615 Sheridan Street
Port Townsend, WA 98368
www.JeffersonCountyPublicHealth.org
Consent Agenda

JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA REQUEST

TO: **Board of County Commissioners**
Mark McCauley, County Administrator

FROM: Veronica Shaw, Deputy Public Health Director

DATE: January 2, 2024

SUBJECT: Agenda item – Data Sharing Agreement with Washington State Department of Health (DOH) for sharing of information concerning Home Visiting Services; January 1, 2024 – December 31, 2028

STATEMENT OF ISSUE:

Jefferson County Public Health (JCPH) requests Board approval of a Data Sharing Agreement between DOH and JCPH for sharing of information concerning Home Visiting Services; January 1, 2024 – December 31, 2028

ANALYSIS/STRATEGIC GOALS/PRO'S and CON'S:

The purpose of this agreement is to address the disclosure of confidential client and program service data required to evaluate home visiting services provided by local agencies under a Home Visiting Services Account (HVSA) contract. DOH is contracted by the Department of Children, Youth, and Families (DCYF) to collect, analyze and report HVSA data to meet DCYF's evaluation, quality assurance and improvement, data collection and reporting requirements.

FISCAL IMPACT/COST BENEFIT ANALYSIS:

There is no financial component to this agreement.

RECOMMENDATION:

JCPH management requests approval of a Data Sharing Agreement with DOH for sharing of information concerning Home Visiting Services; January 1, 2024 – December 31, 2028

REVIEWED BY:

Mark McCauley, County Administrator — Date 12/18/23

CONTRACT REVIEW FORM

Clear Form

(INSTRUCTIONS ARE ON THE NEXT PAGE)

CONTRACT WITH: WA DOH Contract No: AD-23-086

Contract For: Data sharing: Home Visiting Services Term: 01/01/2024 - 12/31/2028

COUNTY DEPARTMENT:	Public Health
Contact Person:	Veronica Shaw
Contact Phone:	x 409
Contact email:	veronica@co.jefferson.wa.us

AMOUNT: -0-

Revenue: _____

Expenditure: _____

Matching Funds Required: _____

Sources(s) of Matching Funds _____

Fund # _____

Munis Org/Obj _____

PROCESS:

- ☐ **Exempt from Bid Process**
- ☐ **Cooperative Purchase**
- ☐ **Competitive Sealed Bid**
- ☐ **Small Works Roster**
- ☐ **Vendor List Bid**
- ☐ **RFP or RFQ**
- ☐ **Other:** _____

APPROVAL STEPS:

STEP 1: DEPARTMENT CERTIFIES COMPLIANCE WITH JCC 3.55.080 AND CHAPTER 42.23 RCW.

CERTIFIED: ☐ **N/A:** ■ Signature Dec 14, 2023 Date

STEP 2: DEPARTMENT CERTIFIES THE PERSON PROPOSED FOR CONTRACTING WITH THE COUNTY (CONTRACTOR) HAS NOT BEEN DEBARRED BY ANY FEDERAL, STATE, OR LOCAL AGENCY.

CERTIFIED: ☐ **N/A:** ■ Signature Dec 14, 2023 Date

STEP 3: RISK MANAGEMENT REVIEW (will be added electronically through Laserfiche):

Electronically approved by Risk Management on 12/14/2023.
State agreement. Cannot change.

STEP 4: PROSECUTING ATTORNEY REVIEW (will be added electronically through Laserfiche):

Electronically approved as to form by PAO on 12/14/2023.

STEP 5: DEPARTMENT MAKES REVISIONS & RESUBMITS TO RISK MANAGEMENT AND PROSECUTING ATTORNEY(IF REQUIRED).

STEP 6: CONTRACTOR SIGNS

STEP 7: SUBMIT TO BOCC FOR APPROVAL

DATA SHARING AGREEMENT
FOR
CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)
BETWEEN
STATE OF WASHINGTON
DEPARTMENT OF HEALTH
AND
Jefferson County Public Health

This Agreement documents the conditions under which the Washington State Department of Health (DOH) receives confidential information or limited Dataset(s) with local agencies providing home visiting services under a Home Visiting Services Account (HVSA) contract with the Department of Children, Youth and Families (DCYF). DOH will collect, process, evaluate and share info according to its partnership with DCYF.

CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION

	INFORMATION RECIPIENT	INFORMATION PROVIDER
Organization Name	Washington State Department of Health (DOH)	Jefferson County Public Health
Business Contact Name	Ashley Beck	Veronica Shaw
Title	Supervising Epidemiologist	Deputy Director
Address	243 Israel Rd. SE P O Box 47835 Olympia, WA 98504-7835	615 Sheridan St Port Townsend, WA 98368
Telephone #	(564) 669-4446	(360) 385-9409
Email Address	ashley.beck@doh.wa.gov	veronica@co.jefferson.wa.us
IT Security Contact	John Weeks	DJ Dimick
Title	DOH Chief Information Security Officer	Network Technician
Address	PO Box 47890 Olympia, WA 98504-7890	PO Box 1220 Port Townsend, WA 98368
Telephone #	360-999-3454	(360) 385-9171
Email Address	Security@doh.wa.gov	ddimick@co.jefferson.wa.us
Privacy Contact Name	Michael Paul	Sarah Jane
Title	DOH Chief Privacy Officer	Public Health Nurse, NFP
Address	PO Box 47890 Olympia, WA 98504-7890	615 Sheridan St Port Townsend, WA 98368
Telephone #	(564) 669-9692	(360) 385-9424
Email Address	privacy.officer@doh.wa.gov	sjane@co.jefferson.wa.us

DEFINITIONS

Authorized user means a recipient's employees, agents, assigns, representatives, independent contractors, or other persons or entities authorized by the data recipient to access, use or disclose information through this agreement.

Authorized user agreement means the confidentiality agreement a recipient requires each of its Authorized Users to sign prior to gaining access to Public Health Information.

Breach of confidentiality means unauthorized access, use or disclosure of information received under this agreement. Disclosure may be oral or written, in any form or medium.

Breach of security means an action (either intentional or unintentional) that bypasses security controls or violates security policies, practices, or procedures.

Confidential information means information that is protected from public disclosure by law. There are many state and federal laws that make different kinds of information confidential. In Washington State, the two most common are the Public Records Act RCW 42.56, and the Healthcare Information Act, RCW 70.02.

Data storage means electronic medicomputers and similar devices.

Data transmission means the process of transferring information across a network from a sender (or source), to one or more destinations.

Direct identifier Direct identifiers in research data or records include names; postal address information (other than town or city, state and zip code); telephone numbers, fax numbers, e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate /license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

Disclosure means to permit access to or release, transfer, or other communication of confidential information by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record.

Encryption means the use of algorithms to encode data making it impossible to read without a specific piece of information, which is commonly referred to as a "key". Depending on the type of information shared, encryption may be required during data transmissions, and/or data storage.

Human subjects research; human subject means a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.

Identifiable data or records contains information that reveals or can likely associate the identity of the person or persons to whom the data or records pertain. Research data or records with direct identifiers removed, but which retain indirect identifiers, are still considered identifiable.

Limited dataset means a data file that includes potentially identifiable information. A limited dataset does not contain direct identifiers.

Potentially identifiable information means information that includes indirect identifiers which may permit linking an individual to that person's health care information. Examples of potentially identifiable information include:

- birth dates;
- admission, treatment or diagnosis dates;
- healthcare facility codes;
- other data elements that may identify an individual. These vary depending on factors such as the geographical location and the rarity of a person's health condition, age, or other characteristic.

Restricted confidential information means confidential information where especially strict handling requirements are dictated by statutes, rules, regulations or contractual agreements. Violations may result in enhanced legal sanctions.

State holidays State legal holidays, as provided in RCW 1.16.050.

Health care information means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care...." RCW 70.02.010(7)

Health information is any information that pertains to health behaviors, human exposure to environmental contaminants, health status, and health care. Health information includes health care information as defined by RCW 70.02.010 and health related data as defined in RCW 43.70.050.

