

**Exhibit D – Sample Contract – Aging, Blind or Disabled (ABD) Medical Evidence Reviews
RFQ 1436-522**

 <p>PERSONAL SERVICE CONTRACT Aged, Blind or Disabled (ABD) Program Medical Evidence Reviews</p>		DSHS Contract Number:	
<p>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.</p>		Program Contract Number: Contractor Contract Number:	
CONTRACTOR NAME		CONTRACTOR doing business as (DBA)	
CONTRACTOR ADDRESS		WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)	DSHS INDEX NUMBER
CONTRACTOR CONTACT	CONTRACTOR TELEPHONE	CONTRACTOR FAX	CONTRACTOR E-MAIL ADDRESS
DSHS ADMINISTRATION	DSHS DIVISION	DSHS CONTRACT CODE 3043PS-35	
DSHS CONTACT NAME AND TITLE		DSHS CONTACT ADDRESS	
DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL ADDRESS	
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT?		CFDA NUMBER(S)	
CONTRACT START DATE	CONTRACT END DATE	CONTRACT MAXIMUM AMOUNT	
EXHIBITS. The following Exhibits are attached and are incorporated into this Contract by reference: <input checked="" type="checkbox"/> Data Security: Exhibit A – Data Security Requirements <input type="checkbox"/> Exhibits (specify):			
<p>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.</p>			
CONTRACTOR SIGNATURE		PRINTED NAME AND TITLE	DATE SIGNED
<p>Draft - Please Do Not Sign</p>			
DSHS SIGNATURE		PRINTED NAME AND TITLE	DATE SIGNED
<p>Draft - Please Do Not Sign</p>		Caleb Clark, Contracts Officer DSHS/ESA-Community Services Division	

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 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.

DSHS General Terms and Conditions

- 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.
- 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:

DSHS General Terms and Conditions

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

DSHS General Terms and Conditions

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 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.

DSHS General Terms and Conditions

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.
- 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.

DSHS General Terms and Conditions

Additional General Terms and Conditions – Personal Service Contracts:

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 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.

DSHS General Terms and Conditions

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 the tenth (10th) working day following the date of filing subject to DES approval. 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. 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,

DSHS General Terms and Conditions

Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to www.ojp.usdoj.gov/ocr/ 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:
 - (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.

25. 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.

26. Termination for Default. The CCLS Chief 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.

27. 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)

DSHS General Terms and Conditions

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.

28. 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.

29. 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 458-20-101 (Tax registration and tax reporting) 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, insurance, or other expenses for Contractor or Contractor's staff shall be Contractor's sole responsibility.

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. "ABD" means the Aged, Blind, or Disabled state-funded cash assistance program administered by CSD.
 - b. "Business Day" means Monday through Friday excluding state holidays. A Business Day starts at 12:00 a.m. (midnight) and ends at 11:59 p.m.
 - c. "Client" means a person applying for or receiving ABD or HEN Referral benefits.
 - d. "Client Identification Number" means a unique nine-digit number assigned by DSHS to each Client.
 - e. "CSD" means the Community Services Division of the Economic Services Administration (ESA) within DSHS.
 - f. "CSO" means a DSHS Community Services Office within the CSD.
 - g. "Data" means the information that is disclosed or exchanged as described by this Contract.
 - h. "Disability Specialist" means the trained DSHS employee responsible for determining eligibility for ABD cash assistance.
 - i. "DSHS Contact" means the DSHS Contact listed on page 1 of this Contract, or their designee.
 - j. "DDDS" means the Division of Disability Determination Services of the Economic Services Administration (ESA) within DSHS.
 - k. "Duration" means the number of months the impairment is expected to persist with available treatment.
 - l. "Functional Limitation" means the impact of impairment on the ability to perform basic work activities in a routine job setting, including the areas of cognitive and social functioning outlined in WAC 388-449-0020, and the exertional limitations, functional physical capacity, non-exertional physical limitations, and functional limitations defined in WAC 388-449-0030.
 - m. "HEN Referral" means the Housing and Essential Needs Referral program administered by CSD.
 - n. "Medical Evidence" means clinical findings from an examination or interview, and supporting documentation, including testing.
 - o. "Onset Date" means the date the Client's medical or mental health condition began to have a significant impact on one or more basic work activities as defined in WAC 388-449-0001
 - p. "Pending Disciplinary Action" means a statement of charges filed with the Washington State Department of Health (DOH) or any Division or Administration of DSHS. This action means DOH or DSHS has ordered the Contractor to suspend or discontinue services.
 - q. "Portable Devices" means electronic devices to include, but 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

