Washington State Department of Social & Health Services Transforming lives	**INTERLOCAL DATASHARE AGREEMENT** **Integrated Client Data Repository Authorization**	DSHS Agreement Number: 2091-96717

This Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the Contractor identified below, and is issued pursuant to the Interlocal Cooperation Act, chapter 39.34 RCW.	Program Contract Number: Contractor Contract Number:

CONTRACTOR NAME Department of Children, Youth, and Families		CONTRACTOR doing business as (DBA)	
CONTRACTOR ADDRESS 1500 Jefferson St SE Olympia, WA 98504		WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)	DSHS INDEX NUMBER 206397
CONTRACTOR CONTACT Tammy Cordova	CONTRACTOR TELEPHONE (360) 701-0211	CONTRACTOR FAX	CONTRACTOR E-MAIL ADDRESS tammy.cordova@dcyf.wa.gov

DSHS ADMINISTRATION Facilities, Finance and Analytics Administration	DSHS DIVISION Research and Data Analysis	DSHS CONTRACT CODE 8000DC-91
DSHS CONTACT NAME AND TITLE Barbara Lucenko Program Manager	DSHS CONTACT ADDRESS 1115 Washington St SE Olympia, WA 98504-5204	
DSHS CONTACT TELEPHONE (360) 902-0890	DSHS CONTACT FAX (360) 902-0705	DSHS CONTACT E-MAIL ADDRESS barbara.lucenko@dshs.wa.gov
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT? No		CFDA NUMBER(S)
AGREEMENT START DATE 11/12/2020	**AGREEMENT END DATE** 11/01/2025	MAXIMUM AGREEMENT AMOUNT No Payment

EXHIBITS. The following Exhibits are attached and are incorporated into this Agreement by reference:

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

☒ **Exhibits (specify): EXHIBIT B – ICDR Data Request Form; EXHIBIT C –RDA Data Use Agreement; EXHIBIT D – DCYF Data Elements; EXHIBIT E – IN19 Client Services Data**

The terms and conditions of this Agreement 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 Agreement, between the parties. The parties signing below represent they have read and understand this Agreement, and have the authority to execute this Agreement. This Agreement shall be binding on DSHS only upon signature by DSHS.

CONTRACTOR SIGNATURE Stephen Cotter	PRINTED NAME AND TITLE Office Chief - Contracts and Procurement	DATE SIGNED 11/16/2020
DSHS SIGNATURE Will Taplin	PRINTED NAME AND TITLE William Taplin, Contracts Counsel	DATE SIGNED 11/16/2020

DSHS General Terms and Conditions

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

   a. “Central Contracts and Legal Services” means the DSHS central headquarters contracting office, or successor section or office.

   b. “Confidential Information” or “Data” means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.

   c. “Contract” or “Agreement” means the entire written agreement between DSHS and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original.

   d. “CCLS Chief” means the manager, or successor, of Central Contracts and Legal Services or successor section or office.

   e. “Contractor” means the individual or entity performing services pursuant to this Contract and includes the Contractor’s owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, “Contractor” includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

   f. “Debarment” means an action taken by a Federal agency or official to exclude a person or business entity from participating in transactions involving certain federal funds.

   g. “DSHS” or the “Department” means the state of Washington Department of Social and Health Services and its employees and authorized agents.

   h. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key;” a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 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.

   i. “Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.

   j. “Physically Secure” means that access is restricted through physical means to authorized individuals only.

   k. “Program Agreement” means an agreement between the Contractor and DSHS containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by DSHS.

   l. “RCW” means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at http://apps.leg.wa.gov/rcw/.

m. “Regulation” means any federal, state, or local regulation, rule, or ordinance.

n. “Secured Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.

o. “Subcontract” means any separate agreement or contract between the Contractor and an individual or entity (“Subcontractor”) to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract.

p. “Tracking” means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.

q. “Trusted Systems” include only the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service (“USPS”) first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

r. “WAC” means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at http://apps.leg.wa.gov/wac/.

2. **Amendment.** This Contract may only be modified by a written amendment signed by both parties. Only personnel authorized to bind each of the parties may sign an amendment.

3. **Assignment.** The Contractor shall not assign this Contract or any Program Agreement to a third party without the prior written consent of DSHS.

4. **Billing Limitations.**

a. DSHS shall pay the Contractor only for authorized services provided in accordance with this Contract.

b. DSHS shall not pay any claims for payment for services submitted more than twelve (12) months after the calendar month in which the services were performed.

c. The Contractor shall not bill and DSHS shall not pay for services performed under this Contract, if the Contractor has charged or will charge another agency of the state of Washington or any other party for the same services.

5. **Compliance with Applicable Law.** At all times during the term of this Contract, the Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to, nondiscrimination laws and regulations.

6. **Confidentiality.**

a. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential

Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:

(1) as provided by law; or,

(2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.

b. The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the Confidential Information by:

(1) Allowing access only to staff that have an authorized business requirement to view the Confidential Information.

(2) Physically Securing any computers, documents, or other media containing the Confidential Information.

(3) Ensure the security of Confidential Information transmitted via fax (facsimile) by:

(a) Verifying the recipient phone number to prevent accidental transmittal of Confidential Information to unauthorized persons.

(b) Communicating with the intended recipient before transmission to ensure that the fax will be received only by an authorized person.

(c) Verifying after transmittal that the fax was received by the intended recipient.

(4) When transporting six (6) or more records containing Confidential Information, outside a Secured Area, do one or more of the following as appropriate:

(a) Use a Trusted System.

(b) Encrypt the Confidential Information, including:

i. Encrypting email and/or email attachments which contain the Confidential Information.
ii. Encrypting Confidential Information when it is stored on portable devices or media, including but not limited to laptop computers and flash memory devices.

Note: If the DSHS Data Security Requirements Exhibit is attached to this contract, this item, 6.b.(4), is superseded by the language contained in the Exhibit.

(5) Send paper documents containing Confidential Information via a Trusted System.

(6) Following the requirements of the DSHS Data Security Requirements Exhibit, if attached to this contract.

c. Upon request by DSHS, at the end of the Contract term, or when no longer needed, Confidential Information shall be returned to DSHS or Contractor shall certify in writing that they employed a DSHS approved method to destroy the information. Contractor may obtain information regarding approved destruction methods from the DSHS contact identified on the cover page of this Contract.

d. Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Confidential Information requiring special handling (e.g. protected health information) must be destroyed on-site through shredding, pulping, or incineration.

e. Notification of Compromise or Potential Compromise. The compromise or potential compromise of Confidential Information must be reported to the DSHS Contact designated on the contract within one (1) business day of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

7. **Debarment Certification.** The Contractor, by signature to this Contract, certifies that the Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions (Debarred). The Contractor also agrees to include the above requirement in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor becomes Debarred. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor becomes Debarred during the term hereof.

8. **Governing Law and Venue.** This Contract shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in Superior Court for Thurston County.

9. **Independent Contractor.** The parties intend that an independent contractor relationship will be created by this Contract. The Contractor and his or her employees or agents performing under this Contract are not employees or agents of the Department. The Contractor, his or her employees, or agents performing under this Contract will not hold himself/herself out as, nor claim to be, an officer or employee of the Department by reason hereof, nor will the Contractor, his or her employees, or agent make any claim of right, privilege or benefit that would accrue to such officer or employee.

10. **Inspection.** The Contractor shall, at no cost, provide DSHS and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located. These inspection rights are intended to allow DSHS and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.

11. **Maintenance of Records.** The Contractor shall maintain records relating to this Contract and the performance of the services described herein. The records include, but are not limited to, accounting procedures and practices, which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. All records and other material relevant to this Contract shall be retained for six (6) years after expiration or termination of this Contract.

Without agreeing that litigation or claims are legally authorized, if any litigation, claim, or audit is started before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

12. **Order of Precedence.** In the event of any inconsistency or conflict between the General Terms and Conditions and the Special Terms and Conditions of this Contract or any Program Agreement, the inconsistency or conflict shall be resolved by giving precedence to these General Terms and Conditions. Terms or conditions that are more restrictive, specific, or particular than those contained in the General Terms and Conditions shall not be construed as being inconsistent or in conflict.

13. **Severability.** If any term or condition of this Contract is held invalid by any court, the remainder of the Contract remains valid and in full force and effect.

14. **Survivability.** The terms and conditions contained in this Contract or any Program Agreement which, by their sense and context, are intended to survive the expiration or termination of the particular agreement shall survive. Surviving terms include, but are not limited to: Billing Limitations; Confidentiality, Disputes; Indemnification and Hold Harmless, Inspection, Maintenance of Records, Notice of Overpayment, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of Property.

15. **Contract Renegotiation, Suspension, or Termination Due to Change in Funding.**

If the funds DSHS relied upon to establish this Contract or Program Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, after the effective date of this contract but prior to the normal completion of this Contract or Program Agreement:

a. At DSHS's discretion, the Contract or Program Agreement may be renegotiated under the revised funding conditions.

b. At DSHS's discretion, DSHS may give notice to Contractor to suspend performance when DSHS determines that there is reasonable likelihood that the funding insufficiency may be resolved in a timeframe that would allow Contractor's performance to be resumed prior to the normal completion date of this contract.

(1) During the period of suspension of performance, each party will inform the other of any conditions that may reasonably affect the potential for resumption of performance.

(2) When DSHS determines that the funding insufficiency is resolved, it will give Contractor written notice to resume performance. Upon the receipt of this notice, Contractor will provide written notice to DSHS informing DSHS whether it can resume performance and, if so, the date of resumption. For purposes of this subsubsection, "written notice" may include email.

(3) If the Contractor's proposed resumption date is not acceptable to DSHS and an acceptable date cannot be negotiated, DSHS may terminate the contract by giving written notice to Contractor. The parties agree that the Contract will be terminated retroactive to the date of the notice of suspension. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the retroactive date of termination.

c. DSHS may immediately terminate this Contract by providing written notice to the Contractor. The termination shall be effective on the date specified in the termination notice. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination. No penalty shall accrue to DSHS in the event the termination option in this section is exercised.

16. **Waiver.** Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Contract. Only the CCLS Chief or designee has the authority to waive any term or condition of this Contract on behalf of DSHS.

Additional General Terms and Conditions – Interlocal Agreements:

17. **Disputes**. Both DSHS and the Contractor ("Parties") agree to work in good faith to resolve all conflicts

at the lowest level possible. However, if the Parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either Party may reduce its description of the dispute in writing, and deliver it to the other Party for consideration. Once received, the assigned managers or designees of each Party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Secretary of DSHS ("Secretary") and the Contractor's Agency Head ("Agency Head") or their deputies or designated delegates. Both Parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the Secretary and Agency Head.

Upon receipt of the referral and relevant documentation, the Secretary and Agency Head will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Secretary and Agency Head may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Secretary and Agency Head are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

The final decision will be put in writing, and will be signed by both the Secretary and Agency Head. If the Agreement is active at the time of resolution, the Parties will execute an amendment or change order to incorporate the final decision into the Agreement. The decision will be final and binding as to the matter reviewed and the dispute shall be settled in accordance with the terms of the decision.

If the Secretary and Agency Head are unable to come to a mutually acceptable decision, the Parties will request intervention by the Governor, per RCW 43.17.330, in which case the governor shall employ whatever dispute resolution methods that the governor deems appropriate in resolving the dispute.

Both Parties agree that, the existence of a dispute notwithstanding, the Parties will continue without delay to carry out all respective responsibilities under this Agreement that are not affected by the dispute.

18. **Hold Harmless**.

a. The Contractor shall be responsible for and shall hold DSHS harmless from all claims, loss, liability, damages, or fines arising out of or relating to the Contractor's, or any Subcontractor's, performance or failure to perform this Agreement, or the acts or omissions of the Contractor or any Subcontractor. DSHS shall be responsible for and shall hold the Contractor harmless from all claims, loss, liability, damages, or fines arising out of or relating to DSHS' performance or failure to perform this Agreement.

b. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.