Human research review is the process used by institutions that conduct human subject research to ensure that:

- the rights and welfare of human subjects are adequately protected;
- the risks to human subjects are minimized, are not unreasonable, and are outweighed by the potential benefits to them or by the knowledge gained; and
- the proposed study design and methods are adequate and appropriate in light of the stated research objectives.

Research that involves human subjects or their identifiable personal records should be reviewed and approved by an institutional review board (IRB) per requirements in federal and state laws and regulations and state agency policies.

Identifiable data or records: contains information that reveals or can likely associate with the identity of the person or persons to whom the data or records pertain. Research data or records with direct identifiers removed, but which retain indirect identifiers, are still considered identifiable.

Indirect identifiers are indirect identifiers in research data or records that include all geographic identifiers smaller than a state , including street address, city, county, precinct, Zip code, and their equivalent postal codes, except for the initial three digits of a ZIP code; all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such age and elements may be aggregated into a single category of age 90 or older.

Normal business hours are state business hours Monday through Friday from 8:00 a.m. to 5:00 p.m. except state holidays.

GENERAL TERMS AND CONDITIONS

I. USE OF INFORMATION

The Information Recipient (DOH) agrees to strictly limit use of information obtained or created under this Agreement to the purposes stated in Exhibit I (and all other Exhibits subsequently attached to this Agreement). For example, unless the Agreement specifies to the contrary the DOH agrees not to:

- Link information received under this Agreement with any other information.
- Use information received under this Agreement to identify or contact individuals.

The DOH shall construe this clause to provide the maximum protection of the information that the law allows.

II. SAFEGUARDING INFORMATION

A. CONFIDENTIALITY

DOH agrees to:

- Follow DOH small numbers guidelines as well as dataset specific small numbers requirements. (Appendix D)
- Limit access and use of the information:
  - To the minimum amount of information .
  - To the fewest people.
  - For the least amount of time required to do the work.
- Ensure that all people with access to the information understand their responsibilities regarding it.
- Ensure that every person (e.g., employee or agent) with access to the information signs and dates the "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.
  - Retain a copy of the signed and dated form as long as required in Data Disposition Section.

The DOH acknowledges the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

B. SECURITY

The DOH assures that its security practices and safeguards meet Washington State Office of the Chief Information Officer (OCIO) security standard 141.10 *Securing Information Technology Assets*.

For the purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates meets OICIO standard 141.10 "Securing Information Technology Assets."

The DOH agrees to adhere to the Data Security Requirements in Appendix B. The DOH further assures that it has taken steps necessary to prevent unauthorized access, use, or modification of the information in any form.

Note: The DOH Chief Information Security Officer must approve any changes to this section prior to Agreement execution. IT Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

C. BREACH NOTIFICATION

The DOH shall notify the DOH Chief Information Security Officer (security@doh.wa.gov) within one (1) business days of any suspected or actual breach of security or confidentiality of information covered by the Agreement.

III. RE-DISCLOSURE OF INFORMATION

DOH agrees to not disclose in any manner all or part of the information identified in this Agreement except as the law requires, this Agreement permits, or with specific prior written permission by the Secretary of the Department of Health.

If the DOH must comply with state or federal public record disclosure laws and receives a records request where all or part of the information subject to this Agreement is responsive to the request: DOH will notify the Information Provider of the request ten (10) business days prior to disclosing to the requestor. The notice must:

- Be in writing;
- Include a copy of the request or some other writing that shows the:
  - Date DOH received the request; and
  - The DOH records that the DOH believes are responsive to the request and the identity of the requestor, if known.

IV. OTHER PROVISIONS

With the exception of agreements with British Columbia for sharing health information, all data must be stored within the United States.

V. AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

VI. CAUSE FOR IMMEDIATE TERMINATION

The DOH acknowledges that unauthorized use or disclosure of the data/information or any other violation of sections II or III, and appendices A or B, may result in the immediate termination of this Agreement.

VII. CONFLICT OF INTEREST

The DOH may, by written notice to the Information Provider:

Terminate the right of the Information Provider to proceed under this Agreement if it is found, after due notice and examination by the Contracting Office that gratuities in the form of entertainment, gifts or otherwise were offered or given by the Information Provider, or an agency or representative of the Information Recipient, to any officer or employee of the DOH, with a view towards securing this Agreement or securing favorable treatment with respect to the awarding or amending or the making of any determination with respect to this Agreement.

