxes,

General Terms and Conditions

insurance, or other expenses for Contractor or Contractor's staff shall be Contractor's sole responsibility.

29. HIPAA Compliance.

a. Definitions.

- (1) "Business Associate" means the "Contractor", as used in this Contract and as defined in 45 CFR 160.103, who performs or assists in the performance of an activity for or on behalf of the Covered Entity that involves the use or disclosure of client protected health information (PHI). Any reference to Business Associate in this Contract includes Business Associate's employees, agents, officers, subcontractors, third party contractors, volunteers, or directors.
- (2) "Covered Entity" means DSHS, a Covered Entity as defined in 45 CFR 160.103.
- (3) "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or used in whole or part by or for the Covered Entity to make decisions about Individuals.
- (4) "Electronic Protected Health Information (EPHI)" means protected health information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 162.103.
- (5) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.
- (6) "Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- (7) "Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.
- (8) "Protected Health Information (PHI)" means information created or received by Business Associate from or on behalf of Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or past, present, or future payment for provision of health care to an Individual. 45 CFR 160.103. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. 45 CFR 160.103. PHI is information transmitted or held in any form or medium. 45 CFR 160.103. PHI does not include education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USCA 1232g(a)(4)(B)(iv).
- (9) "Use" includes the sharing, employment, application, utilization, examination, analysis, canonization or commingling of PHI with other information.

b. Compliance. Business Associate shall perform all Contract duties, activities and tasks in compliance with HIPAA and its attendant regulations as promulgated by the U.S. Department of Health and Human Services, the Center for Medicare and Medicaid Services, the Office of the Inspector General, and the Office of Civil Rights.

c. Use and Disclosure of PHI. Business Associate is limited to the following permitted and required

General Terms and Conditions

uses or disclosures of DSHS client PHI:

- (1) **Duty to Protect DSHS Client PHI.** Business Associate shall protect PHI from, and shall establish appropriate safeguards to prevent, the unauthorized disclosure of PHI in accordance with the terms and conditions of this Contract and state and federal law, including any regulations governing the security of PHI and the transmission, storage or maintenance of electronic data that contains PHI, for as long as the PHI is within its possession and control, even after the termination or expiration of this Contract.
- (2) **Return of DSHS Client PHI.** Business Associate shall, within ten (10) working days of termination or expiration of this Contract, in accordance with Contract Termination and Expiration Procedures, and at the discretion of Covered Entity, either return or destroy all PHI, including PHI in possession of third parties under contract to Business Associate. If return or destruction is infeasible, Business Associate shall protect such PHI and limit its further use and disclosure to those purposes that make return or destruction infeasible for as long as the PHI is within the Business Associate's possession and control, even after the termination or expiration of this Contract.
- (3) **Minimum Necessary Standard.** Business Associate shall apply the HIPAA Minimum Necessary standard to any use or disclosure of DSHS client PHI necessary to achieve the purposes of this Contract. See, 45 CFR 164.514 (d)(2) through (d)(5).
- (4) **Disclosure as Part of the Provision of Services.** Business Associate shall only use or disclose DSHS client PHI as required to perform the services specified in this Contract or as required by law, and shall not use or disclose such PHI in any manner inconsistent with the use and disclosure restrictions placed on the Covered Entity by HIPAA.
- (5) **Impermissible Use or Disclosure of DSHS client PHI.** Business Associate shall report to DSHS in writing all uses or disclosures of PHI not provided for by this Contract within one (1) working day of becoming aware of the unauthorized use or disclosure of the PHI. Upon request by DSHS, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible use or disclosure.
- (6) **Failure to Cure.** If DSHS learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this Contract and reasonable steps by DSHS do not end the violation, DSHS shall terminate this Contract. If termination is not feasible, DSHS will report the problem to the Secretary of the federal Department of Health and Human Services (Secretary).
- (7) **DSHS Notice of Requests for Disclosure.** DSHS will notify Business Associate when DSHS client PHI is requested from DSHS that has been previously provided to Business Associate by DSHS. The parties will jointly determine whether Business Associate has received a duplicate request or if Business Associate has the original or sole copy of the PHI.
- (8) **Consent to Audit.** Business Associate shall give reasonable access to DSHS client PHI, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of DSHS, to the Secretary and/or to DSHS for use in determining DSHS' compliance with HIPAA privacy requirements.

d. Individual Rights.

(1) Accounting of Disclosures.

- (a) Business Associate shall document all disclosures of DSHS client PHI and information

General Terms and Conditions

related to such disclosures.

- (b) Within ten (10) working days of a request from DSHS, Business Associate shall make available to DSHS the information in Business Associate's possession that is necessary for DSHS to respond in a timely manner to a request for an accounting of disclosures of DSHS client PHI. See, 45 C.F.R. 164.504 and 164.528.
 - (c) At the request of DSHS, Business Associate shall respond, in a timely manner and in accordance with HIPAA, to requests by Individuals for an accounting of disclosures of PHI.
 - (d) If any Individual asks Business Associate for an accounting of disclosures of DSHS client PHI, or for access to or amendment of PHI in a Designated Record Set, Business Associate shall within ten (10) working days forward the request to DSHS for response.
 - (e) Business Associate's record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested except for disclosures that occurred prior to the HIPAA compliance date for the Covered Entity.
- (2) Amendment. If DSHS amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and DSHS has previously provided the PHI or record that is the subject of the amendment to Business Associate, then DSHS will inform Business Associate of the amendment pursuant to 45 CFR 164.526 (c)(3).
- e. Third Party Agreements. Business Associate shall enter into a written contract, that contains the same terms, restrictions, and conditions as the HIPAA and HITECH Compliance provisions in this Contract, with any agent, subcontractor, independent contractor, or other third party that has access to the DSHS client PHI accessible to Business Associate under the terms of this Contract.

