Washington State DEPARTMENT OF SOCIAL & HEALTH SERVICES

INDIAN NATION PROGRAM AGREEMENT DATA SHARE AGREEMENT ACES & SEMS WEB

DSHS Agreement Number: 1862-36977

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

Administration or Division Agreement Number:

Indian Nation Agreement Number:

DSHS ADMINISTRATION	DSHS DIVISION	DSHS INDEX NUMBER	CCS CONTRACT CODE
Economic Services Administration	Community Services Division	3214	3042NS-62

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Martin Bohl Program Administrator	712 Pear St SE Olympia, WA 98504-5440

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(360)725-4656	(360)725-4904	martin.bohl@dshs.wa.gov

INDIAN NATION NAME	INDIAN NATION ADDRESS
South Puget Intertribal Planning Agency	3104 SE Old Olympic Hwy Shelton, WA 98584-7731

INDIAN NATION CONTACT NAME: Whitney Jones

INDIAN NATION CONTACT TELEPHONE	INDIAN NATION CONTACT FAX	INDIAN NATION CONTACT E-MAIL
(360) 426-3990	(360) 427-8003	wjones@spipa.org

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

PROGRAM AGREEMENT START DATE	PROGRAM AGREEMENT END DATE	MAXIMUM PROGRAM AGREEMENT AMOUNT
09/01/2018	08/31/2021	No Payment

EXHIBITS. When the box below is marked with a check (✓) or an X, the following Exhibits are attached and are incorporated into this Indian Nation Program Agreement by reference:

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

☒ **Exhibits (specify): Exhibit B – Assurances & Certifications form, Exhibit C – Washington State Department of Social & Health Services – Notice of Nondisclosure, Exhibit D – DSHS Form 9-989 (Confidentiality Statement – Tribal Employee)**

By their signatures below, the parties agree to the terms and conditions of this Indian Nation Program Agreement and all documents incorporated by reference. No other understandings or representations, oral or otherwise, regarding the subject matter of this Program Agreement shall be deemed to exist or bind the parties. The parties signing below certify that they are authorized, as representatives of their respective governments, to sign this Program Agreement.

	PRINTED NAME AND TITLE	DATE SIGNED
INDIAN NATION SIGNATURE: Whitney Jones	Whitney Jones, Executive Dir.	1/21/19
DSHS SIGNATURE (CSD ACES): Christine Burton CSD Contracts Officer	PRINTED NAME AND TITLE: Christine Simmonds, Contracts Officer DSHS/ESA-Community Services Division	DATE SIGNED: 2/5/19
DSHS SIGNATURE (DCS SEMS):	PRINTED NAME AND TITLE: Maria Sosa DSHS/ESA/DCS	DATE SIGNED: 1/22/19

1. Government to Government Relations

a. The South Puget Intertribal Planning Agency (SPIPA), TANF program, named above, includes four federally recognized Indian Tribes: the Nisqually Indian Tribe, Skokomish Indian Tribe, Puyallup Tribe and the Squaxin Island Tribe. Both the State of Washington and the aforementioned Tribes represented by SPIPA are sovereign governments. SPIPA and DSHS agree to these Special General Terms and Conditions for the purpose of furthering the government-to-government relationship acknowledged in the Centennial Accord and to achieve their mutual objectives of providing efficient and beneficial services to their people.

b. Nothing in this Agreement shall be construed as a waiver of tribal sovereign immunity.

2. Definitions

a. "ACES" means Automated Client Eligibility System.

b. "Centennial Accord" means the agreement entered into between federally recognized tribes in Washington State and the State of Washington on August 4, 1989.

c. "ESD" means the Employment Security Department of Washington State.

d. ""Federal" means the United States of America.

e. "Fob" means a type of security token: a small hardware device with built-in authentication mechanisms that provide two factor authentication of users.

f. "SEMS" means Support Enforcement Management System.

g. "SGN" means Statewide Governmental Network.

h. "Software Security Token" means a type of two-factor authentication security software that is used to verify the identity of the user accessing database information, as defined in this contract. The SST represents software placed on the user's computer.

i. "State" means the state of Washington.

j. "TANF" means Temporary Assistance to Needy Families.

k. "Tribe" or "Tribal" means the entity performing services pursuant to this Indian Nation Program Agreement. This includes the Tribe's officers, directors, trustees, employees and/or agents unless otherwise stated in this Indian Nation Program Agreement. For purposes of this Indian Nation Program Agreement, the Tribe is not considered an employee or agent of DSHS.

l. "South Puget Intertribal Planning Agency" or "SPIPA" means the entity performing services pursuant to this Indian Nation Program Agreement. This includes the SPIPA's officers, directors, trustees, employees and/or agents unless otherwise stated in this Indian Nation Program Agreement. For purposes of this Indian Nation Program Agreement, SPIPA is not considered an employee or agent of DSHS.