In the event this Agreement is terminated as provided in (a) above, the DOH shall be entitled to pursue the same remedies against the Information Provider as it could pursue in the event of a breach of the Agreement by the Information Provider. The rights and remedies of the DOH provided for in this section are in addition to any other rights and remedies provided by law. Any determination made by the Contracting Office under this clause shall be an issue and may be reviewed as provided in the "disputes" clause of this Agreement.

VIII. DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the DOH and the Information Provider and it cannot be resolved, either party may submit a request for a dispute resolution to the Contracts and Procurement Unit. The parties agree that this resolution process shall precede any action in a judicial and quasi-judicial tribunal. A party's request for a dispute resolution must:

- Be in writing and state the disputed issues, and
- State the relative positions of the parties, and
- State the Information Provider's name, address, and his/her department agreement number, and
- Be mailed to the DOH contracts and procurement unit, P. O. Box 47905, Olympia, WA 98504-7905 within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue which he/she now disputes.

This dispute resolution process constitutes the sole administrative remedy available under this Agreement.

IX. EXPOSURE TO DOH BUSINESS INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO CONTRACT WORK

During the course of this contract, DOH may inadvertently become aware of information unrelated to this agreement. DOH will treat such information respectfully, recognizing the Information Provider relies on public trust to conduct its work. This information may be hand written, typed, electronic, or verbal, and come from a variety of sources.

X. GOVERNANCE

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington and any applicable federal laws. The provisions of this Agreement shall be construed to conform to those laws.

In the event of an inconsistency in the terms of this Agreement, or between its terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

- Applicable Washington state and federal statutes and rules;
- Any other provisions of the Agreement, including materials incorporated by reference.

XI. HOLD HARMLESS

Each party to this Agreement shall be solely responsible for the acts and omissions of its own officers, employees, and agents in the performance of this Agreement. Neither party to this Agreement will be responsible for the acts and omissions of entities or individuals not party to this Agreement. DOH and the Information Provider shall cooperate in the defense of tort lawsuits, when possible.

XII. LIMITATION OF AUTHORITY

Only the Authorized Signatory for DOH shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of DOH. No alteration, modification, or waiver of any clause or condition of this Agreement is effective or binding unless made in writing and signed by the Authorized Signatory for DOH.

XIII. SEVERABILITY

If any term or condition of this Agreement is held invalid, such invalidity shall not affect the validity of the other terms or conditions of this Agreement, provided, however, that the remaining terms and conditions can still fairly be given effect.

XIV. SURVIVORSHIP

The terms and conditions contained in this Agreement which by their sense and context, are intended to survive the completion, cancellation, termination, or expiration of the Agreement shall survive.

XV. TERMINATION

Either party may terminate this Agreement upon 30 days prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement prior to the effective date of termination.

XVI. WAIVER OF DEFAULT

This Agreement, or any term or condition, may be modified only by a written amendment signed by the Information Provider and DOH. Either party may propose an amendment.

Failure or delay on the part of either party to exercise any right, power, privilege or remedy provided under this Agreement shall not constitute a waiver. No provision of this Agreement may be waived by either party except in writing signed by the Information Provider or DOH.

XVII. ALL WRITINGS CONTAINED HEREIN

This Agreement and attached Exhibit(s) contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement and attached Exhibit(s) shall be deemed to exist or to bind any of the parties hereto.

XVIII. PERIOD OF PERFORMANCE

This **Agreement** shall be effective from January 1, 2024 through December 31, 2028.

Special Terms And Conditions

I. The Washington Department of Children, Youth, and Families (DCYF) is responsible for administering the state's Home Visiting Services Account (HVSA). DCYF administers contracts with local organizations to provide the voluntary home visiting services funded through this account, as one of an array of early childhood and family support services administered with the goal of ensuring that the state's children are thriving and Kindergarten ready. The Department of Health (DOH), under contract to DCYF, provides data management and program evaluation for the HVSA. DCYF and DOH require access to identifiable client level data to carry out responsibilities for program planning, evaluation, and integration of data with the state's educational and health data systems.