- r. "Portable Media" means media to include, but not limited to: optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, removable or external hard disk drives), or flash media (e.g. Compact Flash, SD, MMC).
- s. "Properly Completed Invoice" means the Contractor has entered all information accurately in the billing documentation provided by or as instructed by DSHS.
- t. "Referral" means sending medical evidence to the Contractor for review using a web-based application or secure email.
- u. "Severity" has the meaning defined in WAC 388-449-0035, 388-449-0040, 388-449-0045 and WAC 388-449-0050.
- v. "Written Notice" means a letter or memorandum on paper, or a message sent electronically via secure e-mail. DSHS has discretion over which medium is used to send the Written Notice.

2. Purpose

The purpose of this Contract is for the Contractor to use their diagnostic and clinical expertise to review a client's medical evidence and DSHS's assessment of the following: diagnosis, severity, functional limitations, duration, onset date, and information regarding the impact(s) of a substance use disorder.

3. Qualifications and Licensing/Credentialing Requirements

a. Qualification Requirements. The Contractor must:

- (1) Be a health professional licensed in Washington State or the state where the services are performed. The following health professionals may perform work under this contract:
 - (a) Physician;
 - (b) Psychiatrist;
 - (c) Psychologist;
 - (d) Advanced registered nurse practitioner (ARNP) for impairments within their licensed scope of practice;
 - (e) Physician assistant (PA) for impairments within their licensed scope of practice.
- (2) Have no pending or active disciplinary actions or licensure sanctions.
- (3) Submit an application packet containing the Exhibits provided under the Request for Qualifications (RFQ) #1436-522: ESA Medical and Psychological Services. Should the Contractor need access to this information, they should contact the DSHS Contact on Page 1 of this Contract.
- (4) Provided a copy of their Curriculum Vitae to the DSHS Contact in order to confirm the Contractor has the requisite training and experience to perform services.

b. Experience.

The Contractor must have:

Special Terms and Conditions

- (1) At least one (1) year of practice in Clinical or Forensic psychology; or
- (2) At least one (1) year of experience evaluating work-related impairments; or
- (3) At least six (6) months experience working as a:
 - (a) Medical Consultant for DDDS.

c. Maintenance of Licensing Requirements.

- (1) The Contractor shall immediately cease providing services when the Contractor receives any notice that:
 - (a) Their license to practice has been suspended or expired;
 - (b) A disciplinary or sanction has been filed or taken against accreditation, license or registration; or
 - (c) The Department of Health (DOH) has placed any stipulation or condition on the Contractor's license.
- (2) The Contractor shall provide a copy of all notices listed in subsection c (1) above to the DSHS Contact by email or fax within one (1) business day of receipt of any such notice.

4. Statement of Work. The Contractor shall provide the services, and otherwise do all things necessary for or incidental to the performance of work, as set forth below:

- a. Accept and respond to CSD referrals for review of medical evidence.
 - (1) At the discretion of the DSHS Contact, referrals may be sent either through a designated web-based application where the Contractor can log in and view referrals, or via secure email.
 - (2) Referrals can be up to 10MB in size, and are typically between 2 and 5MB each.
- b. Notify the DSHS Contact within one (1) business day when the Contractor has examined or is treating the client. At this point the DSHS Contact shall reassign the referral.
- c. Notify the DSHS Contact when the Contractor is unavailable to accept referrals:
 - (1) At least seven (7) days in advance for planned absences;
 - (2) Due to any unplanned absences; or
 - (3) Due to equipment failure.
- d. Respond to accepted referrals by:
 - (1) Evaluating the medical evidence and the information recorded by the Disability Specialist on the Review of Medical Evidence form (DSHS Form #13-899).
 - (2) Completing the DSHS Review of Medical Evidence form (DSHS Form #13-899) by computer word processing program.