19. **Ownership of Material**. Material created by the Contractor and paid for by DSHS as a part of this Contract shall be owned by DSHS and shall be "work made for hire" as defined by Title 17 USCA, Section 101. This material includes, but is not limited to: books; computer programs; documents; films; pamphlets; reports; sound reproductions; studies; surveys; tapes; and/or training materials. Material which the Contractor uses to perform the Contract but is not created for or paid for by DSHS is owned by the Contractor and is not "work made for hire"; however, DSHS shall have a perpetual license to use

this material for DSHS internal purposes at no charge to DSHS, provided that such license shall be limited to the extent which the Contractor has a right to grant such a license.

20. **Subrecipients**.

a. General. If the Contractor is a subrecipient of federal awards as defined by 2 CFR Part 200 and this Agreement, the Contractor shall:

(1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Catalog of Federal Domestic Assistance (CFDA) title and number, award number and year, name of the federal agency, and name of the pass-through entity;

(2) Maintain internal controls that provide reasonable assurance that the Contractor is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;

(3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;

(4) Incorporate 2 CFR Part 200, Subpart F audit requirements into all agreements between the Contractor and its Subcontractors who are subrecipients;

(5) Comply with the applicable requirements of 2 CFR Part 200, including any future amendments to 2 CFR Part 200, and any successor or replacement Office of Management and Budget (OMB) Circular or regulation; and

(6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to https://ojp.gov/about/offices/ocr.htm for additional information and access to the aforementioned Federal laws and regulations.)

b. Single Audit Act Compliance. If the Contractor is a subrecipient and expends $750,000 or more in federal awards from any and/or all sources in any fiscal year, the Contractor shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Contractor shall:

(1) Submit to the DSHS contact person the data collection form and reporting package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;

(2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a “Summary Schedule of Prior Audit Findings” reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.

c. Overpayments. If it is determined by DSHS, or during the course of a required audit, that the Contractor has been paid unallowable costs under this or any Program Agreement, DSHS may require the Contractor to reimburse DSHS in accordance with 2 CFR Part 200.

21. Termination.

a. Default. If for any cause, either party fails to fulfill its obligations under this Agreement in a timely and proper manner, or if either party violates any of the terms and conditions contained in this Agreement, then the aggrieved party will give the other party written notice of such failure or violation. The responsible party will be given 15 working days to correct the violation or failure. If the failure or violation is not corrected, this Agreement may be terminated immediately by written notice from the aggrieved party to the other party.

b. Convenience. Either party may terminate this Interlocal Agreement for any other reason by providing 30 calendar days' written notice to the other party.

c. Payment for Performance. If this Interlocal Agreement is terminated for any reason, DSHS shall only pay for performance rendered or costs incurred in accordance with the terms of this Agreement and prior to the effective date of termination.

22. Treatment of Client Property. Unless otherwise provided, the Contractor shall ensure that any adult client receiving services from the Contractor has unrestricted access to the client's personal property. The Contractor shall not interfere with any adult client's ownership, possession, or use of the client's property. The Contractor shall provide clients under age eighteen (18) with reasonable access to their personal property that is appropriate to the client's age, development, and needs. Upon termination of the Contract, the Contractor shall immediately release to the client and/or the client's guardian or custodian all of the client's personal property.

Special Terms and Conditions

1. Purpose and Duration

a. Background. The DSHS Research and Data Analysis Division (RDA) provides analytic services to DSHS programs and other state agency partners including the Department of Children, Youth, and Families (DCYF). RDA's analytic work on behalf of public programs generally relies on broad-based, legally authorized, secure access to identified administrative data, which is linked and organized in an Integrated Client Data Repository (ICDR) maintained by RDA. This Data Share Agreement supports the integration of DCYF data sources into the ICDR. The Agreement describes RDA's commitment to handle data securely, to use data appropriately, and to proactively engage DCYF in (a) approval of analytic activities using its data and (b) review of analytic products derived from its data. This agreement further describes DCYF's retention of full control over further disclosure of its data, in cases where external parties may seek to obtain extracts from the ICDR containing DCYF data.

b. Purpose. The purpose of this contract is:

(1) To establish a Data Share Agreement (DSA) between DSHS/RDA and DCYF to document the conditions for integration of DCYF data sources into the RDA ICDR.

(2) To establish the conditions under which RDA staff are authorized to use confidential DCYF Data, including child abuse and neglect Data subject to CAPTA, to perform Business Operations or Research activities on behalf of DCYF, or on joint behalf of DCYF, DSHS, and/or other state agency partners (e.g., the Health Care Authority).

(3) To establish the conditions under which DCYF Data housed in the ICDR may be disclosed outside of RDA, and how DCYF will control the use and disclosure process.

c. Scope. Other RDA DSAs describe access to and use of DCYF Data for (a) Client Registry, (b) surveys conducted by the RDA Management Information and Survey Research Section, and (c) other special project and infrastructure development activities. Data use and disclosure associated with these separately contracted activities are governed by the associated SLAs.

d. Period of Performance. This DSA is effective from the date signed, until termination. Either party may terminate this agreement with a minimum of 60 days advanced notice. The DSA may be amended by mutual agreement of the parties for additional terms.

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

a. "Analytic Extracts" are in Limited Data Set Format or are Identified Data Sets subject to Minimum Necessary requirements that are created from an Integrated Client Data Repository to address specific analytic needs of Authorized Users.

b. "Authorized User" means an employee or contractor of DSHS, HCA or DCYF, or other state agency or public health agency, or a student or faculty member of an institution of higher education, who has a legitimate business need to access the confidential information in a RDA Integrated Client Data Repository, is qualified to perform the requisite analyses, and is a party to a WSIRB Confidentiality Agreement for access to identified information for Research purposes, a contract with the Data Owners for access to identified information for Business Operations purposes, and/or an RDA Data Use Agreement for access to a Limited Data Set.

c. "Breach" means the acquisition, access, Use, Disclosure, or loss of Confidential Information in a manner not permitted by state and federal law, or non-compliance with the conditions of this agreement, associated contracts, or WSIRB Confidentiality Agreements.

d. “Business Operations” means non-research activities performed on behalf of DSHS, DCYF, or another state agency, and includes program evaluations, analytics, surveys, QA/QI, federal reporting and other activities in support of agency programs and/or administration. Business operations is used herein synonymously with health care operations as defined in 45 CFR 164.501.

e. “CAN” means child abuse and neglect incident information that are reported in FamLink and elsewhere in DCYF Data systems and are subject to restrictions in CAPTA.

f. “CAPTA” means the Child Abuse Prevention and Treatment Act, a federal statute that governs the confidentiality of CAN Data.

g. “Coded Data Standard” means that the investigators using the Limited Data Set cannot readily ascertain the identity of the individuals to whom the coded private information pertains because, for example, the investigators and the holder of the key enter into an agreement prohibiting the release of the key to the investigators under any circumstances. (Department of Health and Human Services, Office of Human Research Protections, “Coded Private Information or Specimens Used in Research, Guidance – 2008)

h. “Covered Entity” means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (45 CFR 160.103)

i. “Data” means the information that is disclosed or exchanged as described by this Data Share Agreement (DSA). For purposes of this DSA, Data means the same as “Confidential Information.”

j. “Data Owner” means the agency, or program within the agency, that supplies the data to RDA. Data Owner is used synonymously with Data Supplier.

k. “Data Repository” means a database or collection of databases that have been created or organized to facilitate the conduct of multiple research studies, including future studies not yet envisioned. It may also have been created for other purpose in addition to research, such as administrative and clinical purposes. (Washington State Institutional Review Board Procedures Manual)

l. “Data Use Agreement” means an agreement that meets the specifications in 45 CFR 164.514(e)(4) for disclosure of a Limited Data Set.

m. “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information (45 CFR 160.103)

n. “DSA” means this Data Share Agreement, also referred to as the Agreement.

o. “ICDR Data Marts” means analytic environments (SQL databases and file shares containing SAS data sets) containing multiple linked data tables designed to support a wide range of analytic activities including descriptive policy analysis, program evaluation, and predictive modeling. ICDR Data Mart tables are in a Limited Data Set Format and contain person-level records from which analysts can derive a longitudinal perspective on service utilization, outcomes, risk factors, residential location, and client demographics.

p. “Identified Data” means individual client level data that do not meet the HIPAA Limited Data Set Standard at 45 CFR 164.514(e)(2).

q. “Integrated Client Data Repository (ICDR)” means the Data Repository created by RDA and housed on secure servers at the Washington State Data Center. The ICDR has been created to facilitate efficient use of linked cross-program Data to support research and business operations activities on behalf of DSHS, DCYF and the other state agencies that supply the Data.

r. “Limited Data Set” is a Data Set in which the sixteen direct identifiers listed in the HIPAA Limited Data Set Standard (45 CFR 164.514(e)(2)) have been removed from the individual level records, and for which the recipient has signed a Data Use Agreement that meets the specifications in 45 CFR 164.514(e)(4) which prohibits the recipient from attempting to re-identify the individuals whose information is contained in the Limited Data Set. The records in a Limited Data Set are Non-Identified, but are considered Protected Health Information and are subject to Breach reporting requirements in Subpart D of 45 CFR Part 164. Limited Data Sets may be used only for research, public health and health care operations activities.

s. “Limited Data Set Format” means the sixteen direct identifiers listed in the HIPAA Limited Data Set Standard (45 CFR 164.514(e)(2)) have been removed from the individual level records. It does not imply that the recipient has signed a Data Use Agreement which prohibits the recipient from re-identifying the records in the data set. RDA analysts who need to update Data in a Limited Data Set Format may be given access to the identifier cross-walk file for that purpose.

t. “Minimum Necessary” means the least amount of Data necessary to accomplish the purpose for which the Data are needed.

u. “Non-Identified Data” means individual level client Data that contain personal, medical, health, cost, or service delivery information, but that exclude all of the sixteen direct identifiers in the HIPAA Limited Data Set Standard at 45 CFR 164.514(e)(2).

v. “On behalf of DCYF” means that DCYF has authorized the analytic activity through a Service Level Agreement, contract, Data Use Agreement, IRB Confidentiality Agreement, or written communication by an authorized representative of DCYF.

w. “Protected Health Information (PHI)” means individually identifiable health information that is created or received by a covered entity and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. (45 CFR 160.103)

x. “RDA” means the DSHS Research and Data Analysis Division which is part of the DSHS Hybrid Covered Entity when it performs covered functions on behalf of another covered entity or health care component of DSHS. (45 CFR 164.105)

y. “Receiving Party” means the Department of Social and Health Services Research and Data Analysis Division (DSHS/RDA).

z. “Research” means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. (45 CFR 46.102)

aa. “Use” means, with respect to individually identifiable health and other Confidential Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (45 CFR 160.103)

3. Roles and Responsibilities

a. The Receiving Party shall:

(1) Submit a research application to the Washington State Institutional Review Board (WSIRB) to establish an Integrated Client Data Repository (ICDR) that will contain linked, client-level Data across multiple DSHS, DCYF, and other state agency programs.

(2) Import identified, confidential, client-level Data from DCYF into RDA for inclusion in the ICDR under research disclosure authority documented in a legally-binding Confidentiality Agreement per RCW 42.48. The Data provided to RDA by DCYF programs that were formerly part of DSHS, remain unchanged.

(3) When required, write routines for creating ICDR Analytic Extracts with all direct identifiers removed, producing Limited Data Sets containing Non-Identified Data at the individual client level.

(4) Use the linked, cross-program Data in ICDR Limited Data Sets, or Identified Data, if authorized under the terms of this agreement, for a variety of Research and Business Operations purposes on behalf of DSHS, DCYF, and other state agency management.

(5) Disclose ICDR Limited Data Sets to non-RDA users using a defined protocol with disclosure review and approval authority shared by RDA and the Data Owners.

(6) Consult with DCYF regarding thresholds of activities using DCYF Data in the RDA Integrated Client Data Repository that must be reported to and authorized by the designated DCYF Administrator.