- DOH may use identifiable client level data to link with other child health data sets to evaluate program reach, impact of home visiting services, and plan for future home visiting services.
- DCYF will receive identifiable client level data from DOH necessary to link with other early childhood data sets to help identify needs and plan for services.
- DCYF will also conduct its own analyses of HVSA data or may contract with consultants for analyses. DCYF may share client level data with or without direct identifiers with contracted parties to conduct analyses of HVSA program data. Direct identifiers will only be shared for those clients who have consented.
- DOH may share a limited dataset with DCYF contractor to support continuous quality improvement activities with the Information Provider.

In all handling of identifiable client level data DOH, DCYF, and DCYF contractors will abide by state and federal law, as well as their own policies and procedures, for protection of confidential and personally identifiable information.

II. Information Provider will retain all rights and control of client records consistent with its legal and ethical obligations to clients.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date of last signature below.

INFORMATION RECIPIENT
State of Washington Department of Health

INFORMATION PROVIDER
Jefferson County Washington,
for Jefferson County Public Health

Signature	**Signature**
Print Name	**Print Name** **Heidi Eisenhour, Chair** **Jefferson County Board of Commissioners**
Date	**Date**
	Approved as to form only:  December 14, 2023 **Philip C. Hunsucker,** **Date** **Chief Civil Deputy ProsecutingAttorney**

EXHIBIT I

1. PURPOSE AND JUSTIFICATION FOR SHARING THE DATA

Provide a detailed description of the purpose and justification for sharing the data, including specifics on how the data will be used.

This data sharing agreement addresses the disclosure of client and program services data required of the Information Provider funded by the Home Visiting Services Account (HVSA) in Washington State to meet evaluation, quality assurance and improvement, data collection and reporting as required by the Department of Children, Youth, and Families. **RCW 43.216.130 – Authorization of the Home Visiting Services Account**

DOH is contracted by the Department of Children, Youth, and Families (DCYF) to collect, analyze and report HVSA data to meet DCYF's evaluation, quality assurance and improvement, data collection and reporting requirements.

In order to facilitate families' access to needed services and assessment, assurance and improvement of program quality, DCYF is requiring funded programs to provide identifiable data to DOH. DOH will, in turn use this information for HVSA evaluation activities. DOH will also forward identifiable data to Department of Children, Youth, and Families to carry out its responsibilities for program planning and evaluation per the terms of DOH contractual data sharing agreement with DCYF, information shared is considered confidential. Additionally, DOH will provide potentially identifiable data back to the information provider, per the terms of this current agreement, and DCYF Contractors, per the terms of individual agreements with each partner.

Is the purpose of this agreement for human subjects research that requires Institutional Review Board (IRB) approval?

☐ Yes ☒ No

If yes, has an IRB review and approval been received? If yes, please provide copy of approval. If No, attach exception letter.

☐ Yes ☒ No

2. PERIOD OF PERFORMANCE

This **Exhibit** shall have the same period of performance as the **Agreement** unless otherwise noted below:

Exhibit ___ shall be effective from_____through_____.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement (Include the name of the database and a list of all the data elements being provided):

To accomplish the HVSA reporting requirements, the Information Provider agrees to share all program data routinely collected on clients, as required by HVSA contract requirements, HVSA approved demographic, service utilization, benchmark performance measures and continuous quality assurance and improvement. This agreement permits transfer of client, services and workforce data for all clients served with HVSA funds. Data will include the following: demographics, enrollment and discharge data, dates of home visits, screening results, referral information and assessment results, as well as workforce data on home visitors and supervisors, selected by the program or model to meet HVSA reporting requirements, per the information providers' contract with DCYF for provision of home visiting services, as reads in the attachment: Data Collection, Reporting and HVSA Aligned Measures.

For purposes of this agreement **client** is defined as the primary caregiver(s) and children in the household participating in HVSA-funded services. Workforce is defined as the home visitor and supervisor providing services to the client. Each home visitor and supervisor should be identified with a unique identifier that can be linked to each client he or she works with. Home visit is defined as the modality of service delivery, for enrolled clients during which services are provided and information collected or documented.