30. HITECH Compliance.

- a. The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") was adopted as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act and its implementing regulations impose new requirements on Business Associates with respect to privacy, security, and breach notification. These provisions of the HITECH Act and the regulations applicable to Business Associates are collectively referred to as the "HITECH Business Associate Provisions." The Contractor acknowledges and agrees that to the extent it is functioning as a Business Associate of DSHS, the Contractor will comply with the HITECH Business Associate Provisions and with the obligations of a Business Associate, as prescribed by HIPAA and the HITECH Act.
- b. Breach Notification.
 - (1) In the event of a breach of unsecured protected health information (PHI) or disclosure that compromises the privacy or integrity of PHI obtained from DSHS or involving DSHS clients, Business Associate will take all measures required by state or federal law. Business Associate will provide Covered Entity with a copy of its investigation results and other information requested by Covered Entity. Business Associate will report all PHI breaches to the Department of Health and Human Services, Office of Civil Rights (OCR) as required by 45 CFR Parts 160 and 164, and will also provide notification to the DSHS Privacy Officer that a report has been filed with OCR.
 - (2) Business Associate will notify Covered Entity within one (1) business day by telephone and in writing of any acquisition, access, use or disclosure of PHI and/or EPHI not allowed by the

General Terms and Conditions

provisions of this Agreement of which it becomes aware, and of any instance where the PHI is subpoenaed, copied or removed by anyone except an authorized representative of Covered Entity or the Business Associate. 45 CFR §§164.304, 164.314 (a)(2)(C), 164.504(e)(2)(ii)(C), and 164.400-414.

- (3) Business Associate will notify the DSHS Privacy Officer within one (1) business day by telephone or e-mail of any potential breach of security or privacy. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the breach, to include the following: date and time of the breach, medium that contained the PHI, origination and destination of PHI, Business Associate unit and personnel associated with the breach, detailed description of PHI, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible for the mitigation. Business Associate will address communications to:

DSHS Privacy Officer
Washington State Department of Social and Health Services
1115 Washington Street SE
PO Box 45135
Olympia, WA 98504-5135
Telephone: 360-902-8278
Fax: 360-902-7855
E-mail: DSHSPrivacyOffcer@dshs.wa.gov

- (4) If Covered Entity determines that Business Associate or its agent(s) is responsible for a breach of unsecured PHI:
- (a) necessitating notification of Individuals under 45 CFR § 164.404, Business Associate bears the responsibility and costs for notifying the affected Individuals and receiving and responding to those Individuals' questions or requests for additional information;
 - (b) necessitating notification of the media under 45 CFR § 164.406, Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;
 - (c) necessitating notification of the Department of Health and Human Services (DHHS) Secretary under 45 CFR § 164.408, Business Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and
 - (d) Covered Entity will take appropriate remedial measures up to termination of this contract.

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. "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.
 - e. "ESA" means Economic Services Administration.
 - f. "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.
 - g. "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.
 - (b) Establish a Washington Connection SAW account with either an Employee or a Supervisor access level:

Special Terms and Conditions

- 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 information 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 household if that person is not registered in the Address Confidentiality Program (ACP):
 - (a) Application Status

Special Terms and Conditions

A = approved

P = Pending

D = Denied

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

- (b) Eligibility history (12 month rolling) from DSHS and/or HCA
- (c) Benefit amount for cash and food assistance programs only
- (d) Number in the household associated with each program receiving benefits
- (e) Benefit end date for each certification period

(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.

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 74.04.060, 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.

Special Terms and Conditions

- 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. 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. The Contractor agrees to keep Applicant information according to DSHS policy and procedures: <http://asd.dshs.wa.gov/rpau/rpau-adminpolicy.htm>.
 - (1) 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 or by the prior written consent of the other party.

6. Consideration

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

7. 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.

Special Terms and Conditions

8. 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

9. Interpretation

Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule, the Electronic Transactions Standards, or any other requirement under HIPAA.

10. Property Rights

All PHI will be and remain the exclusive property of Covered Entity. Business Associate agrees that it acquires no title or rights to the PHI, including any de-identified information, as a result of this Agreement.

Special Terms and Conditions

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. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access DSHS Confidential Information.
 - b. "Hardened Password" means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.
 - c. "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. **Data Transport.** When transporting DSHS Confidential Information electronically, including via email, the Data will be protected by:
 - a. Transporting the Data within the (State Governmental Network) SGN or Contractor's internal network, or;
 - b. Encrypting any Data that will be in transit outside the SGN or Contractor's internal network. This includes transit over the public Internet.
3. **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.** 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.** 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 Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 5. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured 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 Secured Area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. 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.

Special Terms and Conditions

- 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 Secured 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 Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.
- 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 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 with a key length of at least 128 bits
 - (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.

Physically Secure the portable device(s) and/or media by

 - (d) Keeping them in locked storage when not in use
 - (e) Using check-in/check-out procedures when they are shared, and
 - (f) Taking frequent inventories
 - (2) When being transported outside of a Secured Area, portable devices and media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data.
 - (3) Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.

Special Terms and Conditions

- (4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

h. Data stored for backup purposes.

- (1) DSHS data 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 in Section 5. Data Disposition
- (2) DSHS 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 in Section 5. Data Disposition.

4. 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.
- b. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,
- c. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
- d. DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
- e. 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.
- f. When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.
- g. 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.

5. **Data Disposition.** When the contracted work has been completed or when no longer needed, except as noted in 4.b above, 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	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or
Removable media (e.g. floppies, USB flash drives,	

Special Terms and Conditions

portable hard disks) excluding optical discs	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

6. **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.
7. **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.