(7) Establish policies and procedures for managing, using and disclosing ICDR Analytic Extracts, including circumstances when Identified Data can be used and disclosed.

b. DCYF shall:

(1) Continue to provide RDA with access to identified, confidential, client-level Data in FamLink and other DCYF data systems using source systems approved under the terms of this agreement and mutually agreed upon data access and/or transfer protocols.

(2) Consult as needed with the RDA Director, RDA Deputy Director, and/or RDA Senior Research Managers if questions or concerns arise about the import, management, use and disclosure of DCYF Data housed in RDA Integrated Client Data Repository.

(3) Consult with RDA senior staff regarding the creation of customized ICDR Limited Data Sets and Analytic Extracts that meet the research and analytic needs of DCYF.

(4) Work with RDA to establish thresholds of activities using DCYF Data in the RDA Integrated Client Data Repository that must be reported to and authorized by the designated DCYF Administrator.

(5) Consult with the Washington State Institutional Review Board about the level of review required to conduct DCYF Research projects using linked Data housed in RDA Integrated Client Data Repository.

4. **Exhibit A – Data Security Requirements.** RDA shall protect, segregate, and dispose of data from DCYF as described in Exhibit A, and meet all other requirements specified in Exhibit A.

5. **Supremacy Clause**

In the event there is a conflict between this Agreement and any other Agreement executed between DSHS/RDA and DCYF, with regard to the contents of this Data Share Agreement, this Agreement shall control.

6. **Legal Authority for Data Sharing**

The following statutes and regulations provide authority for sharing these data: RCW 39.34, Interlocal Cooperation Act; RCW 42.48, Release of Records for Research, RCW 43.216, Department of Children, Youth, and Families; RCW 26.44.031(6), Records-Maintenance and Disclosure; 42 USC § 5106A(b)(2)(B)(viii)(VI), Child Abuse Prevention and Treatment Act; 45 CFR 205.50(a)(1)(i), Safeguarding Information for the Financial Assistance Programs.

7. **Data Classification**

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the Chief Information Officer. (See Section 4, *Data Security*, of *Securing IT Assets Standards* No. 141.10 in the *State Technology Manual* at **http://ofm.wa.gov/ocio/policies/manual.asp**)

The Data that is the subject of this DSA is classified as indicated below:

☐ Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

☐ Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

☒ Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

Personal Information about individuals, regardless of how that information is obtained.

Information concerning employee personnel records.

Information regarding IT infrastructure and security of computer and telecommunications systems.

☒ Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.

Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

8. **General Constraints on Use of the Data**

a. This Agreement does not constitute a release of the DCYF Data for the Receiving Party's discretionary use. Receiving Party may use the Data accessed under this DSA only to carry out the purposes and permitted uses described herein (See: Sections 1, 8, and 9). Any other use of the DCYF Data is not permitted without prior written permission from DCYF.

b. The Receiving Party, DCYF, other state agencies, and public health agencies, and their contractors, authorized to use (i.e., Authorized Users) Analytic Extracts from the RDA Integrated Client Data Repository shall use the Data only to perform research, public health, or business operations activities in the normal course of business.

c. The Receiving Party, DCYF, other state agencies, and public health agencies, and their contractors, authorized to use (i.e., Authorized Users) Analytic Extracts from the RDA Integrated Client Data Repository may not re-disclose the Confidential Information to any other party for any other purpose unless specifically authorized by this Data Share Agreement or by the written authorization of the Data Owners.

d. Any reports written by the Receiving Party, DCYF, other state agencies, and public health agencies, and their contractors, using Analytic Extracts from the RDA Integrated Client Data Repository shall include only aggregate Data about clients. No identifying client information may be reported or otherwise released to any unauthorized persons. All reports based on the RDA Integrated Client Data Repository must conform to DOH Guidelines for Working with Small Numbers.

e. All requests for use or disclosure of RDA Integrated Client Data Repository Analytic Extracts for research or evaluation purposes must be submitted to the Washington State Institutional Review Board (WSIRB). If WSIRB determines a formal IRB review is required, a written Research Application must be submitted and approved by the WSIRB, and a legally-binding Confidentiality Agreement must be established between the person(s) requesting the Analytic Extracts and the Data Owners, before any Data will be disclosed. Questions about whether a proposed activity constitutes research shall be referred to WSIRB for review and determination. It is expected that most uses by RDA staff of DCYF data will be business operations activities not subject to WSIRB review.

f. The Minimum Necessary standard in 45 CFR 164.514(d) applies to all Data used and disclosed under this Agreement. ICDR Analytic Extracts are by default disclosed in Limited Data Set configuration, but Identified Data Sets may be used or disclosed if necessary to perform the work and if appropriate legal authority is documented. Separate project SLAs may establish the legal authority for data to be used in an identified form to support DCYF business operations. Final decisions on whether identified ICDR extracts can be used or disclosed for a proposed activity will be made by the Data Owners.

g. Substance use disorder (SUD) Data subject to 42 CFR Part 2, mental health services (MH) Data subject to RCW 70.02.230-240, and child abuse and neglect Data (CAN) subject to the Child Abuse Prevention and Treatment Act (CAPTA; 42 USC § 5106A) may only be used or disclosed for Business Operations purposes under contract with and on behalf of the Data Owners. For purposes of this Agreement, all DCYF Child Welfare Data are considered to be subject to CAPTA, unless DCYF explicitly states otherwise in writing.

h. HCA ProviderOne Data in the RDA Integrated Client Data Repository are Protected Health Information (PHI). When PHI is linked to non-PHI, the entire linked record is subject to HIPAA requirements. ICDR Analytic Extracts that contain PHI may only be disclosed for Business Operations purposes in a Limited Data Set with SUD/MH/CAN Data redacted unless the activity is being performed under contract with and/or on behalf of the Data Owner (HCA). This restriction does not apply to DSHS use of HCA PHI for Business Operations which is authorized in 45 CFR 164.506(c)(4).

i. The Receiving Party will maintain a current Authorized User list of the names and email addresses of all employees of the Receiving Party, DCYF, other state agencies or public health agencies, and their contractors, who have been given access to RDA Integrated Client Data Repository Analytic Extract files. This list will be reviewed at least twice annually to verify that all persons continue to require access to the ICDR Analytic Extract files. Access by external parties to DCYF data in the ICDR will be limited to entities authorized by DCYF to have such access, through a legally-binding Confidentiality Agreement or another contractual vehicle.

j. The Receiving Party will provide DCYF with an annual report that cumulatively lists each project, person, and/or organization by or to whom RDA Integrated Client Data Repository Analytic Extracts containing DCYF Data have been Used or Disclosed. The report will summarize the nature of the project and the purpose of the disclosure, will indicate whether the records disclosed were in Limited Data Set Format or identified, and whether they were subject to special disclosure restrictions in 42 CFR Part 2, RCW 70.02.200-240, and/or CAPTA.

9. **Statement of Work.** RDA 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. Project or Task Objectives:

RDA is reorganizing its data environment by overlaying a data repository infrastructure on the foundational linked data stores and databases in RDA (e.g., the Client Services Database and Client Outcomes Database). The resulting Integrated Client Data Repository will provide greater protection for the highly confidential and sensitive Data RDA manages, will maintain compliance with applicable statutes and regulations, and will facilitate efficient use of linked cross-program Data to support research and business operations activities on behalf of DSHS and the state agencies that supply the Data. In addition to the foundational linked databases, the ICDR may encompass a series of specialized repositories created for specific users or purposes. All the repositories will employ the same methods and procedures for access, use and disclosure that are defined in this DSA.

b. How Analytic Extracts from the Integrated Client Data Repository are managed and configured:

(1) RDA access to direct identifiers in the RDA Integrated Client Data Repository is limited to a defined group of staff administering the Data Repository, creating extracts from source Data systems, creating and updating Analytic Extracts, performing Data security and archival functions, and/or performing Business Operations activities on behalf of Data Owners. Enterprise IT staff have access to servers storing direct identifiers in the RDA ICDR to perform system administration, security, and related functions.

(2) The primary ICDR Data Marts created to support RDA Business Operations activities will be in a Limited Data Set Format with direct identifiers removed. Identified Data Sets may be used or disclosed if necessary to perform the work and if appropriate authorizations are documented. Identifier cross-walk files with restricted access contain the information needed to re-identify Analytic Extracts in Limited Data Set Format. Staff need to access identifier cross-walk files will be assessed separately from need to access ICDR data sets in a Limited Data Set Format. RDA analysts who need to update Data in a Limited Data Set Format may have access to the identifier cross-walk file for that purpose.

(3) ICDR Analytic Extracts that are disclosed to non-RDA requestors will generally be Limited Data Sets unless the Data Owners authorize disclosure of Identified Data Sets. Limited Data Sets created by RDA may include an encrypted code that allows re-identification of the Limited Data Set records by select RDA staff, but not by the person who is the recipient of the Limited Data

Set and has signed the RDA Data Use Agreement.

c. Use and Disclosure of ICDR Analytic Extracts containing DCYF Data:

(1) Internal RDA use of ICDR Analytic Extracts for Business Operations

(a) RDA use of DCYF Data for Business Operations conducted at the request of DCYF may be authorized by a Service Level Agreement or contract with DCYF, or written approval (e.g., email) from an authorized representative of DCYF.

(b) RDA use of DCYF Data for Business Operations initiated at the request of agencies other than DCYF may be authorized by a contract between the requestor, RDA and DCYF, or written approval (e.g., email) from an authorized representative of DCYF.

(c) RDA staff shall submit analytic products created by Business Operations or Research activities using DCYF Data to DCYF prior to publication. RDA will summarize Business Operations and Research activities that use ICDR Analytic Extracts in an annual report to WSIRB and to the Data Owners.

(2) Disclosure of ICDR Analytic Extracts to Users External to RDA for Business Operations

(a) Disclosure of an ICDR Analytic Extract is authorized by an executed Data Share Agreement or similar agreements between the requestor and the Data Owner(s). All persons external to RDA requesting disclosure of an ICDR Analytic Extract must submit an ICDR Data Request Form (Exhibit B) to the RDA Analytic Information Governance Administrator and to the Data Owner(s) for preliminary review of the request. If the recipient of an ICDR analytic extract receives DCYF data in a Limited Data Set, the recipient must sign an RDA Data Use Agreement that prohibits re-identification of the LDS records.

(3) Research

(a) All requests to Use or Disclose an ICDR Analytic Extract for research or evaluation purposes must be submitted to the WSIRB.

(b) Approval of Research Requests. If the research activity requires a full WSIRB review, execution of a Confidentiality Agreement is required to authorize Use or Disclosure of an ICDR Analytic Extract containing DCYF data for research.

10. Data Sharing

a. Purpose

(1) Activity for which Data is needed: The Receiving Party needs the requested Data to construct an Integrated Client Data Repository that will contain linked, individual-level Data about clients receiving public benefit services from DSHS, DCYF, and other state agencies.

(2) How Data Recipient will use Data: The Receiving Party, DCYF, other state agencies and public health agencies, and their contractors, authorized to use Analytic Extracts from RDA Integrated Client Data Repository will use the Confidential Information only to perform research, public health, or business operations activities in the normal course of business.

b. Description of Data

(1) Data Elements: The Receiving Party requests access to all Data included in Exhibit D, DCYF Data Elements, and in Exhibit E, IN19 Client Services Interface Data. DCYF may provide RDA with access to additional data sources and data elements to conduct analyses to support DCYF business operations. Authorization for access to DCYF client data not included in Exhibits D and E must be provided in writing by an authorized representative of DCYF. All requirements for data security, use, access, disclosure, and linkage will apply to data authorized through this process.

(2) Time frames for Data disclosure or exchange: Access to DCYF Databases listed in Exhibit D is continuous. Exhibit E identifies eight IN19 files sent monthly.

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

Individual level client Data from DCYF will be linked to client level data from the Health Care Authority (HCA), from DSHS Administrations, and from other state agencies to construct the RDA Integrated Client Data Repository.

c. Data Access or Transfer:

(1) Method: DCYF Databases: SQL to SQL data replication which is maintained by DCYF. IN19 files: Monthly FTP via the ESB.