Data to be shared will be entered by Information Provider into electronic databases approved by DOH within 5-7 business days of collection and the prior months data should be entered within 5-7 business days of after prior month of service ends.

Information provider will obtain consent from families and maintain consents on record. Consents should be shared with DOH every month within 30 days after the month ends. Consent will authorize Information Recipient to also complete other performance measurement reporting on performance indicators such as Child Maltreatment.

RESPONSIBILITIES
Data Provider:

- Amend program consent documents to assure that clients are queried for consent to use of identified data for reporting and quality improvement purposes within 3 visits after enrollment.
- Ensure collection of any HVSA required data elements.
- Assign a responsible staff member to manage the data sharing agreement and act as principal liaison to DOH for this work.
- Complete data collection and transfer on the time schedule identified in Attachment A.
- Assist DOH staff in addressing any data quality and implementation problems.

DOH:

- Design and support the data transfer processes.
- Train and provide technical assistance to staff for the effective and efficient collection and sharing of data as described in this agreement.
- Produce program specific reports as requested by the program and specific to the continuous quality assurance and improvement, this may involve the sharing of potentially identifiable (category 3 or 4) data with Information Provider, DCYF or DCYF contractor. Our intent is to work with programs to provide reports based on program needs and interest and the within the workload permitted in the DOH's contract with DCYF.
- Use the shared data to develop HVSA report information and reduce reporting burden to programs wherever possible.
- Monitor areas where required improvement was attained or not and report results to Information Provider. Summary results may also be reported to DCYF and DCYF contractor for quality improvement purposes
- Data provided to DOH for HVSA activities will be maintained for three (3) years after the end of the Home Visiting Services Account. At the end of this time, all electronic and paper printouts of the data held by DOH will be destroyed.
- Maintain a data archive that will be updated monthly by the Data Provider's data transfers.
- Extract client level data necessary for DCYF and DOH federal reporting.
- Coordinate any necessary amendments to this data sharing agreement.

The information described in this section is:

☒ Restricted Confidential Information (Category 4)

☐ Confidential Information (Category 3)

☐ Potentially identifiable information (Category 3)

☐ Internal [public information requiring authorized access] (Category 2)

☐ Public Information (Category 1)

Any reference to data/information in this Agreement shall be the data/information as described in this Exhibit.

4. STATUTORY AUTHORITY TO SHARE INFORMATION

DOH statutory authority to obtain and disclose the confidential information or limited Dataset(s) identified in this Exhibit to the Information Provider:

RCW 43.20.050 – Powers and duties of state board of health
RCW 43.70.050 – Collection, use, and accessibility of health-related data
RCW 70.02.050 – Disclosure without patient's authorization

DCYF statutory authority to disclose the confidential or limited Dataset(s):
RCW 43.216.159 – Home visitation programs – Funding – Home visitation services coordination or consolidation plan.

5. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

- ☐ DOH Web Application (indicate application name):
- ☒ Washington State Managed File Transfer Service (mft.wa.gov)
- ☐ Encrypted CD/DVD or other storage device
- ☐ Health Information Exchange (HIE)**
- ☒ Other: (describe the methods for access/transfer)**

  For Nurse Family Partnership (NFP) programs, DOH staff will access the National Service Organization's database and download data directly to DOH through their https protocol.

  For any programs using the national VisitTracker data system managed by DataKeepers, DOH staff will access the data system and download data directly through their https protocol.

  For other HVSA-funded programs, data will be shared with DOH via MFT.

****NOTE:** DOH Chief Information Security Officer must approve prior to Agreement execution. DOH Chief Information Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

FREQUENCY OF ACCESS/TRANSFER

- ☐ One time: DOH shall deliver information by _____ (insert date)
- ☒ Repetitive: frequency or dates see Attachment A
- ☐ As available within the period of performance stated in Section 2.

