



**INDIAN NATION
PROGRAM AGREEMENT
Treasury Offset - Tribal IV-D Program**

DSHS Agreement Number
1862-23198

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 a DSHS and Indian Nation Agreement on General Terms and Conditions, which is incorporated by reference.

Administration or Division Agreement Number

Indian Nation Agreement Number

DSHS ADMINISTRATION
Economic Services Administration

DSHS DIVISION
Division of Child Support

DSHS INDEX NUMBER
1317

CCS CONTRACT CODE
3000NC-62

DSHS CONTACT NAME AND TITLE
Saundra Cheek
Program Administrator

DSHS CONTACT ADDRESS
712 Pear St SE
PO Box 9162
Olympia, WA 98507-9162

DSHS CONTACT TELEPHONE
(360)664-5025

DSHS CONTACT FAX
(360)664-5342

DSHS CONTACT E-MAIL
scheek@dshs.wa.gov

INDIAN NATION NAME
Quinault Indian Nation

INDIAN NATION ADDRESS
PO Box 689
214 4th Street
Taholah, WA 98587

INDIAN NATION FEDERAL EMPLOYER IDENTIFICATION NUMBER

INDIAN NATION CONTACT NAME
Gina James

INDIAN NATION CONTACT TELEPHONE
(360) 276-8211

INDIAN NATION CONTACT FAX
(360) 276-0293

INDIAN NATION CONTACT E-MAIL
gjames@quinault.org

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

CFDA NUMBERS

PROGRAM AGREEMENT START DATE
01/01/2018

PROGRAM AGREEMENT END DATE
12/31/2020

MAXIMUM PROGRAM AGREEMENT AMOUNT
No Payment

EXHIBITS. When the box below is marked with a check (4) or an X, the following Exhibits are attached and are incorporated into this Indian Nation Program Agreement by reference:
 Exhibits (specify): Indian Nation Data Security Requirements Exhibit A, Tribal IV-D Monthly Debt Summary for Treasury Offset Program Reporting Sample - Exhibit B
 No Exhibits.

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.

INDIAN NATION SIGNATURE

PRINTED NAME AND TITLE
Gina V. James, Program Mng.

DATE SIGNED
1-16-18

DSHS SIGNATURE

PRINTED NAME AND TITLE
Ann Polanco, Contracts Administrator
DSHS/ESA/DCS Headquarters

DATE SIGNED
1/16/18

1. Government to Government Relations

- a. The Indian Nation named above and the State of Washington are sovereign governments. The Indian Nation and DSHS agree to the terms of this program agreement, 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 the public.
- b. Nothing in this Agreement shall be construed as a waiver of tribal sovereign immunity.

2. Definitions

- a. "Administrative Review" means the process described in 45 CFR 303.72 whereby a noncustodial parent may contest certification of a debt for Treasury Offset
- 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. "CFR" means the Code of Federal Regulations.
- d. "CP" means the Custodial Parent.
- e. "Data" means "confidential information" or "confidential data" as defined the DSHS and Indian Nation Agreement on General Terms and Conditions (INGT&C).
- f. "DCS" means the Division of Child Support of the Economic Services Administration.
- g. "ESA" means the DSHS Economic Services Administration.
- h. "Indian Nation GT&C" is the DSHS and Indian Nation Agreement on General Terms and Conditions.
- i. "NCP" means the Non-Custodial Parent.
- j. "TANF" means Temporary Assistance to Needy Families.
- k. "Treasury Offset Program Withholding" means the type of service requested on Child Support Enforcement Transmittal #1 in Section 1 Action, Block 5 Other sent to the local DCS office
- l. "Tribe" means the entity requesting 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.
- m. "Tribal IV-D Program" or "Tribal Child Support Program" means an Indian Tribe in Washington State that administers a federally-approved child support programs.
- n. "USC" means the United States Code.

3. Purpose

The Purpose of this Agreement is for the DSHS Division of Child Support (DCS) to provide debt certification for Treasury Offset Withholding action on cases involving Tribal Child Support programs.

4. Statement of Work

a. CASE REQUIREMENTS

The Tribe will ensure the case meets the requirements listed in 45 CFR 303.72(a) before sending DCS a referral for treasury offset reporting of debt. The requirements are currently as follows:

- (1) The debt is based on an established court or administrative order.
- (2) The NCP's name and social security number (SSN) are correct.
- (3) For a non-assistance case, the Tribe will:
 - (a) Ensure that the debt is at least \$500.
 - (b) Provide a current address for a non-assistance CP.
- (4) For a TANF case, the Tribe will ensure that the debt is:
 - (a) At least \$150 and
 - (b) Past due for at least thirty (30) days

b. REFERRAL PROCESS

- (1) The Tribal IV-D Program will request treasury offset services by sending a referral to the local DCS field office for each NCP case they want certified. The referral will include, but is not limited to:
 - (a) Child Support Enforcement Transmittal #1 – Initial Request
 - (b) Relevant court orders
 - (c) Debt calculation
- (2) The Tribe will indicate on the referral that they are requesting Treasury Offset Program Withholding.