(2) Requirements for access: RDA requests access to DCYF Data via email to the Administrator for Data & Reporting.

(3) Frequency of Exchange: DCYF Databases: Exhibit D data tables are refreshed weekly. Exhibit E IN19 files are transmitted monthly.

d. HIPAA Compliance and Breach Notification

RDA and DCYF agree that the RDA Integrated Client Data Repository contains Protected Health Information (PHI) and that Analytic Extracts from the Integrated Client Data Repository must be treated as PHI in compliance with the requirements in HIPAA Rules. RDA shall report any potential Breaches of PHI or other Confidential Information or other violations of HIPAA Rules to the Enterprise Technology Operations Center (ETOC) at ETOC@dshs.wa.gov and to the DCYF Privacy Officer at dcyf.privacyofficer@dcyf.wa.gov, Security Contact at chris.martin@dcyf.wa.gov, and DCYF primary contract contact within 1 business day of becoming aware of the potential violation. For Breaches involving over 500 individuals, or potentially over 500 individuals, RDA must also notify the DSHS Privacy Officer at DSHSprivacyofficer@dshs.wa.gov.

11. Billing Procedures and Payment

Some costs incurred to administer the RDA Integrated Client Data Repository will be recovered in separate agreements negotiated with partner agencies that will use Analytic Extracts generated by the repository.

12. Governance

Data governed by this Data Share Agreement are disclosed to RDA under DSHS Research Application 2019-103. This research application was submitted to obtain WSIRB approval to construct and maintain the RDA Integrated Client Data Repository, and to authorize Data Owners to disclose confidential data to the ICDR under research disclosure authority in RCW 42.48. Authority for DCYF to disclose their Data to RDA for this purpose will continue as long as DSHS Research Application 2019-103 remains in active status with the WSIRB and the terms of the Confidentiality Agreement are satisfied

13. Contacts for Notice

a. The primary program contact for this Contract for DSHS shall be:

Lareina La Flair, Research Manager
DSHS Research and Data Analysis Division
360 902-0712
lareina.laflair@dshs.wa.gov

b. The primary program contact for this Contract for DCYF shall be:

Tammy Cordova, Data and Reporting Administrator
DCYF Office of Innovation, Alignment, and Accountability
1500 Jefferson St. SE, Olympia, WA 98504
Phone: (360) 701-0211
E-mail: tammy.cordova@dcyf.wa.gov

14. Disputes – Both parties agree to work in good faith to resolve all conflicts at the lowest level possible. However, if the parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either party may reduce its description of the dispute in writing, and deliver it to the other party for consideration. Once received, the assigned managers or designees of each party will work to informally and amicably resolve the issue within five (5) business days. If the managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Secretary of DSHS and the Secretary of DCYF, or to their deputy or designated delegate. Both parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the DSHS Secretary and the DCYF Secretary.

Upon receipt of the referral and relevant documentation, the DSHS Secretary and DCYF Secretary will confer to consider the potential options for resolution, and to arrive at a decision within fifteen (15) business days. The DSHS Secretary and DCYF Secretary may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the DSHS Secretary and the DCYF Secretary are unable to come to a mutually acceptable decision within fifteen (15) days, they may agree to issue an extension to allow for more time.

Both parties agree that, the existence of a dispute notwithstanding, the parties will continue without delay to carry out their respective responsibilities that are not affected by the dispute under the Cooperative Agreement or applicable SLA(s).The final decision will be put in writing and will be signed by both the DSHS Secretary and DCYF Secretary. If the Cooperative Agreement is active at the time of resolution and amendment of the Agreement is warranted for ongoing clarity, the parties will execute an amendment to incorporate the final decision into the Agreement. If this dispute process is used, the resolution decision will be final and binding as to the matter reviewed and the dispute shall be settled in accordance with the terms of the decision. If the foregoing process does not result in resolution of the dispute, either party may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor’s process shall control.

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.

Exhibit B

RDA Integrated Client Data Repository (ICDR)
Data Request Form

Under terms of RDA Data Share Agreements with the Washington State Agencies that own the data, employees of State Agencies, public health agencies, academic institutions, and their contractors, who have legitimate research or business/health care operations needs and relevant analytic qualifications may request disclosure and use of ICDR Analytic Extracts.

ICDR Analytic Extracts are by default in Limited Data Set format with all direct identifiers removed per 45 CFR 164.514(e), and may be used only for research, public health or business/health care operations purposes. As a condition for receiving an ICDR Limited Data Set, your organization is required to establish a Data Use Agreement with RDA.

Please complete all fields in this Data Request Form and submit it to: RDA Analytic Information Governance Administrator. If you have questions about how to complete this form, call the RDA Analytic Information Governance Administrator at: 360 902-0712.

REQUESTOR INFORMATION	
Requestor Name:	Job Title:
Business Phone:	Business Email:
Name of Organization:	Is Your Organization a Covered Entity? Yes □ No □ Don’t Know □
Will a Contractor require access to the requested data? Yes □ Contractor’s Name: No □	Lead Contractor: Business Phone: Business Email:
At the end of this form list all individuals, including IT and contractor staff, who would be given access to the data being requested. These individuals must sign and submit to the RDA Analytic Information Governance Administrator the DSHS Nondisclosure of Confidential Information (DSHS 03-374B). Employees of Washington State Agencies are not required to sign DSHS 03-374B.	
DETAILS OF THE REQUEST	
Project Title:	
Provide a detailed statement of the purpose of the proposed activity:	
Provide a brief summary of the methods used in the proposed activity:	
Please attach a list of requested data elements and descriptions and identify the State Agencies and/or DSHS Administrations that own the data: **This is a request for:** New data □ Modification of existing data □ Access to existing data □ Other □ If Other, please explain:	

The data you are requesting would be used for:
Research ☐ Program Evaluation ☐ Business or Health Care Operations ☐ Other ☐ If Other, please explain:

The proposed analyses will be performed on behalf of one or more Data Owners: Yes ☐ No ☐ If yes, specify:

The proposed analyses will be done under contract with a Washington State Agency: Yes ☐ No ☐
If Yes, specify with whom, and provide the name and contact information for the contract administrator:

Does your request include the following restricted data?	**Yes**	**No**	**Don't know**
Physical health services (PHI):	☐	☐	☐
Substance use disorder Tx (PHI):	☐	☐	☐
Mental health services or Tx (PHI):	☐	☐	☐
Health care data on STD services or TX (PHI):	☐	☐	☐
Data on incidents of child abuse and neglect:	☐	☐	☐
Data on children in out-of-home placement:	☐	☐	☐
Non-public Vital Records data:	☐	☐	☐
Criminal justice system non-conviction data:	☐☐	☐	
Education Data subject to FERPA:	☐	☐	☐

Will a Limited Data Set meet the needs of your request? Yes ☐ No ☐ Don't Know ☐
If No, explain why identified data are necessary, and identify the legal authority for the use of identified data:

Disclosure of identified data requires a contract or data share agreement with each Washington State Agency data owner.

Please note you are required to sign a Data Use Agreement as a condition for receipt of a Limited Data Set. This Data Use Agreement requires that your organization has appropriate safeguards in place to prevent inappropriate use or disclosure of the information in the Limited Data Set. The minimum data security standards your organization must have in place are specified in the attached Data Security Standards Exhibit.

By submitting this form to the RDA Analytic Information Governance Administrator, I attest that the information provided is accurate and complete to the best of my knowledge.

LIST ALL INDIVIDUALS WHO WILL HAVE ACCESS TO THE ICDR DATA SETS

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Name:______________________________

Organization:______________________________

Business Email:______________________________

Please insert additional pages if needed.

Exhibit C

RDA Data Use Agreement

Washington State
Department of Social and Health Services
Research and Data Analysis Division

This Agreement is entered into by and between the Washington State Department of Social and Health Services, Research and Data Analysis Division (“RDA”), the Data Owner(s), the Requestor (“Requestor”), and individuals named on Attachment A (attached hereto and incorporated herein) as of the Effective Date noted on Attachment A.

RDA is providing Protected Health Information (“PHI”) and/or other confidential information in the form of a Limited Data Set to the Requestor for the purpose(s) specified in Attachment A. In compliance with the Health Insurance Portability and Accountability Act and regulations promulgated thereto (collectively “HIPAA”), and with other statutes and regulations[1] governing the access, use and disclosure of confidential client information, RDA is required to obtain assurances from Requestor that Requestor will only use or disclose PHI and/or confidential information as permitted herein. The parties enter into the Agreement as a condition for RDA furnishing a Limited Data Set to Requestor, and as a means of Requestor providing the assurances about use and disclosure. The provisions of the Agreement are intended to meet the Data Use Agreement requirements of HIPAA.

NOW, THEREFORE, the parties agree as follows:

1. **Definitions**. Each capitalized term used in this Agreement and not otherwise defined, shall have the meaning given it in HIPAA.
2. **Term**. This Agreement shall commence on the date signed by the Data Owner(s) and continue until terminated in accordance with Section 5, below.
3. **Prohibition**. This Agreement between the Requestor and RDA prohibits RDA from releasing the key needed to re-identify the Limited Data Set records to the Requestor under any circumstances.
4. **Requestor’s Obligations**. Requestor shall:
   a. Use and disclose the PHI and/or other confidential information in the Limited Data Set provided by RDA only for the purpose identified in Attachment A, or as otherwise required by law, and for no other purposes.
   b. Use and disclose the PHI and/or other confidential information in the Limited Data Set provided by RDA only among the individuals listed in Attachment A.
   c. Use appropriate administrative, physical, and technical safeguards to prevent use or disclosure of the PHI and/or other confidential information in the Limited Data Set other than as provided in this Agreement.
   d. Assure that the use of Limited Data Set(s) disclosed under this Agreement complies with all requirements in the DSHS Information Security Standards Exhibit, attached to this Agreement, and to the corresponding Security Standards of the other agencies that may own the data.
   e. Immediately report to the RDA Analytic Information Governance Administrator any use or disclosure, or potential use or disclosure, of the PHI and/or other confidential information in the Limited Data Set(s) provided by RDA other than as expressly permitted by this Agreement.
   f. Ensure that all the Requestor’s employees, agents and/or contractors to whom the Requestor provides or intends to provide the PHI and/or other confidential information in the Limited Data Set provided by RDA are identified in Attachment A, sign the DSHS Agreement on Nondisclosure of Confidential Information (DSHS 03-374B) or equivalent Washington State Agency form, and comply with all restrictions and conditions specified in this Agreement.
   g. Not identify or attempt to identify individuals whose PHI and/or other confidential information included in the Limited Data Set provided by RDA, nor contact or attempt to contact any of the individuals whose information is contained in the Limited Data Set.
   h. Not link or attempt to link the PHI and/or other confidential information in the Limited Data Set provided by RDA with any other individual level information from other sources.

[1] Including but not limited to USC § 5106A(b)(2)(B)(viii)(VI), RCW 70.02, 42 CFR Part 2.

i. Not use or disclose more PHI and/or other confidential information than the minimum necessary to allow its employees or contractors to perform their functions pursuant to the purpose identified in Attachment A.

j. Not publish or disseminate any findings or reports based on analyses of the Limited Data Set provided by RDA before submitting those findings and reports for review by RDA and the Data Owners.

k. Indemnify, defend and hold harmless from all costs and expenses (including attorney's fees) for any claims that relate to a release of PHI and/or other confidential information or that relate to a breach of Requestor's obligations under this Agreement.

5. **Termination.** This Agreement terminates five years from the Effective Date in Attachment A. The Requestor may submit written requests for extensions of this Agreement for a period of an additional two years if work needed to complete the purpose of the request is not finished. RDA may terminate this Agreement upon 10 days notice to Requestor, if Requestor violates or breaches any material term or condition of this Agreement. RDA may terminate this Agreement without cause upon 30 days written notice. **Upon** termination, Requestor shall promptly return or destroy all copies and derivatives or subsets of the Limited Data Set provided by RDA and certify to RDA and the Data Owners that this requirement has been satisfied. If return or destruction of the Limited Data Set is not feasible, the Requestor shall make such alternative disposition of provided and derived information as directed by RDA and the Data Owners. The exercise of remedies pursuant to this section shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

6. **Governing law and Venue.** This Agreement shall be governed by the laws of the State of Washington. Venue for any claim, **action**, or suit, whether state or federal, between Requestor and RDA shall be Thurston County, Washington.