6. DATA DISPOSITION

Unless otherwise directed in writing by the DOH Business Contact, at the end of this Agreement, or at the discretion and direction of DOH, the Information Recipient shall:

- ☐ Immediately destroy all copies of any data provided under this Agreement after it has been used for the purposes specified in the Agreement . Acceptable methods of destruction are described in Appendix B. Upon

completion, the Information Recipient shall submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐ Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes specified in the Agreement, along with the attached Certification of Data Disposition (Appendix C)

☐ Retain the data for the purposes stated herein for a period of time not to exceed _____ (e.g., one year, etc.), after which Information Recipient shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☒ Other (Describe): Retain the data for the purposes stated herein for a period of time not to exceed five years following the end of the Home Visiting Services Account, after which DOH shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

7. RIGHTS IN INFORMATION

DOH agrees to provide, if requested, copies of any research papers or reports prepared as a result of access to DOH information under this Agreement for DOH review prior to publishing or distributing.

In no event shall the Information Provider be liable for any damages, including, without limitation, damages resulting from lost information or lost profits or revenue, the costs of recovering such Information, the costs of substitute information, claims by third parties or for other similar costs, or any special, incidental, or consequential damages, arising out of the use of the information. The accuracy or reliability of the Information is not guaranteed or warranted in any way and the information Provider's disclaim liability of any kind whatsoever, including, without limitation, liability for quality, performance, merchantability and fitness for a particular purpose arising out of the use, or inability to use the information.

☐ If checked, please submit the following:

8. ALL WRITINGS CONTAINED HEREIN

This Agreement and attached Exhibit(s) contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement and attached Exhibit(s) shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the parties have executed this Exhibit as of the date of last signature below.

INFORMATION RECIPIENT
State of Washington Department of Health

INFORMATION PROVIDER
Jefferson County Washington,
for Jefferson County Public Health

Signature	**Signature**
Print Name	**Print Name** **Heidi Eisenhour, Chair** **Jefferson County Board of Commissioners**
Date	**Date**

APPENDIX A

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it. Below are key elements:

A. CONFIDENTIAL INFORMATION

Confidential information is information federal and state law protects from public disclosure. Examples of confidential information are social security numbers, and healthcare information that is identifiable to a specific person under RCW 70.02. The general public disclosure law identifying exemptions is RCW 42.56.

B. ACCESS AND USE OF CONFIDENTIAL INFORMATION

1. Access to confidential information must be limited to people whose work specifically requires that access to the information.
2. Use of confidential information is limited to purposes specified elsewhere in this Agreement.

C. DISCLOSURE OF CONFIDENTIAL INFORMATION

1. DOH may disclose an individual's confidential information received or created under this Agreement to that individual or that individual's personal representative consistent with law.
2. DOH may disclose an individual's confidential information, received or created under this Agreement only as permitted under the ***Re-Disclosure of Information*** section of the Agreement, and as state and federal laws allow.

D. CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE

DOH's unauthorized use or disclosure of confidential information is the basis for the Information Provider immediately terminating the Agreement. DOH may also be subject to administrative, civil and criminal penalties identified in law.

E. ADDITIONAL DATA USE RESTRICTIONS: (if necessary)

Signature: _____

Date: _____

APPENDIX B

DATA SECURITY REQUIREMENTS

Protection of Data

The storage of Category 3 and 4 information outside of the State Governmental Network requires organizations to ensure that encryption is selected and applied using industry standard algorithms validated by the NIST Cryptographic Algorithm Validation Program. Encryption must be applied in such a way that it renders data unusable to anyone but authorized personnel, and the confidential process, encryption key or other means to decipher the information is protected from unauthorized access. All manipulations or transmissions of data within the organizations network must be done securely.

DOH agrees to store information received under this Agreement (the data) within the United States on one or more of the following media, and to protect it as described below:

A. Passwords

1. Passwords must always be encrypted. When stored outside of the authentication mechanism, passwords must be in a secured environment that is separate from the data and protected in the same manner as the data. For example passwords stored on mobile devices or portable storage devices must be protected as described under section *F. Data storage on mobile devices or portable storage media*.

2. Complex Passwords are:
   - At least 8 characters in length.
   - Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
   - Do not contain the user's name, user ID or any form of their full name.
   - Do not consist of a single complete dictionary word but can include a passphrase.
   - Do not consist of personal information (e.g., birthdates, pets' names, addresses, etc.).
   - Are unique and not reused across multiple systems and accounts.
   - Changed at least every 120 days.