c. PAYMENT OF ADMINISTRATIVE COSTS

- (1) Every three (3) months, the ESA Fiscal Office will send an invoice listing the previous quarter's administrative costs associated with the Tribe's referred cases.
- (2) Within thirty (30) days of the date of the invoice, the Tribe will pay for the administrative costs that the Department of the Treasury Bureau of Fiscal Service charged DCS for servicing debts referred for collection. The current fees required by law are found in DCL-17-07. These Dept. of Treasury administrative costs are subject to change each federal fiscal year.
 - (a) Within thirty (30) days of being informed of the change in costs, DCS will notify the Tribe of the change in costs.
- (3) The Tribe shall make checks payable to "DSHS/DCS", reference the "Tribe Name / DCS Treasury Offset Agreement" on the check, and remit payment to:

ESA/OS Fiscal/DCS Accounting Unit
PO Box 45445
Olympia WA 98504-5445

Exception: DCS will not bill the Tribe for these costs if DCS, on its own behalf, also certified another debt for the same NCP in the same year.

d. DISTRIBUTION OF TREASURY OFFSET FUNDS

- (1) DCS distributes collections received from the Treasury Bureau of Fiscal Service to past due support on certified debt only as required in 45 CFR 302.51. DCS will send applicable funds to the Tribe via electronic funds transfer (EFT) or state check from the DCS bank account.
 - (a) If DCS distributes funds to the Tribe, and DCS must return any portion of the distributed funds, the Tribe agrees to repay the reversed funds. Reversals may occur due to reporting inaccurate debt, an incorrect social security number for the NCP whose debt is reported, or for other reasons.
 - i. DCS will include the reversal in the next quarterly invoice.
 - ii. DCS will work with the Tribe to establish a payment plan for the repayment of these funds to DCS.
 - iii. The Tribe will repay DCS within 30 days of being notified DCS returned funds to the Treasury.
- (2) The Tribe shall make checks payable to "DSHS/DCS", reference the "Tribe Name / DCS Treasury Offset Agreement", NCP name and DCS case number on the check, and remit payment to:

ESA/OS Fiscal/DCS Accounting Unit
PO Box 45445
Olympia WA 98504-5445

- (3) The Tribe agrees to return to DCS any portion of the funds that result in an overpayment due to NCP payments following certification.

e. ADMINISTRATIVE REVIEW ON CASES REFERRED BY A TRIBAL IV-D PROGRAM

If the NCP requests an administrative review because the NCP contests certification of a debt for Treasury Offset:

- (1) DCS will send a copy of the administrative review request to the Tribe.
- (2) If there is **only** tribal interest in the certified funds, the Tribe agrees to perform the administrative review as required in CFR § 303.72. The Tribe will notify DCS in writing of the administrative review decision which will allow the Tribal Liaison to take any necessary action.
- (3) In cases where there is a joint tribal and DCS interest in the certified funds, DCS and the Tribe will work together to provide the administrative review:
 - (a) DCS will make the final determination on debt DCS certified on DCS own behalf.
 - (b) The Tribe makes the final determination on any debt certified on its behalf, and provides

DCS with written recommendations instructing DCS if and how to provide relief to the NCP regarding any debt certified on the Tribe's behalf.

f. CASE CLOSURE

DCS will close the case after receiving from the Tribe a Child Support Enforcement Transmittal #2 form, requesting closure.

5. Description of the Data

a. At the request of the Tribal IV-D program signing this agreement, DCS shall release the following information related to a case certified for treasury offset when necessary for processing and distributing federal offset funds:

- (1) Confirmation that a payment is from administrative funds and that DCS applied it to certified arrears.
- (2) All documentation received from the NCP pertaining to the request for an administrative review or a hardship review.

b. The Tribal IV-D program will provide a monthly debt summary to DCS by the 10th of each month listing critical debt information for each case certified for treasury offset (see h.1.b.) and Exhibit B.

6. Exchange of Administrative Data

a. Method and Frequency of Exchange of Data:

- (1) DCS will provide the data listed in g. (1) (see above) by the following methods: hand deliver, mail, secured email, or telephone.
 - (a) If mailed, the data (hard copy) will be sent using any of the methods (Trusted Systems) in 1.i. of Exhibit A.
- (2) The Tribal IV-D Program must submit a monthly summary to the Tribal Liaison in the local DCS field office by the 10th of every month. An example is included as Exhibit B. The summary is required to ensure that the debt certified for treasury offset is accurate, and must include the following information for each case:
 - (a) NCP's name
 - (b) CP's name
 - (c) DCS case number (D#), if known (if not, include NCP social security number)
 - (d) Balance of the debt as of the last day of the prior month
 - (e) Date and amount of last payment received by the tribe included in the debt balance

7. Monitoring

a. To ensure the accuracy of debts referred for certification is maintained, the Tribe will:

- (1) Perform internal inspections to monitor compliance with the requirements of this agreement.

(2) Annually ensure staff is briefed on procedures and instructions for protecting confidential information and terms of this agreement.

b. DCS may test compliance with the terms of this Agreement by reviewing:

(1) The Tribal IV-D Monthly Debt Summary (10th of the Month) – Exhibit B, and

(2) Timeliness of payments received per the quarterly invoice, and

(3) The Agreement with the Tribal IV-D Program to monitor compliance.

B. Legal References in This Contract

All references in the contract to IRC, USC, CFR, RCW, or WAC chapters or sections shall include any successor, amended, or replacement code, regulation or statute.

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 subcontractor must be submitted to the DSHS Contact specified for this contract for review and approval.