To be Completed by the RDA Analytic Information Governance Administrator:

RDA Assessment of Data Request:

This activity is for: Research ☐ Program Evaluation ☐ Business Operations ☐
If this is a Business Operations activity conducted by DSHS, HCA or DCYF, is the activity being conducted "on behalf" of the Data Owner(s)? Yes ☐ No ☐ NA ☐
If this is a Business Operations activity conducted by a Non-DSHS/HCA/DCYF entity, is the activity being conducted under contract with the Data Owner(s)? Yes ☐ No ☐ NA ☐

By signing this DUA the Data Owner(s) concur with the assessment above and provide permission for RDA to use or disclose the Limited Data Set as described in the attached Data Request Form.

SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Agreement effective on the Date signed by the Data Owner(s).

Research and Data Analysis:	**Requestor:**
Name: ______________________________	Name: ______________________________
Signature: ___________________________	Signature: ___________________________
Title: _______________________________	Title: _______________________________
Organization: ________________________	Organization: ________________________
Date: _______________________________	Date: _______________________________

Data Owner: HCA ☐ DCYF ☐ DSHS ☐

Name: ________________________________

Signature: _____________________________

Organization: __________________________

Title: _________________________________

Date: _________________________________

Data Owner: HCA ☐ DCYF ☐ DSHS ☐

Name: ________________________________

Signature: _____________________________

Organization: __________________________

Title: _________________________________

Date: _________________________________

Data Owner: HCA ☐ DCYF ☐ DSHS ☐

Name: ________________________________

Signature: _____________________________

Organization: __________________________

Title: _________________________________

Date: _________________________________

Data Owner: HCA ☐ DCYF ☐ DSHS ☐

Name: ________________________________

Signature: _____________________________

Organization: __________________________

Title: _________________________________

Date: _________________________________

Attachment A

(Attach the complete ICDR Data Request Form)

Exhibit D

DCYF Data Elements

(Defined by Data Source and Table Name)

JRAODS

AssessmentSource
BackupDate
CRB_BadCountyObligations
CRB_ObligationStaging
CRB_PhysicalLocationStaging
CRBCountyLocationsHistory
CRBCountyLocationsYesterday
CRBCountyProgramAllOffensesHistory
CRBCountyProgramAllOffensesYesterday
CRBCountyProgramHistory
CRBCountyProgramTransferHistory
CRBCountyProgramTransferYesterday
CRBCountyProgramYesterday
CRBFlatFileAllOffenses
CRBFlatFileCaseManager
CRBFlatFileClientRelationship
CRBFlatFileCountyLocations
CRBFlatFileCountyProgramTransfer
CRBFlatFileLocation
CRBFlatFileMentalHealth
CRBFlatFileStaging
CRBObligation
CRBOffense
CRBParoleAllOffensesHistory
CRBParoleAllOffensesYesterday
CRBParoleCaseManagerHistory
CRBParoleCaseManagerYesterday
CRBParoleClientRelationshipHistory
CRBParoleClientRelationshipYesterday
CRBParoleHistory
CRBParoleMentalHealthHistory
CRBParoleMentalHealthYesterday
CRBParoleYesterday
CRBPhysicalLocation
CRBRaimuAssessment
CRBResHistoricalMinMaxRelease
CRBResidentialAllOffensesHistory
CRBResidentialAllOffensesYesterday
CRBResidentialCaseManagerHistory

CRBResidentialCaseManagerYesterday
CRBResidentialClientRelationshipHistory
CRBResidentialClientRelationshipYesterday
CRBResidentialHistory
CRBResidentialMentalHealthHistory
CRBResidentialMentalHealthYesterday
CRBResidentialYesterday
CustomReportFlatFile
JRAMentalHealth
ResHistoricalReleaseIDs
DimDate

JRAProd

Form
FormToObligation
FormToRecurrenceType
Rating
RatingType
RecurrenceType
RoleToOrganization
Summary
TraumaSymptom
TraumaSymptomQuestionType
TraumaticExperience
TraumaticExperienceQuestionType
ClientToOrganization
CountyPrograms
CourtAction
CourtActionToObligation
CourtActionToOffense
DischargeDetails
Jurisdiction
Obligation
ObligationTestingRequired
ObligationToClientToOrganization
Offense
PersonAddress
ResidentialSentence
ResidentialSentence_Adjustment
ResidentialSentence_PriorOffense
SWS
VersionToObligationAttachRules
Attachment
Axosoft
AxosoftService
AxosoftServiceToActModule
HelpRequest

HelpRequestToClient
HelpRequestToDeveloper
HelpRequestToStatus
HelpRequestToWorkAround
menuItemToBugItem
Narrative
WorkAround
ClientRelationship
Module
ModuleClientRelated
ModuleStaffRelated
ModuleToObligation
ModuleToOverride
OrphanModule
Response
ResponseDateTime
ResponseInteger
ResponseModule
ResponseNarrative
ResponseOrganization
ResponsePerson
__RefactorLog
aaaDOCNumbers
aaaDuplicateClient
aaaFacilityGender
aaaoblg
AAAParoleObligation
aaaSavyAudit
aaaSavyPartTwo
aaAxosoft
AAAYOPTxOpportunities
aaCFC
aadr334Match
aadr344
aaICD
aaJuvisDOBMatch
aaJuvisLeadingZero
aaJuvisOnly
aaMissingJRANumber
aaNotificationToLocation
aaOffense
aaParoleDays
AAParoleObligation
aaPossibleClientDuplicates
aaPropertyCrimes
aaRarLevelStudy
aaSealedRecords

aaUWObligation
ACDADiagnosis
ACDADrugHistory
ACDADrugHistoryToDrug
ACDADrugUseDetails
ACDAPolysubstanceHistory
ACDAPolysubstanceKeybroker
ActModuleDependencies
ACTSystemOutage
ACTUser
ActUserTemplate
ActUserTemplateToBusinessRoles
ADPHistoryTable
AggregatedProcedureUsage
ApplicationUserHistory
AuditAfterDischargeAccess
AuditOutsideCaseloadAccess
AuditReportPrinted
AuditReportViewed
AuditUserAccess
BadClientStatus
BadObligationNotificationRequired
BadObligationTestingRequired
BarCode
BCA
BCAToTargetBehaviorVersion
BoxNumber
bug.menuItemToBugItem
CaseNote
CaseNoteClientAttendance
CaseNoteDetail
CaseNoteNarrative
CaseNotePersonAttendance
CaseNoteRTMClientToPerson
CaseNoteRTMClientToStaff
CaseNoteStaffAttendance
CaseNoteToDomainNarrative
CaseNoteToObligation
CaseNoteToReentryPlan
CATSCFIncidents
CERDAdjustment
cfcAssessmentData
cfcAssessmentOutcome
CfcCase
CfcDOCFirearmOffenders
CfcOffense
CfcOffenseCodeLUT

CfcPerson
CfcPrior
Client
ClientBirthPlace
ClientCulture
ClientEmployer
ClientHandout
ClientHandoutToCaseNote
ClientRecoICDRetention
ClientRegistryTransfer
ClientRoom
ClientsNotAttendingGroup
ClientToPerson
CommonModuleToARI
CommonModuleToCFIR
CommonModuleToIR
CommunityFacilityEligibility
CommunityPlacementEligibleObligation
CourtActionToOffense
CPSPerson
CPSPersonDetail
CPSPersonIDToModuleID
CPSPersonToPerson
CPSPersonToPersonToClientToPerson
CSDB_PA1_Address
CSDB_PC1_PersonCase
CSDB_PPE_People
CSDB_PPI_AlternateID
CSDB_PPN_PersonName
CSDB_PPR_PersonRace
CSDB_PS4_ServiceSpan
CSDB_PSV_ServiceDefinition
CSDBIDTable
DataDictionary
DataIntegrityErrors
DiagnosticPacket
DiagnosticPacketToScannedDocumentType
DiaryCaICDReview
DomainNarrative
DomainNarrativeToTransitionItem
DVR
DVROrientation
DVROutcome
DVRReferral
DVRService
DynamicADPColumns
DynamicCountyPgmRosterCheckedColumns

DynamicCountyPgmRosterColumns
DynamicRosterCheckedColumns
DynamicRosterColumns
EnhancementRequestRanking
FamilyLink
Gang
GangAffiliation
GangToGangRelationship
Homeless
HomelessNote
HomePageToMenu
HomePageToStaff
HomePageToUser
HomePageToUserType
InvalidPersonName
IRStaffRestrictedAccess
ITADomainScores
ITMCaseNote
ITPToTargetBehavior
JR_1906
JRAddress20160524_outScrubbed
JRAMentalHealth
JRANumber
JRAStage_Error
JuvisNumber
MandatedCERD
Modules
MultifactorAuthenticationFingerprint
MultiFactorPIN
NextWarrantNumber
Note
ObligationToClientToOrganization
ObligationToPhysicalLocation
OffenderIDRequestDolRecipient
OriginalPersonAddress
OrphanCaseNote
OverrideToCERDAdjustment
OverrideToMandatedCERD
ParHistoryTypeTable
PBSErrorTracking
PBSSent
PendingDOCSentence
PersonAddressValidation
PersonName
PhysicalLocationNarrative
PhysicalLocationToAppointmentScheduleDates
PhysicalLocationToClientFamilyStatus

PhysicalLocationToClientStatus
PhysicalLocationToClientToOrganization
PhysicalLocationToClientToStaff
PhysicalLocationToDeadTime
PhysicalLocationToJurisdiction
PhysicalLocationToMAR
PhysicalLocationToObligation
PhysicalLocationToObligationSupervisionLevel
PhysicalLocationToSanction
PhysicalLocationToSSS
PriorityManager
ProcAudit
ProcedureUsage
ProcedureUsagePerDay
ProcsFromSystem
ProposedCFRules
RACF
RACFAll
RAIMU
RARFemale
RARM
RARMale
ReentryPlan
ReentryPlanToDomainNarrative
ReentryPlanToObligation
ReleaseDate
ReleaseDateToOrganization
ReportingServicesCRBUsage
ReportingServicesUsage
ResidentContactsToFamilyMember
Restitution
RestitutionPayment
RevokeToRecommit
RTMCaseNote
SAS
ScrubbedAddress
ServicePlan
ServicePlanFFTInfo
ServicePlanParole
ServicePlanParoleStatus
ServicePlanProvider
ServicePlanScreenOut
SOGIE
SSA
SSN
SSS
StaffTalk

StaffTalkComment
StaffTalkCommentToTransitionItem
StaffTalkContact
StaffTalkFlag
Subscription
SubscriptionCaseload
SubscriptionClient
SubscriptionModule
SubscriptionOrg
SubscriptionStaff
SubstanceAbuseTx
TargetBehavior
TargetBehaviorVersion
TaskBusinessRole
TaskOrganization
TransitionContributor
TransitionItem
TransitionItemType
TransitionReport
TreatmentPlanCaseNoteDetail
TreatmentPlanCaseNoteToTargetBehaviorVersion
TreatmentPlanCaseNoteToTreatmentPlanGoal
TreatmentPlanCaseNoteToTreatmentPlanGoalVersion
TreatmentPlanGoal
TreatmentPlanGoalVersion
TreatmentPlanHomeworkAssignment
TreatmentPlanHomeworkReview
TreatmentPlanMotivation
TRN_ActUserRole
TRN_ActUserRole_History
TRN_Address
TRN_Address_Domestic
TRN_ApplicationUser
TRN_ApplicationUserRole
TRN_ARI
TRN_ARI_Legal_Requirements
TRN_ARI_Media_Involvement
TRN_ARI_Parole_Incident_Characteristics
TRN_ARI_Parole_Incident_Characteristics_To_TRN_ARI_Incident_Type
TRN_ARI_Parole_Youth_Information
TRN_ARI_Residential_Incident_Characteristics
TRN_ARI_Residential_Incident_Characteristics_To_TRN_ARI_IncidentType
TRN_ARI_To_Client
TRN_ARI_To_Community_Facility_Incident_Reports
TRN_ARI_To_Incident_Reports
TRN_BCA
TRN_BCA_Audit