3. Statement of Work

a. Programs Receiving and Providing Data

(1) SPIPA is the data recipient; contact information is listed on page number one under Indian Nation name.

(2) DSHS is the data provider; contact information is listed on page number one under DSHS Administration.

b. Purpose

(1) The purpose of this agreement is to provide access to data for the limited purpose of assisting the Tribe in administering their Tribal Title IV-A TANF Program, DSHS shall provide the Tribe with access to:

(a) Automated Client Eligibility System (ACES)

(b) Support Enforcement Management System (SEMS)

(c) Employment Security Department (ESD) earnings and benefit information.

c. Description of Data

(1) ACES Data

Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to ACES.

(2) SEMS Data

Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to SEMS cases where the Tribe is coded on the SEMS case. DSHS will provide the Tribe's staff with electronic inquiry only access to Child Support information for verification of child support cases, family relationships, and financial history as authorized under RCW 26.23.120. The IV-D data in SEMS that DCS may provide to a Tribal IV-A program is limited to the purposes provided for in 45 CFR 307.13.

(3) Confidential Benefit and Wage Employment Data

Designated employees or contracted staff of the Tribe shall have limited read-only web based secured access to confidential benefit and wage employment data collected through the Unemployment Compensation (UC) program.

d. Data Access or Transfer

(1) Unique user identification numbers and passwords obtained from DSHS are required in order for the authorized tribal staff to log on to ACES and SEMS.

(2) The Tribe will need to submit the IP numbers of the workstations that will need to access ACES and SEMS.

(3) ACES/SEMS - Method of Access / Transfer

(a) Connection to ACES and SEMS will occur in one of the following two ways, either:

i. Through a workstation attached to the intergovernmental network (IGN), or

ii. DSHS will grant data access to ACES and SEMS for designated staff through a Virtual Private Network (VPN) connection provided by the Information System Services Division (ISSD), which uses fobs or software security tokens (SST) as a secondary factor of authentication, in addition to user identification and password.

(A) The Tribe will elect whether the secondary factor of authentication will be either fobs or SSTs.

(B) If the Tribe opts to use fobs:

1. DSHS will provide a maximum of four (4) dual ACES-SEMS fobs to the Tribal TANF program free of charge. Each of the four (4) fobs will provide access to both ACES & SEMS.

2. Each of the fobs provided must be assigned to only one (1) individual, and access and use of the fobs shall not be shared between program employees or contracted staff.

3. Fobs lost or damaged by the Tribe may be replaced by DSHS. DSHS may charge the Tribe $75.00 to replace a lost or damaged fob.

(C) If the Tribe opts to use SST's:

1. DSHS will provide a maximum of four (4) dual ACES-SEMS SST's to the Tribal TANF program free of charge. Each of the four (4) SST's will provide access to both ACES & SEMS.

2. Each of the SST's provided must be assigned to only one (1) individual, and access and use of the SST's shall not be shared between program employees or contracted staff.

e. Limitations on Use of Data

(1) The Tribe shall ensure that Tribal TANF employees or contracted staff persons have access to ACES and SEMS records only when necessary to fulfill the TANF requirements of their program.

(2) ACES – SEMS Security Monitoring

(a) The Tribe shall assign a person as a security monitor as a point of contact for ACES and SEMS.

(b) The security monitor will:

i. Route ACES access requests through the ESA Information Technology Division Central Support Help Desk.

ii. Route SEMS access requests through the DCS Program Manager.

iii. Assist in DSHS' efforts to monitor the security provisions of the DSA, by annually reviewing, completing and submitting the Assurances and Certifications form (see **Exhibit B**) to DSHS on the following dates:

(A) September 1, 2019

(B) September 1, 2020

(C) September 1, 2021

iv. Notify the ESA Information Technology Division Central Support Help Desk immediately when employees or contracted staff that have access to ACES terminate employment, transfer, or change duties.

v. Notify the DCS Program Manager immediately when employees or contracted staff that have access to SEMS terminate employment, transfer, or change duties.

vi. Perform the following actions upon an employee or contracted staff member (with SEMS or ACES access) terminating employment, transferring, or changing duties:

(A) Promptly revoke access that is no longer needed or appropriate. Disable (revoke) all user IDs within five business days of the termination.

(B) Notify the employee or contracted staff member of his or her duty to keep information confidential.

(C) Disable (revoke) all access and user IDs immediately when an employee or contracted staff member is terminated for cause.

(c) Supervisors and/or managers must promptly report to the security monitor duty changes or other personnel changes for which removal or reduction of computer system privileges is appropriate.

f. Frequency of Exchange

The exchange of data is accomplished through on-line transactions that may occur whenever the application is available

g. Security of Data

(1) The Tribe shall secure the data provided in accordance with the requirements of **Exhibit A – Data Security Requirements.**

(2) The Tribe shall exercise due care to protect data from unauthorized physical and electronic access. Due care includes establishing and maintaining security policies, standards, and procedures which detail:

(a) Access security, identification, and authentication;

(b) Network and workstation security;

(c) Premise security; and

(d) Sanctions for unauthorized use or disclosure of data.

