Washington State Department of Social & Health Services

Transforming lives

COUNTY
DATASHARE AGREEMENT
Washington Connection

DSHS Agreement Number: 2263-42291

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

Administration or Division Agreement Number

County Agreement Number

DSHS ADMINISTRATION	DSHS DIVISION	DSHS INDEX NUMBER	DSHS CONTRACT CODE
Economic Services Administration	Community Services Division	1231	3067CS-63

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Jessica Gempler Program Administrator	712 SE Pear St Olympia, WA 98504

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(509)655-0117	Click here to enter text.	Jessica.gempler@dshs.wa.gov

COUNTY NAME	COUNTY ADDRESS
Pacific County Pacific County Health & Human Services	7013 Sandridge Rd. Long Beach, WA 98631

COUNTY CONTACT NAME: Katie Lindstrom

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(360) 642-9300	(360) 642-9352	koien@co.pacific.wa.us

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

PROGRAM AGREEMENT START DATE	**PROGRAM AGREEMENT END DATE**	MAXIMUM PROGRAM AGREEMENT AMOUNT
05/01/2022	04/30/2024	No Payment

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

☒ **Data Security: Exhibit A – Data Security Requirements**

☐ **Other Exhibits (specify):**

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

COUNTY SIGNATURE(S)	PRINTED NAME(S) AND TITLE(S)	DATE(S) SIGNED

DSHS SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
	Alice Hildebrant, Contracts Officer DSHS/ESA/Community Services Division	

Special Terms and Conditions

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

   a. "Applicant(s)" means individuals submitting an application, a renewal or reporting a change for benefits or services.

   b. "Assisting Agency" means community or faith based organizations, tribal, city, or county municipalities who provide trained employees or volunteers to help applicants complete and submit online applications through Washington Connection. These agencies must sign a Data Share Agreement with DSHS and each employee and volunteer of the agency with access to Applicant information must complete a DSHS non-disclosure form. Any reference to Assisting Agency includes the Assisting Agency's employees, agents, officers, subcontractors, third party contractors, volunteers, or directors.

   c. "Authorized Representative" means someone designated by the Applicant to talk with DSHS about his/her benefits. This individual is authorized to act on the Applicant's behalf for eligibility purposes.

   d. "Contractor Contact", referenced on page one of this agreement, means the person who handles the day-to-day duties related to this agreement. This person may or may not be the one who signs this agreement on behalf of the Contractor.

   e. "Data" means the information that is exchanged as described by this Agreement that is specifically protected by law which may impose penalties for wrongful disclosure. This includes protected health information under the HIPAA Privacy Rule.

   f. "ESA" means Economic Services Administration.

   g. "SAW" means SecureAccess Washington. SAW is a single sign-on application gateway created by Washington State's Department of Information Services to access government services accessible via the Internet.

   h. "Washington Connection" means the web-based benefit portal that provides access to a broad array of federal, state and local services and benefits to address basic needs.

2. **Purpose:** To allow an Assisting Agency to help Washington residents complete an online application to provide more effective access to available federal, state and local services through the Washington Connection benefit portal and carry out other activities designed to help them maintain eligibility. This agreement also includes contractors that submit paper applications to DSHS.

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

   a. The Assisting Agency listed on page one of this Data Share Agreement is the Contractor, and DSHS is the Data Provider in this agreement. In exchange for the receipt of information, the Contractor agrees to abide by the terms and conditions in this agreement.

      (1) Anyone at the Contractor agency with access to Data will be required to read and complete a non-disclosure agreement annually. The Contractor must maintain these forms and make them available for inspection.

      (2) When Contractors use Washington Connection for applications, DSHS will work with them to:

(a) Establish access to the DSHS Washington Connection and online application.

(b) Establish a Washington Connection SAW account with either an Employee or a Supervisor access level:

i. *Employee Access* allows the individual to view, edit and submit applications when the employee has provided direct access with the application through Washington Connection as part of their work at the Assisting Agency.

ii. *Supervisor Access* includes all functions of the Employee Access plus the ability to: view, edit and submit all applications associated with employees assigned to the supervisor in the Washington Connection profile; add, modify, and delete employees; reassign applications between employees under the same supervisor, and request a summary page of all application status (submitted or incomplete) associated with the Assisting Agency.