TRN_Caching_TableManifest
TRN_CDP_Data
TRN_CFIR
TRN_CFIR_Narrative
TRN_CFIR_Notifications
TRN_CFIR_Sanctions
TRN_Client_AlternateIdentification
TRN_Client_AlternateName
TRN_Client_Death
TRN_Client_Marks
TRN_Client_PhysicalAttributes
TRN_Client_Picture
TRN_Client_Pregnant
TRN_Client_Race
TRN_ClientFamilyStatus
TRN_ClientHtWt
TRN_ClientIncidentRole
TRN_ClientPendingPhase
TRN_ClientStatus
TRN_ClientToIncident
TRN_ClientToOrganization
TRN_ClientToStaff
TRN_ConsentForm
TRN_CountyProgramRevoke
TRN_CountyPrograms
TRN_CountyServed
TRN_CourtAction
TRN_CourtActionToObligation
TRN_CourtActionToOffense
TRN_CRA
TRN_DADiagnostic
TRN_DATreatmentReceived
TRN_DeadTimeDetails
TRN_DischargeDetails
TRN_Domain_City
TRN_Domain_Country
TRN_Domain_County
TRN_Domain_Language
TRN_Domain_Obligation_ServicesReceived
TRN_Domain_Obligation_ServicesReceivedOutcome
TRN_Domain_Offense
TRN_Domain_OffenseCharactisticMatrix
TRN_Domain_PlacementType
TRN_Domain_RaceMap
TRN_Domain_StateTerritoryPossessions
TRN_Domain_ZipCode
TRN_Domain_ZipCodeToCity

TRN_DomainColumn
TRN_DomainTable
TRN_DomainType
TRN_DomainTypeColumn
TRN_Exception
TRN_FFPApprovalStatus
TRN_Incident
TRN_Incident_CommunityFacility
TRN_Incident_Parole
TRN_Incident_Residential
TRN_IR
TRN_IR_CFDomainAnswer
TRN_IR_CFInformation
TRN_IR_ClientInfo
TRN_IR_Deleted
TRN_IR_Detail
TRN_IR_DomainAnswer
TRN_IR_DomainCodeSortOrder
TRN_IR_IncidentCharacteristics
TRN_IR_IncidentReferral
TRN_IR_Interventions
TRN_IR_MedicalAttention
TRN_IR_PersonInvolvement
TRN_IR_RestraintUse
TRN_IR_RestrictedStaffRelatedDomainCode
TRN_IR_StaffInfo
TRN_IR_TableLookup
TRN_IRtoTRN_RoomConfinementAndIsolation
TRN_ISCA
TRN_ISCAOffenseSeriousnessLevel
TRN_ISCARiskLevel
TRN_ITP
TRN_ITP_To_TargetB
TRN_ITPFamily
TRN_ITPGeneralTreatment
TRN_ITPHierarchy
TRN_ITPMotivation
TRN_ITPNarrative_Detail
TRN_ITPSkill
TRN_ITPSpecialTreatment
TRN_ITPTargetB
TRN_ITPTargetB_To_BCA
TRN_JRAStaff
TRN_JRAStaffEncryptionKeys
TRN_JRAStaffTitle
TRN_JRAStaffToOrganization
TRN_Jurisdiction

TRN_KeyGenerator
TRN_LENotificationNarrative
TRN_LENotifications
TRN_LENotificationToLENotification
TRN_NextJRANumber
TRN_Notification
TRN_NotificationFaxSatus
TRN_NotificationsSentToOrganizations
TRN_NotifySent
TRN_Obligation
TRN_Obligation_AggregatedParole
TRN_Obligation_AggregatedResidence
TRN_Obligation_CourtOrderedTesting
TRN_Obligation_CourtOrderedTestingResult
TRN_Obligation_MedicalNeed
TRN_Obligation_NotificationRequired
TRN_Obligation_ServicesReceived
TRN_Obligation_ServicesReceivedOutcome
TRN_Obligation_SupervisionLevel
TRN_ObligationRemainderOfSentence
TRN_Offense
TRN_Offense_Notification_Rules
TRN_OFRCounty
TRN_OFROrganization
TRN_OrganizationAddress
TRN_OrganizationElectronicAddress
TRN_Override
TRN_OverrideStaff
TRN_ParoleContact
TRN_ParoleContactTypes
TRN_ParoleExtend
TRN_ParoleNotes
TRN_ParoleRevoke
TRN_Person
TRN_PersonAddress
TRN_PersonElectronicAddress
TRN_PersonToLanguage
TRN_PhysicalLocation
TRN_PhysicalLocationMoveReason
TRN_PhysicalLocationMoveReasonOther
TRN_PhysicalLocationObligation
TRN_PhysicalLocationSanction
TRN_Progress
TRN_RelationalAssessment
TRN_ReportingServicesCannedReports
TRN_RescindedCommitment
TRN_ResContactComment

TRN_Reservation
TRN_ReservationOverride_History
TRN_ReservationPendingApproval
TRN_ResidentContacts
TRN_ResidentialSentence
TRN_ResidentialSentence_Adjustment
TRN_ResidentialSentence_PriorOffense
TRN_RevokeDate
TRN_ROA
TRN_ROAApprovalJobClassAAA
TRN_ROAApprovers
TRN_ROAPendingApproval
TRN_ROAType
TRN_RoomConfinementAndIsolation
TRN_RTCN
TRN_RTCN_SpecializedData
TRN_RTCNNarrative
TRN_RTCNSkillInfo
TRN_RTCNSpecialized
TRN_RTCNTargetB
TRN_RTR
TRN_Sanction
TRN_Sanction_CommunityFacilityRecommendation
TRN_Sanction_InstitutionManagement
TRN_Sanction_ParoleManagement
TRN_SanctionToObligation
TRN_SAVYAssessmentHistorical
TRN_SchoolNotifications
TRN_ServicePlan
TRN_ServicePlanID
TRN_ServicePlanType
TRN_SessionGoalResponse
TRN_SessionNote
TRN_SessionNoteID
TRN_SessionNoteRelationalAssessment
TRN_SOST
TRN_StaffToIncident
TRN_SWS
TRN_SWS_AUDIT
TRN_Tasks
TRN_TSum
TRN_TSumTargetB
TRN_VictimWitnessNotification
TSumNarrative
UserRequestForm
VictimWitnessNotificationCancel
WarrantViolation

Workflow
WorkflowToTransitionType
WSUITA
ZodModuleUsageLog
LogDeleted
LogUpserted
Reload
MergedResponses
Module
ModuleClientRelated
ModuleOtherRelated
ModuleStaffRelated
ModuleToIC
ModuleToICPerson
ModuleToICPersonOther
ModuleToObligation
OrphanModule
Person
Response
ResponseDateTime
ResponseModule
ResponseModuleToCommonModule
ResponseNarrative
ResponseOrganization
ResponsePerson
ActBusinessRole
AddressFormat
AgeOfFirstUse
AllergyandPreviousMedicationType
AlternateIdentificationType
AltNameType
Anesthesia
Answer
AnswerControlEnabler
AnswerFullQuestionEnabler
AnswerValidation
AntCat
AnticipatedPlacementType
ApprovalStatus
ApprovedRestraintType
ARIIncidentType
Assembly
AssessmentScoringRule
AssessmentSource
AuditTypeOfKey
BugContactType
BugPriorityType

BugStatusType
Calendar
CaseNoteAttendanceType
CaseNoteGroup
CaseNoteType
CaseNoteTypeMaximum
CaseNoteTypeToActBusinessRole
CaseNoteTypeToNarrativeTemplate
CaseNoteTypeToRule
CaseNoteTypeToTransitionModuleType
CategoryType
CategoryTypeToModuleType
CensusBureauOffenseCode
CensusBureauOffenseType
CerdAdjustmentReason
CERDAdjustmentType
CERDAdjustmentTypeToCERDAdjustmentReason
CfOtherViolation
CfSeriousViolation
CHRQuestionNumberRelationship
ClientDocumentType
ClientHandoutStatus
ClientHandoutType
ClientOrganizationRelationshipType
ClientProcessState
ClientRace
ClientToOrganizationRelationTypeToObligationType
CltStaffRelat
CommFacRecType
commonModuleType
CommunityFacilityChangeCode
ComplexionToWarrantCode
ContactType
ControlType
CountyOrganizationType
CountyProgramPlacementTypeToRevokePlacementType
CountyProgramType
CountyReleaseType
CourtOrder
CPSPersonRelationshipType
CPSPersonType
CriminalClass
CriminalClassRank
CrudType
CSDBAlternateID
CSDBPersonRelationCodes
Culture

DeadTimeType
DeathType
DiaryCardType
DischargeLocationType
DischargeReleaseType
DMHSAnswer
DMHSAnswerControlEnabler
DMHSAnswerFullQuestionEnabler
DMHSAnswerValidation
DMHSControlType
DMHSLevel
DMHSQuestion
DMHSQuestionToAnswer
DMHSScore
DMHSSection
DominantHand
Drug
DrugGroup
DSHSNativeAmericanCode
DSHSTribeCode
DVROutcome
DVRStatus
ElectronicAddressType
EndReason
EyeToWarrantCode
FamilyStatus
FirearmEnhancementRule
FoodOmitDomainType
Frequency
GangToGangRelationshipType
Gender
GenderServed
HairToWarrantCode
HomePageType
ImageType
IPGenerator
IR_DomainAnswer
IR_DomainAnswerType
IRAnswer
IRIC
IRICActionTypes
IRICGroups
IRICRoleCombos
IRModuleType
IRQuestion
IRQuestionToAnswer
IRVersion

IRVersionToQuestion
IRVersionToQuestionAnswer
ISCAAnswer
ISCAMatrix
ISCAQuestion
IsolationConfinementReason
IssueType
ITADomains
ITAScoreNorm
ITAScoreNormRange
ITAScoreThreshold
ITAScoreType
ITPRank
JobTitle
JRATransitionType
JurisdictionType
JuvenileDispositionSentenceCategory
JuvenileOffenseCharacteristic
LanguageNote
LivingUnitDesignation
LivingUnitDesignationType
LivingUnitTransferReasons
LocMgtState
LocType
MandatedCERDType
ManifestInjustice
MarkType
medAnswer
medAppointmentType
medAxisType
medGroup
MedicalImageMapLabel
MedicalImageMapRegion
medModuleType
medQuestion
medQuestionGroup
medQuestionToAnswer
medRecurrenceType
medScheduleGroupType
medSection
MelissaDataCode
MentalHealthAssessmentType
MenuAccess
MenuDirectories
MenuDirectoriesToActBusinessRoles
MenuDirectoriesToMenuItems
MenuGoLiveDates

MenuGoLiveTypes
MenuItems
MenuItemsToActBusinessRoles
MiddleNameStatus
ModuleType
ModuleTypeToQuestionAnswerID
MoveReason
NarrativeTemplate
NarrativeType
NasellePlacementRules
NotifyRequiredType
NotifySentType
Numbers
Oblg_Outcomes_tbl
Oblg_Services_Tbl
OblgType
ObligationEndRule
ObligationFromCode
OffenseGroup
OffenseModifier
OffenseNotificationRules
OffenseToWarrantCode
OldServicePlanType
Organization
OrganizationName
OrganizationPlacementScreenOut
OrganizationType
OrgRegionRole
OrgType
ParExtType
ParoleFTENeedRule
ParoleMgtType
ParoleReleaseConditions
ParoleRevokeType
ParRevType
ParType
PBSEthnicity
PBSOffense
PBSOrgNameLookUp
PBSQuestions
PBSToJRAEthnicity
PBSToJRAOffense
PBStoZodQuestionToAnswer
PeriodAccrual
Periodicity
PhysicalAddressType
PhysicalAttribute