(3) To limit potential security breaches, if a Fob or SST is inactive for more than ninety (90) days, DSHS may deactivate it.

(4) DSHS provided data stored by the Tribe may not be accessed remotely — no use of external networks (e.g. the Internet) is allowed under this agreement.

(5) The Tribe shall track the location of any copies or backups of data provided by DSHS. The method of tracking shall be sufficient to provide the ability to audit the protections afforded the copied data sets.

(6) In the case of hardware failure, the Tribe must protect data by removing the hard drive before shipping equipment for repair.

h. Confidentiality and Nondisclosure:

(1) The Tribe shall protect confidential information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other State, Federal, or Tribal laws including the following incorporated by reference:

(a) SEMS IV-D Data:

i. RCW 42.56.230 Personal Information

ii. RCW 26.23.120 Information & Records – Confidentiality – Disclosure – Adjudicative Proceeding – Rules – Penalties

iii. 45 CFR 307.13 Security & Confidentiality for Computerized Support Enforcement Systems in Operation After October 1, 1997

iv. 20 CFR 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information

v. 42 USC 654(26) Safeguarding Confidential Information

(b) ACES Data:

i. RCW 74.04.060 Records, Confidential – Exception – Penalty

ii. RCW 42.56.230 Personal Information

iii. 42 USC 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information

(2) For Child Support information contained in SEMS or the Title IV-D program, all information is private and confidential and shall be exempt from disclosure under RCW 42.56 or other Federal, State or Tribal laws.

(3) The Tribe shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements.

(4) The Tribe, its employees and contracted staff may use confidential Information or data gained by reason of this Agreement only for the purposes of this Agreement.

(5) The Tribe shall not disclose nor transfer any information as described in this Program Agreement to any party in whole or in part, or to any individual or agency unless the information is exempt from disclosure under applicable State, Federal or Tribal laws.

(6) All confidential information DSHS receives from the Tribe under this Agreement will be kept confidential by DSHS employees as required by State, Federal or Tribal laws.

(7) Notice of Nondisclosure

(a) ACES: SPIPA must ensure each employee or contracted staff person with access to ACES and/or ESD records or information annually signs the Washington State Department of Social and Health Services, Notice of Nondisclosure (Nondisclosure form) (Exhibit C) prior to DSHS granting access.

SPIPA shall retain a signed copy of the Nondisclosure form on file for monitoring purposes and made available for DSHS review upon request.

(b) SEMS: SPIPA must ensure that each employee or contracted staff person with SEMS access (including, but not limited to ESD information) annually reviews and signs the Federal and State data access requirements listed in the SEMS, Confidentiality Statement – Tribal Employee (DSHS 9-989) (Exhibit D), prior to DSHS granting access. Staff with direct access must also annually electronically acknowledge this agreement.

SPIPA shall retain a signed copy of the DSHS 9-989 form (**Exhibit D**) on file for monitoring purposes and made available to DSHS review upon request.

(8) Notification of unauthorized disclosure:

SPIPA shall notify the Economic Services Administration (ESA) within one (1) business day of discovery of any unauthorized disclosure of ACES, SEMS or ESD information. Notification to ESA shall be done by sending an email to databreach@dshs.wa.gov.

4. Disputes

Disputes shall be resolved in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between DSHS and the four (4) Tribes participating in the SPIPA Tribal TANF program: Nisqually, Skokomish, Puyallup and Squaxin Island Tribes.

5. Termination

Termination of this Agreement shall be in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between DSHS and the four (4) Tribes participating in the SPIPA Tribal TANF program: Nisqually, Skokomish, Puyallup and Squaxin Island Tribes.

APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL

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 Indian Nation and on a network outside the control of the Indian Nation. 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 Indian Nation staff are not present to ensure that non-authorized staff cannot access it.

n. "Trusted Network" means a network operated and maintained by the Indian Nation, 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 Indian Nation 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 Indian Nation staff for violating that policy.

b. If the Data shared under this agreement is classified as Category 4, the Indian Nation 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 Indian Nation 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 Indian Nation 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 Indian Nation's network (the Data stays within the Indian Nation's network at all times), enforce password and logon requirements for users within the Indian Nation'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 Indian Nation'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 Indian Nation 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 Indian Nation's staff. Indian Nation will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Indian Nation, 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 Indian Nation 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 Indian Nation 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 an Indian Nation'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 an Indian Nation'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 Indian Nation 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) Indian Nation has written procedures in place governing use of the Cloud storage and Indian Nation attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the Indian Nation 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 Indian Nation will possess a decryption key for the Data, and the decryption key will be possessed only by the Indian Nation and/or DSHS.

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