Special Terms and Conditions

- (3) Indicating whether the following information recorded by the Disability Specialist is supported by the medical evidence contained in the referral: diagnosis, severity, functional limitations, duration, onset date, and information regarding the impact(s) of a substance use disorder
 - (4) Sending the completed Review of Medical Evidence form (DSHS Form #13-899) to the CSO by use of a designated website, or by secure email at the discretion of the DSHS Contact.
 - (5) Notify the DSHS Contact within one (1) business day upon discovery of a discrepancy with a referral or the completion of the Review of Medical Evidence form (DSHS Form #13-899).
- e. The Contractor shall return the completed Review of Medical Evidence form (DSHS Form #13-899) within five (5) business days, starting the day after the receipt of the referral.

5. Contractor Training

The Contractor shall attend any Contractor training deemed necessary by CSD to perform services under this contract. Training is at the discretion of CSD and may be conducted in-person or in the form of a conference call or online class.

6. Consideration.

Total consideration payable to the Contractor for satisfactory performance of the work under this Contract, including any and all expenses, shall be based on the following:

- a. For each completed Review of Medical Evidence form (DSHS Form #13-899):
 - (1) \$24, when returned within three (3) business days of the referral.
 - (2) \$19, when returned within four (4) to five (5) business days of the referral.
 - (3) \$14 when returned after five (5) business days of the referral.
- b. Business days do not include the day of the referral.

7. Billing and Payment

- a. Invoice System.
 - (1) The Contractor shall submit monthly invoices and documentation of delivery of services using a State Form A-19 Invoice Voucher or other such forms as designated by the DSHS Contact.
 - (2) Consideration for services rendered shall be payable upon receipt of properly completed invoices. The Contractor shall submit invoices to DSHS, Community Services Division (CSD), P.O. Box 45470, Olympia, WA 98504-5470 not more often than monthly and no less than quarterly.
 - (a) Only the calendar month of services shall be billed per invoice.
 - (3) The rates shall be in accordance with those set forth in Section 5, Consideration, of this Contract.
 - (4) All billing invoice forms shall be typewritten or completed using a computer word processing or spreadsheet program.

Special Terms and Conditions

b. Payment.

- (1) Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and acceptance, by the DSHS Contact, of the properly completed invoice.
- (2) Payment shall be sent to the address designated by the Contractor on page 1 of this Contract.
- (3) DSHS may at its sole discretion, withhold payment claimed by the Contractor for services rendered, if the Contractor fails to satisfactorily comply with any term or condition of this Contract.

8. Contractor Information

- a. The Contractor shall within ten (10) business days, provide to the DSHS Contact, any information concerning the Contractor's change of circumstances.
- b. Changes in the Contractor's circumstances include, but are not limited to, a change in:
 - (1) Business name,
 - (2) Address, telephone number, fax number, e-mail address; and
 - (3) Location of practice.
- c. The Contractor shall complete an updated Contractor Intake form (DSHS 27-043) when reporting changes under the above subsection (b).
- d. The Contractor shall provide a minimum of thirty (30) days advance notice to the DSHS Contact when choosing to limit, suspend, or withdraw their availability to perform services including, but not limited to, retirement.

9. Contract Suspension

- a. DSHS may take certain actions in the event the Contractor, or any of its partners, officers, directors, or employees, is investigated by a local, county, state or federal agency, for a matter which DSHS determines may adversely affect the delivery of services provided under this Contract.
- b. DSHS may, without prior notice, suspend the delivery of services pending final resolution of the investigation.
- c. If the Contractor's referrals are in suspense, the Contractor or their representative shall direct all inquiries to the DSHS Contact.

10. Data Sharing. In addition to the requirements in Exhibit A: Data Security Requirements, the Contractor must follow these instructions as well:

- a. Purpose.
 - (1) Activity for which the Data is needed: To assist DSHS in determining eligibility for the ABD program.
 - (2) How the Contractor will use the Data: The Contractor's use is limited to reviewing and evaluating medical evidence provided by DSHS.

Special Terms and Conditions

b. Description of Data.

(1) Data Elements:

(a) Personal Identification Information, which may include, but is not limited to, the following:

- i. Client Name; and
- Client ID Number.

(b) Client personal health information, including medical records.

(c) Referral text comments.

This data may only be used for the purposes intended under the terms of this Contract.

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

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

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

c. Data Access or Transfer.