PhysicalAttributeType
PhysicalLocationAction
PlacementTypeRule
Placeof
PolicyLink
PriorityStatus
PriorityType
Progress
PrsnOrgRelationshipType
PrsnPrsnRelationshipType
QAToTable
Question
QuestionToAnswer
QuestionToAnswerControlType
QuestionToAnswerDisplay
QuestionToAnswerIDsThatRepresentTheSameData
QuestionToAnswerScoreValue
QuestionToSection
QuestionType
RaceGroup
RaceToWarrantCode
RarIPCalcalculatedDaysAfterAdmission
RecoICDRetentionRule
RecurranceType
ReentryDomainOverdueInterval
ReentryDomains
ReentryDomainToYouthPrompt
ReentryNoteType
RegionRelationship
RelationalAssessmentPersonTypeLookup
ReleaseDateType
ReleasePlacementType
ReleaseType
ReoffendRisk
ReoffendRiskAssessmentRange
ReservationCharacteristics
ResidentialReleaseType
RestitutionType
RestrictedTransitionItemRule
RiskAssessmentGrid
RiskAssessmentGridOption2
RiskAssessmentGridOption3
RiskAssessmentReasonForChange
RiskAssessmentType
ROACreatedAs
ROATaskStatusType
RoleType

RoomConfinementReason
RouteOfAdministration
RTMCaseNoteType
SanctionCode
SanctionType
SASLevel
SAVYSexualAggressionLevel
ScannedDocumentType
SchemaType
SchemaTypeToModuleType
Section
SecurityRole
SentAdjType
SentenceGrid
SentenceType
ServicePlanCategory
ServicePlanGroup
ServicePlanOutcome
ServicePlanOutcomeToGroup
ServicePlanParoleStatus
ServicePlanScreenOutReason
ServicePlanScreenOutReasonToGroup
ServicePlanType
ServicePlanTypeToServicePlanCategory
SessionPhase
SOGIEAnswers
SOSTScoreLevel
SpecifierOne
SpecifierTwo
SPLLevel
SPLToFITQualifier
SPLToMentalHealthTargetPopulationFactor
SPLToRARFemaleScores
SSAOrgCode
SSS1andSSS2Question
SSS2MultipleChoice
SSS2Question
SSS2QuestionDescription
SSS2QuestionToMultipleChoice
SSS2Type
SSS2YesNoToNumberQuestion
SSS2YesNoToTextQuestion
SSSSPLLevel
StaffAssessmentRole
StaffRole
StatusType
SupervisionConditionsAddedCondition

SupervisionConditionsRestrictedItem
SupervisionConditionsSearch
SupervisionConditionsType
SupervisionLevelToOrg
SupLevel
Surface
TargetBStatus
TaskEndReasonType
TaskType
TaskVisibilityType
TestType
Tooth
TransitionItem
TransitionItemRule
TransitionItemRuleToACTBusinessRole
TransitionItemRuleToCaseManagerType
TransitionItemStatus
TransitionItemToRole
TransitionItemToType
TransitionModuleType
TransitionModuleTypeToCommonModuleType
TransitionModuleTypeToMedicalModuleType
TransitionRecurrenceType
TransitionType
Treatment
TreatmentHierarchyType
TRN_CaseManagementDueDateRule
TRN_CaseNoteType
TRN_CFIR_OtherViolationTypeLookup
TRN_CFIR_SeriousViolationTypeLookup
TRN_CHRAnswer
TRN_Client_PictureType
TRN_ClientSupervisionLevelLookup
TRN_ContactPlace
TRN_DADiagnosticAnswer
TRN_DATreatmentResultType
TRN_DATreatmentType
TRN_DischargeLocationLookup
TRN_DischargeReleaseReason
TRN_DischargeReleaseRule
TRN_DomainCode
TRN_HierarchyPatternKey
TRN_IncidentType
TRN_ITPOverarchingSkill
TRN_ITPSpecificSkill
TRN_ITPType
TRN_OffenseRank

TRN_Organization_FacilityCapacity
TRN_Organization_Res_Rules
TRN_OverrideSubtype
TRN_OverrideType
TRN_ParoleRevokeRules
TRN_PersonType
TRN_RegionToCounty
TRN_RegionToCourt
TRN_RelatednessPattern
TRN_ROAApprovalJobClass
TRN_ROACategory
TRN_ROAOrgToCategory
TRN_ROATypeLookup
TRN_ROATypeLookupToCategory
TRN_RoomConfinementAndIsolationType
TRN_RTCN_CoreComponents
TRN_RTCN_TxTask
TRN_RTCNSectionNames
TRN_ServicePlanOutcome
TRN_SessionGoal
TRN_SessionNoteStatus
TRN_StaffConfidence
TRN_SWSTypeToObligationType
TRN_TRTransitionType
TSumSectionNames
Version
VersionQuestionAnswerToITAScoreType
VersionToCommonModuleType
VersionToObligationAttachRules
VersionToQuestionAnswer
VersionToQuestionAnswerScoreWeight
VersionToQuestionSection
Victimization
VictimWitnessNotificationMoveType
ViolationType
WarrantViolationType
CRBResObl
HartMentalHealthFlags
HartResObl
parole4hart
Allergy
AppointmentSchedule
AppointmentScheduleDates
AppointmentScheduleToAppointmentType
Axis
ClientAllergyandPreviousMedication
ClientMedicationHistory

ClientProblem
ClientRelationship
ClientToAllergy
Dental
DentalSurface
DentalTooth
Diagnosis
Food
FoodAllergy
ICD
ICD9ToICD10
MAR
MARToObligation
MedicalImageMapCoordinates
MedicationAllergy
Module
ModuleClientRelated
ModuleStaffRelated
ModuleToClientHtWt
ModuleToClientProblem
ModuleToICD
ModuleToObligation
ModuleToScannedDocument
OmitedFood
OrphanModule
PNote
PPNLegacyReport
PrescriptionDrug
Response
ResponseDateTime
ResponseInteger
ResponseModule
ResponseNarrative
ResponsePerson
SpecialDiet
SubstitutedFood
ActionHistory
ActionType
BusinessRole
Coverage
EducationAppointment
Enrollment
EnrollmentForm
EnrollmentFormGuardianName
Form
InitialScreening
LeavingJR

ManagedCarePlanType
NoCoverageReasonType
Note
ParentGuardianContact
RoleToCounty
RoleToOrganization
RoleToRegionName
RoleType
StatusType
TransitionModuleTypeForHomePageTab
YouthAuthorization
SupervisionConditions
SupervisionConditionsApprovalStatus
SupervisionConditionsComments
SupervisionConditionsToSupervisionConditionsAddedCondition
SupervisionConditionsToSupervisionConditionsRestrictedItem
SupervisionConditionsToSupervisionConditionsSearch
SPL
PhysicalLocationToSSS1
PhysicalLocationToSSS2
ReviewStatusType
SSS1
SSS1ClientRelationship
SSS1Module
SSS1ModuleClientRelated
SSS1ModuleStaffRelated
SSS1ModuleToObligation
SSS1OrphanModule
SSS1Response
SSS1ResponseDateTime
SSS1ResponseModule
SSS1ResponseNarrative
SSS2
SSS2ApprovalStatus
SSS2ClientRelationshipAnswer
SSS2DatetimeAnswer
SSS2MultipleChoiceAnswer
SSS2NumberScaleAnswer
SSS2TextAnswer
SSS2ToObligation
SSS2YesNoAnswer
SSSReview
Form
Outcome
OutcomeType
Referral
ReferralType

RoleToOrganization
Suitability
WISeToObligation

CA_Data_Analysis_Temp_DB

Payments FFU

CAChet

CHET
chet_0301
CHET-HST
EDUCATION_RECORDS_REQUEST
HEALTH_MENTAL_HEALTH
Input
MEDICAL_RECORD_REQUEST
NotNFamlink

FamLinkDW

ABUSE_FACT
ABUSE_TYPE_DIM
ADOPTION_FACT
ADOPTION_STATUS_DIM
AFCARS_ADOPT
AFCARS_FOSTER
ALLEGATION_FACT
ASSESSMENT_TYPE_DIM
ASSIGNMENT_ATTRIBUTE_DIM
ASSIGNMENT_FACT
AUTHORIZATION_DIM
AUTHORIZATION_FACT
CALENDAR_DIM
CASE_DIM
CASE_EXTENSIONS_EXCEPTIONS_FACT
CASE_EXTENSIONS_EXCEPTIONS_TYPE_DIM
CASE_NOTE_FACT
CASE_NOTE_TYPE_DIM
CASE_PARTICIPANT_FACT
CASE_PARTICIPANT_STATUS_DIM
COURT_HEARING_FACT
DISCHARGE_REASON_DIM
DISPOSITION_DIM
DLR_RISK_ASSESSMENT_FACT
EDUCATION_DIM
EDUCATION_FACT
FAMILY_ASSESSMENT_GOAL_FACT
FAMILY_ASSESSMENT_NEED_FACT
FAMILY_STRUCTURE_DIM

FINDINGS_DIM
GOAL_NEED_BRIDGE_FACT
GOAL_SERVICE_BRIDGE_FACT
GOAL_TYPE_DIM
HEALTH_ACTIVITY_FACT
HEALTH_ACTIVITY_TYPE_DIM
HEALTH_CAT_ATTRIBUTE_BRIDGE_FACT
HEALTH_CAT_ATTRIBUTE_DIM
IL_ANSELL_CASEY_ASSESSMENT_FACT
IL_NYTD_QUESTIONS_ATTRIBUTE_DIM
IL_NYTD_QUESTIONS_FACT
IL_SERVICE_CATEGORY_TYPE_DIM
INDEPENDENT_LIVING_BRIDGE_FACT
INDEPENDENT_LIVING_FACT
INTAKE_ATTRIBUTE_DIM
INTAKE_FACT
INTAKE_PARTICIPANT_FACT
INTAKE_PARTICIPANT_ROLES_DIM
INTAKE_SERVICE_BRIDGE_FACT
INTAKE_TYPE_DIM
INTAKE_VICTIM_FACT
INVESTIGATION_ASSESSMENT_FACT
INVESTIGATION_PARTICIPANT_FACT
INVESTIGATION_TYPE_DIM
LEGAL_ACTION_DIM
LEGAL_FACT
LEGAL_JURISDICTION_DIM
LEGAL_RESULT_DIM
LEGAL_STATUS_DIM
LEGAL_TPR_REFERRAL_FACT
LOCATION_DIM
MEETING_CHILD_PRTC_TEAM_FACT
MEETING_CPT_ADDTN_PART_FACT
MEETING_CPT_CURR_PRVD_FACT
MEETING_CPT_PART_FACT
MEETING_CPT_SRVC_FAMILY_FACT
MEETING_DIM
MEETING_FACT
MEETING_PARTICIPANT_FACT
MEETING_SHARED_ACTION_PLAN_FACT
MEETING_SHARED_PARTICIPANT_FACT
MEETING_TYPE_DIM
MENTAL_HEALTH_EVAL_DIM
NCANDS
OUTCOME_DIM
PAYMENT_DIM
PAYMENT_FACT
PEOPLE_DIM
PERMANENCY_FACT
PERMANENCY_PLAN_DIM
PLACEMENT_CARE_AUTH_DIM

PLACEMENT_CARE_AUTH_FACT
PLACEMENT_FACT
PLACEMENT_RESULT_DIM
PLACEMENT_TYPE_DIM
PRE_ADOPTION_LEGAL_FACT
PRIMARY_ASSIGNMENT_FACT
PROVIDER_DIM
PROVIDER_PART_FACT
RELATIONSHIP_DIM
REMOVAL_DIM
REMOVAL_EPISODE_FACT
REPEAT_MALTREATMENT_FACT
RESPONSE_TIME_EXP_DIM
SAFETY_ASSESSMENT_FACT
SERVICE_FACT
SERVICE_REFERRAL_DIM
SERVICE_REFERRAL_FACT
SERVICE_REFERRAL_TYPE_DIM
SERVICE_TYPE_DIM
SIBLING_RELATIONSHIP_FACT
TANF_DIM
TANF_FACT
TRIBE_ATTRIBUTE_DIM
TRIBE_DIM
TRIBE_FACT
WORKER_DIM