(3) Consent Form and Use Limitation

(a) The Contractor must obtain a Consent form via Washington Connection with an e-signature from the Applicant before accessing any Applicant Information. The Contractor must keep any written DSHS consent form obtained from the Applicant onsite and provide them for inspection upon request.

i. DSHS and the Contractor may need to share additional information to provide services, but at no time should the Consent be interpreted to:

(A) Designate the Contractor as an "Authorized Representative"

(B) Allow DSHS to share Applicant information not needed for the purposes under this agreement

(C) Allow DSHS to disclose documents or information from the Applicant's files or records for other purposes outside the scope of this agreement

b. Description of Data

Data is limited to:

(a) application data

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

c. Data Access or Transfer

(1) If applications are received through Washington Connection and the Applicant has indicated consent to share application data, a Contractor may view and print applications, reviews and change of circumstances forms saved or submitted through Washington Connection for 90 calendar days from the last activity day. Application statuses, "submitted" or "not submitted", are also available for 90 calendar days from the last activity day. Contractors submitting paper applications have no ability to view them online.

(2) If the correct client identification number or negative client identification number (includes a minus sign before the number) is entered into the Washington Connection query system, the successful query will result in the display of the following information for the listed head of household if that person is not registered in the Address Confidentiality Program (ACP):

(a) Application Status

A = approved

P = Pending

D = Denied

M = Pending Spend down (with base period and remaining amount)

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

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

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

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

(f) Child's name receiving childcare services

(g) Childcare provider name for each child

(h) Copayment amount for each child

(i) Gross earned income

(3) Requirements for Access

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

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

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

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

d. Limitations on Use of Data

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

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.

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. Inspection.

a. These inspection rights supersede the general terms and conditions of this agreement. The Contractor shall, at no cost, provide DSHS and the Community Services Division Washington Connection Community Partnership Program with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located, as they relate to this agreement. These inspection rights are intended to allow the Program to monitor, audit, and evaluate the Contractor's compliance regarding these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.

b. The Contractor will receive a self-assessment via email no less than once every four (4) years. The self-assessment and other supporting documents will be provided by the DSHS contact listed on page one (1,) or their designee. The self-assessment is meant to ensure compliance with:

(a) Annual review, signing, and retention of Nondisclosure Agreements;

(b) Proof of current liability insurance;

(c) Review of active Washington Connection Partner Account users, access, and privileges;

(d) Confidentiality and Nondisclosure through Client Search and internal consent

c. The Contractor shall complete and return the self-assessment within the timeframe provided by the DSHS contact listed on page one (1,) or their designee (not to exceed 30 calendar days.)

6. Confidentiality and Nondisclosure

a. Both parties may use Personal Information and other information or Data gained by reason of this Agreement only for the purposes of this Agreement.

b. The data to be shared under this agreement is confidential in nature and is subject to state and federal confidentiality requirement that bind the Contractor, its employees, and its subcontractors to protect the confidentiality of the personal information contained in ESA data. Contractors may use personal data and other data gained by reason of this agreement only for the purpose of this agreement.

c. The Contractor shall maintain the confidentiality of personal data in accordance with state and federal laws, and shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements, including restrictions on re-disclosure.

d. Neither party shall link the Data with Personal Information or individually identifiable data from any other source nor re-disclose or duplicate the Data unless specifically authorized to do so in this Agreement.

7. Consideration

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

8. 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.

9. Compensation

a. The Contractor shall not charge the applicant for services or time rendered while assisting with application, renewal, or reporting changes to the Department of Social and Health Services

b. If the applicant requests additional services not included herewith, these services may be subject to fees and should be authorized in writing and signed by the applicant and Contractor under the auspice of separate agreement.

10. 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

11. Contractor Information

The Contractor shall forward to the DSHS Contact person named on page one (1) of this contract (or

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

Exhibit A – Data Security Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.

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

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

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

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

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

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

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

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

(1) Upon suspected compromise of the user credentials.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) Be a minimum of six alphanumeric characters.

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

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

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

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

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

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

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above

paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

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

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

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

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

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

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

(a) Encrypt the Data.

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

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

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

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

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

iii. Taking frequent inventories.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. **Data Segregation**.

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

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

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

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

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

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

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

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

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk

Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

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

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