(1) Method. Referrals from CSOs through DSHS secure website, or via secure email at the discretion of the DSHS Contact.

(2) Portable Devices and Portable Media.

(a) The Contractor must obtain written permission from the DSHS Contact listed on page 1 of this Contract prior to using portable devices or portable media for purposes related to providing services under this Contract.

(b) The Contractor shall provide DSHS with information about the type of portable devices or portable media that will be used.

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

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

- i. Type of portable devices or portable media used;
- ii. Serial Numbers;
- iii. Proof of encryption of DSHS Data; and
- iv. Check-in and check-out system which identifies which of the Contractors staff is using the portable devices or media that contains DSHS Data.

Special Terms and Conditions

- (e) The Contractor must have a process in place that will ensure that they download all DSHS Data on a weekly basis from portable device or portable media to a secure storage method, as described in Exhibit A: Data Security Requirements.
 - (f) The Contractor shall keep a record of dates of the weekly storage download and the storage method.
- (3) The Contractor shall upon the request of DSHS make the records required in this section available to DSHS.
- (4) When services stop or the Contract ends for any reason, or the Contractor is no longer authorized to use a portable device or media to store DSHS client data, the Contractor must immediately:
- (a) Remove all DSHS Client data from the portable device or media and transfer the Client data to a secure storage method as described in Exhibit A: Data Security Requirements.
 - (b) Submit a signed Declaration of Data Disposition form (DSHS 27-108) that states that all DSHS client information has been deleted, purged, erased or destroyed from the Contractor's hard copy and/or electronic files before DSHS authorizes the final payment.
- (5) Requirements for Data Access.
- (a) The Contractor shall limit access to DSHS Client information to their employees whose duties specifically require access to such data in the performance of their assigned duties.
 - (b) Prior to making the information available, the Contractor shall notify all employees with access to the information of the use and disclosure requirements.
 - (c) The Contractor and any employee(s) with access to clients' information shall sign a Notice of Nondisclosure form (provided by DSHS) to acknowledge the data access requirements prior to being granted access to the data.
 - (d) The Contractor shall retain the original signed Notice of Nondisclosure forms for monitoring purposes. The shall make the forms available to DSHS upon request for contract monitoring purposes and ensure they are protected in accordance with Exhibit A: Data Security Requirements.
 - (e) The Contractor and its employee(s) must read and sign the Nondisclosure forms annually.
 - (f) Violations of the Nondisclosure provisions of this Contract 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 (1) year and/or a fine not to exceed five-thousand dollars (\$5,000).
- d. Security of Data.
- (1) Data Protection.

The Contractor shall exercise due care to protect data from unauthorized physical and electronic access. Due care includes establishing and maintaining security policies, standards, and procedures that detail:

Special Terms and Conditions

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

(2) Data Disposition.

- (a) In the event this Contract is terminated for convenience or default, the Contractor shall return or dispose of all DSHS Client Data as prescribed in Exhibit A – Data Security Requirements.
- (b) In the event this Contract is terminated due to Contractor's death or disability, the estate or other legal representative shall return or dispose all DSHS Client Data as prescribed in Exhibit A – Data Security Requirements.
- (c) DSHS shall not process the Contractor's final invoice for payment until such time that the Contractor has completed a signed and submitted Disposition of Data Form (DSHS 27-108) stating that DSHS client records created or obtained for the purposes of the Contract have been deleted, purged, erased or destroyed from the Contractor's hard copy and/or electronic files.

11. Confidentiality and Nondisclosure

- a. The Data to be shared under this Contract is confidential in nature and is subject to state and federal confidentiality requirements that bind the Contractor and its employees to protect the confidentiality of the personal information contained in Economic Services Administration data.
- b. The Contractor may use personal data and other data gained by reason of this Contract only for the purpose of this Contract.
- c. The Contractor shall not disclose, transfer, or sell any such information to any party, except as provided by law or, in the case of Personal Information, without the prior written consent of the person to whom the Personal Information pertains
- d. 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. The Contractor agrees to keep client information according to DSHS policy and procedures.
- e. 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 (1) year and/or a fine not to exceed five-thousand dollars (\$5,000).

12. Equipment and Supplies

The Contractor shall provide all equipment and supplies necessary to provide the contracted services.