FamLinkDW_Common

BRS_CODES
brscontracts
CURRENT_PLACEMENTS_ARCGIS
rptIntake_Assignments
rptIntake_Children
rptIntake_subjects
rptIntakes
rptPlacement_Events
rptPlacements

FamLinkDW_Manager

RACE_REF
RUN_DATE

FamLinkRO

ACCESS_REPORT
ACCESS_REPORT_EMERGENT_RESPONSE
ACCESS_REPORT_NON_EMERGENT_RESPONSE
ACCESS_REPORT_OVERRIDE_BASIS
ACCESS_REPORT_WAC

ADDRESS
ADOPTION_AFTER_18
ADOPTION_ELIG
ADOPTION_ELIG_REDET
ADOPTION_MATCH
AGREEMENT
ALLEGATION
ALLEGED_FATHER
APPROVAL
APPROVAL_HISTORY
ASSESSMENT
ASSIGN_CATEGORY
ASSIGNMENT
AUTHORIZATIONS
CASE_CLOSURE
CASE_GROUP
CASE_PART
CASE_PART_STAT
CASE_REVIEW_FACP
CATEGORY_TYPE
CODE_DESC
CODE_DESC_LRG
CODE_DESC_STATIC
CODE_GRP_DESC
CONTRACT
CONTRACT_PROVIDER
CONTRACT_REGION
COURT_DISP
CPS_REPORT
EPISODE
FACP_CHARACTERISTICS
FACP_FAMILY_ASSESSMENT
FACP_OBJECTIVE
FACP_OBJECTIVE_SERVICE
FACP_OBJECTIVE_TASKS
FACP_PART
FACP_PART_OBJECTIVE
FAMILY_ASSESSMENT
FAMILY_ASSESSMENT_PART
FAMILY_DEV_STAGES
GAIN_SS
HEALTH_MENTAL_HEALTH
HEALTH_MENTAL_HEALTH_PROBLEM
INDEPENDENT_LIVING
INTAKE_PART
INVESTIGATION
LEGAL_ACTION
LEGAL_JURISDICTION
LOCATION
MENTAL_HEALTH
MENTAL_HEALTH_DSM

PAYMENT
PERSON
PERSON_AKA
PERSON_MERGE
PERSON_RELATIONSHIP
PERSON_RELATIVE
PERSON_TRIBE
PLCMNT_CARE_AUTHORITY
PRE_ADOPTION_MATCH
PRESENT_DANGER_ASSMNT
PRESENT_DANGER_ASSMNT_PERSON
PROVIDER_ORG
PROVIDER_PART
PROVIDER_PART_STAT
RATE_SETTING
SA_INTAKE
SA_PART
SA_SAFETY_ASSESSMENT
SA_TASK
SA_TASK_THREAT
SAFETY_ASSESSMENT
SDM_RISK_ASSESSMENT
SERVICE_REFERRAL
SERVICE_REFERRAL_INTAKE
SERVICE_REFERRAL_PART
SERVICE_TYPE
STATE_CODE_DESC
SUBSTANCE_ABUSE
TRIBE
WORKER

SSPS: AuthHist

AuthorizationHistory
DailyAuth

SSPS: PayHist

DailyPay
PayHistIdeal

SSPS: Paragon

AccountCode
ProviderMain
ProviderMainArchive
ProviderMainSupplement
ProviderMainSupplementArchive
SEIUCoveredService
ServiceCode
ServiceCodeArchive

ServiceCodeHHC
ServiceCodeLUT
ServiceCodeMaster
ServiceCodeMASTERArchive
ServiceCodeMF
ServiceGroupLUT
ServiceProgramOwnerName
ServiceResponsibility
ServiceTaxStatus
UnionProviderArchive
UnionRate
VoeType

SSPS: PaymentAdjustment

PaymentAdjustment
PaymentAdjustmentAdjustTypeLUT
PaymentAdjustmentDetail

Exhibit E

IN19 Client Services Interface Data

1. *PA1 – Person address transaction*

ATTRIBUTE_NAME	ATTRIBUTE_NOTES
TRANSACTION TYPE	Allowable *value* (pre-assigned by CSDB): 'PA1'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier for each person (to be assigned by the reporting source).
EFFECTIVE DATE	Use 'YYYYMMDD' date format: do not use hyphens (-) or slashes (/) to separate elements of the date. [Note: submit additional transactions if multiple Effective Dates are reported.]
PERSON RESIDENCE ADDRESS TYPE	Allowable values: see the list of Address Types include in Attachment #6. [Note: submit additional transactions if multiple Person Residence Address Types are reported.]
ADDR FORMAT	Allowable values: see the list of Address Formats (and examples) included in Attachment #7.
LINE 1	Information to be reported on this line depends on ADDR FORMAT (see above).
LINE 2	Information to be reported on this line depends on ADDR FORMAT (see above).
LINE 3	Information to be reported on this line depends on ADDR FORMAT (see above).
LINE 4	Information to be reported on this line depends on ADDR FORMAT (see above).
UNIT ID	Apartment/Duplex/Suite number, etc.
DELIVERY CITY	City name for postal delivery purposes.
STATE	Use the 2-digit postal standard to designate the state of this address.
ZIPPLUS4	5-digit core zip plus, optionally, the 4-digit supplemental zip (with hyphen separating core and supplemental zip). [Note: left-justify this field using trailing spaces where supplemental zip code is not available.]
GEOGRAPHY TYPE NAME	Allowable values: see the list of Geography Types included in Attachment #8. [Notes: (1) report the type for the lowest (most detailed) level of geographic specificity and (2) submit additional transactions is multiple Geography Type Names are reported (omit address info in subsequent transactions).]
GEOGRAPHY IDENTIFIER	Allowable values: depend on GEOGRAPHY TYPE NAME (see above). [Notes: submit additional transactions if multiple Geography Identifiers are reported (omit address info in subsequent transactions).]

2. *PC1 – Person case transaction*

ATTRIBUTE_NAME	ATTRIBUTE_NOTES
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PC1'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
CASE ID	Unique identifier for each case (to be assigned by the reporting source).
PERSON ID	Unique identifier for each person (to be assigned by the reporting source).
RECIPIENT STRING	Unique identifier for a category or class of recipient. Include all elements necessary to identify a unique type of recipient with a colon (:) separating each distinct element. [Note: these values will be negotiated with each reporting source.]
BEGIN DATE	Use 'YYYYMMDD' date format: do not use hyphens (-) or slashes(/) to separate elements of the date. [Notes: (1) report the date that the person was initially associated with the case and (2) submit additional transactions if multiple Begin Dates are reported.]
END DATE	Use 'YYYYMMDD' date format: do not use hyphens (-) or slashes(/) to separate elements of the date. [Note: report the date that the person was last associated with the case.]

3. *PPE – Person transaction*

ATTRIBUTE_NAME	ATTRIBUTE_NOTES
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PPE'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier for each person (to be assigned by the reporting source). Only 1 PERSON ID for each person is allowed per file. If more than 1 PERSON ID per person is submitted, only the last one submitted will be used.
DATE OF BIRTH	Use 'YYYYMMDD' date format: do not use hyphens (-) or slashes (/) to separate elements of the date.
GENDER	Allowable values: F - Female M - Male
RACE CODE	Allowable values: see the list of Race Codes included in Attachment #2. [Note: leave blank where race is Unknown or Unreported.]
ETHNICITY CODE	Allowable values: see the list of Ethnicity Codes included in Attachment #3. [Note: leave blank where ethnicity is Unknown or Unreported.]
DSHS TRIBAL CODE	Allowable values: see the list of Tribal Codes included in Attachment #4.
COUNTRY OF	Allowable values: see the list of Country Codes included in Attachment

ORIGIN CODE	#5.
USA ENTRY DATE	Use 'YYYYMMDD' date format: do not use hyphes (-) or slashes (/) to separate elements of the date.

4. *PPI – Person alternate ID transaction*

ATTRIBUTE_NAME	**ATTRIBUTE_NOTES**
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PPI'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier for each person (to be assigned by the reporting source).
ALTERNATE ID TYPE	Allowable values: see the list of Alternate Identifier Types included in Attachment #11.
ALTERNATE ID VALUE	Allowable values: depend on ALTERNATE ID TYPE (see above). [Note: submit additional transactions if mulitple alternate ID Values are reported.]

5. *PPN – Person name transaction*

ATTRIBUTE_NAME	**ATTRIBUTE_NOTES**
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PPN'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier fo reach person (to be assigned by the reporting source).
NAME FORMAT	Allowable values: see the list of Name Formats (and examples) included in Attachment #12.
FULL NAME OR SURNAMES	Where the value for NAME TYPE is '1', report all elements of the name. Where the value for NAME TYPE is '2', report the surnames(s). [Note: submit additional transactions if mulitple Full Names or Surnames are reported.]
GIVEN NAMES	Where the value for NAME TYPE is '1', report a Null value. Where the value for NAME TYPE is '2', report the given name(s). [Note: submit additional transactions if mulitple Given Names are reported.]

6. *PPR – Race transaction*

ATTRIBUTE_NAME	**ATTRIBUTE_NOTES**
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PPR'
TRANSACTION	Allowable value (pre-assigned by CSDB): '10'

VERSION	
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier fo reach person (to be assigned by the reporting source).
RACE CODE	Allowable values: see the list Race Codes included in Attachment #2

7. *PS4 – Service Span/Person Case Transaction*

ATTRIBUTE_NAME	**ATTRIBUTE_NOTES**
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PPN'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the list of Source System Identifiers included in Attachment #1.
PERSON ID	Unique identifier fo reach person (to be assigned by the reporting source).
NAME FORMAT	Allowable values: see the list of Name Formats (and examples) included in Attachment #12.
FULL NAME OR SURNAMES	Where the value for NAME TYPE is '1', report all elements of the name. Where the value for NAME TYPE is '2', report the surnames(s). [Note: submit additional transactions if mulitple Full Names or Surnames are reported.]
GIVEN NAMES	Where the value for NAME TYPE is '1', report a Null value. Where the value for NAME TYPE is '2', report the given name(s). [Note: submit additional transactions if mulitple Given Names are reported.]

8. *PSV – Service definition transaction*

ATTRIBUTE_NAME	**ATTRIBUTE_NOTES**
TRANSACTION TYPE	Allowable value (pre-assigned by CSDB): 'PSV'
TRANSACTION VERSION	Allowable value (pre-assigned by CSDB): '10'
SOURCE SYSTEM ID	Allowable values: see the l ist of Source System Identifiers included in Attachment #1.
EFFECTIVE DATE	Use 'YYYYMMDD' date format: do not use hyphens (-) or slashes (/) to separate elements of the date. [Note: report the date that the service was originally offered by your agency, not the date that the service was initially provided to the client (use the BEGIN DATE field on the SERVICE SPAN/PERSON CASE File Layout to report the date that the service was first delivered to the client).]
DOLLARS AVAILABLE	Y - Yes N - No

SERVICE UNIT	Allowable values: see the list of Service Units included in Attachment #2.
SHORT TITLE	Abbreviated label for service modality.
LONG TITLE	Extended label for service modality.
DESCRIPTION	Narrative depiction of service modality.
FRS GROUP ACCOUNT	Consists of fields BIENNIUM YEAR thru PROJECT STUCTURE (see 10a - 10r below). [Note: no internal delimiters allowed between sub-fields and (2) leave the appropriate sub-field column(s) blank where an element of the FRS GROUP ACCOUNT is not reported.]
TIE BREAKER	Allowable values: to be negotiated with each reporting source.