Special Terms and Conditions

13. Termination

In addition to the requirements of Section 26 of the General Terms and Conditions of this contract, entitled Termination or Expiration Procedure, the Contractor shall submit a completed, signed Declaration of Data Disposition Form DSHS 27-108 declaring under penalty of perjury that all Client records have been deleted, purged, erased or destroyed from the Contractor's hard copy and/or electronic files. This declaration is to be addressed to the DSHS contact listed on page 1 of the Contract regardless of the reason for termination.

14. Insurance

The DSHS insurance requirements have been waived for this Contract.

15. Monitoring

The Contractor shall be available upon the request of DSHS to participate in the following Contract monitoring activities:

- a. Monitoring at the locations where the Contractor provides contracted services.
- b. Telephone interviews.
- c. Annual completion of the CSD ABD Program Medical Evidence Review Contractor Self-Assessment Monitoring Tool provided by DSHS.

16. Subcontracting

Subcontracting is not permitted under the terms of this Contract.

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

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

Exhibit A – Data Security Requirements

1. **Definitions.** The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
 - a. “AES” means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>).
 - b. “Authorized Users(s)” means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.
 - c. “Business Associate Agreement” means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.
 - d. “Category 4 Data” is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (<https://www.irs.gov/pub/irs-pdf/p1075.pdf>); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.
 - e. “Cloud” means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.
 - f. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key”; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.
 - g. “FedRAMP” means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.
 - h. “Hardened Password” means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.
 - i. “Mobile Device” means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

- j. “Multi-factor Authentication” means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. “PIN” means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.
- k. “Portable Device” means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.
- l. “Portable Media” means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.
- m. “Secure Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.
- n. “Trusted Network” means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.
- o. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

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

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

- a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.
- b. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

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

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

- a. Have documented policies and procedures governing access to systems with the shared Data.
- b. Restrict access through administrative, physical, and technical controls to authorized staff.
- c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.
- d. Ensure that only authorized users are capable of accessing the Data.
- e. Ensure that an employee's access to the Data is removed immediately:
 - (1) Upon suspected compromise of the user credentials.
 - (2) When their employment, or the contract under which the Data is made available to them, is terminated.
 - (3) When they no longer need access to the Data to fulfill the requirements of the contract.
- f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.
- g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:
 - (1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
 - (2) That a password does not contain a user's name, logon ID, or any form of their full name.
 - (3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.
 - (4) That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.
- h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk and enforce password and logon requirements for users by employing measures including:
 - (1) Ensuring mitigations applied to the system don't allow end-user modification.
 - (2) Not allowing the use of dial-up connections.

- (3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.
 - (4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.
 - (5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.
 - (6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point.
- i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:
 - (1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor
 - (2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)
 - (3) Must not contain a “run” of three or more consecutive numbers (12398, 98743 would not be acceptable)
 - j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:
 - (1) Be a minimum of six alphanumeric characters.
 - (2) Contain at least three unique character classes (upper case, lower case, letter, number).
 - (3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.
 - k. Render the device unusable after a maximum of 10 failed logon attempts.

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

- a. **Hard disk drives.** For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
- b. **Network server disks.** For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

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

- c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- e. **Paper documents.** Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.
- f. **Remote Access.** Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.
- g. **Data storage on portable devices or media.**
 - (1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:
 - (a) Encrypt the Data.
 - (b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
 - (c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
 - (d) Apply administrative and physical security controls to Portable Devices and Portable Media by:
 - i. Keeping them in a Secure Area when not in use,

- ii. Using check-in/check-out procedures when they are shared, and
 - iii. Taking frequent inventories.
- (2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.

h. Data stored for backup purposes.

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

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

- (1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:
- (a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.
 - (b) The Data will be Encrypted while within the Contractor network.
 - (c) The Data will remain Encrypted during transmission to the Cloud.
 - (d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.
 - (e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DSHS.
 - (f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.
 - (g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Contractor's network.
- (2) Data will not be stored on an Enterprise Cloud storage solution unless either:
- (a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,

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

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

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

- a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.
- b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.
- c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.
- d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. Data Segregation.

- a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.
 - (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,
 - (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
 - (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
 - (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.
 - (5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.
- b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

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

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

- 9. Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.
- 10. Data shared with Subcontractors.** If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the subcontractor must be submitted to the DSHS Contact specified for this contract for review and approval.