B. Hard Disk Drives / Solid State Drives – Data stored on workstation drives:

1. The data must be encrypted as described under section *F. Data storage on mobile devices or portable storage media*. Encryption is not required when Potentially Identifiable Information is stored temporarily on local workstation Hard Disk Drives/Solid State Drives. Temporary storage is thirty (30) days or less.

2. Access to the data is restricted to authorized users by requiring logon to the local workstation using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts and remain locked for at least 15 minutes, or require administrator reset.

C. Network server and storage area networks (SAN)

1. Access to the data is 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.

2. Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

3. The data are located in a secured computer area, which is accessible only by authorized personnel with access controlled through use of a key, card key, or comparable mechanism.

4. If the servers or storage area networks are not located in a secured computer area **or** if the data is classified as Confidential or Restricted it must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.

D. Optical discs (CDs or DVDs)

1. Optical discs containing the data must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.
2. When not in use for the purpose of this Agreement, such discs must be locked in a drawer, cabinet or other physically secured container to which only authorized users have the key, combination or mechanism required to access the contents of the container.

E. Access over the Internet or the State Governmental Network (SGN).

1. When the data is transmitted between DOH and the Information Provider, access is controlled by the DOH, who will issue authentication credentials.

2. Information Provider will notify DOH immediately whenever:

a) An authorized person in possession of DOH issued credentials is terminated or otherwise leaves the employ of the Information Provider;

b) Whenever a person's duties change such that the person no longer requires access to perform work for this Contract.

3. The data must not be transferred or accessed over the Internet by the Information Provider in any other manner unless specifically authorized within the terms of the Agreement.

   a) If so authorized the data must be encrypted during transmissions using a key length of at least 128 bits. Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required.

   b) Authentication must occur using a unique user ID and Complex Password (of at least 10 characters). When the data is classified as Confidential or Restricted, authentication requires secure encryption protocols and multi-factor authentication mechanisms, such as hardware or software tokens, smart cards, digital certificates or biometrics.

   c) Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

F. Data storage on mobile devices or portable storage media

1. Examples of mobile devices are: smart phones, tablets, laptops, notebook or netbook computers, and personal media players.

2. Examples of portable storage media are: flash memory devices (e.g. USB flash drives), and portable hard disks.

3. The data must not be stored by DOH on mobile devices or portable storage media unless specifically authorized within the terms of this Agreement. If so authorized:

   a) The devices/media must be encrypted with a key length of at least 128 bits, using industry standard mechanisms validated by the National Institute of Standards and Technologies (NIST).

      - Encryption keys must be stored in a secured environment that is separate from the data and protected in the same manner as the data.

   b) Access to the devices/media is controlled with a user ID and a Complex Password (of at least 6 characters), or a stronger authentication method such as biometrics.

c) The devices/media must be set to automatically wipe or be rendered unusable after no more than 10 failed access attempts.

d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactivity activity period of 3 minutes or less.

e) The data must not be stored in the Cloud. This includes backups.

f) The devices/ media must be physically protected by:

- Storing them in a secured and locked environment when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

4. When passwords and/or encryption keys are stored on mobile devices or portable storage media they must be encrypted and protected as described in this section.

G. Backup Media

The data may be backed up as part of DOH's normal backup process provided that the process includes secure storage and transport, and the data is encrypted as described under *F. Data storage on mobile devices or portable storage media.*

H. Paper documents

Paper records that contain data classified as Confidential or Restricted must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records is stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

I. Data Segregation

1. The data must be segregated or otherwise distinguishable from all other data. This is to ensure that when no longer needed by the DOH, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

2. When it is not feasible or practical to segregate the data from other data, then ***all*** commingled data is protected as described in this Exhibit.

J. Data Disposition

If data destruction is required by the Agreement, the data must be destroyed using one or more of the following methods:

Data stored on:	Is destroyed by:
Hard Disk Drives / Solid State Drives	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 , or Delete the data and physically and logically secure data storage systems that continue to be used for the storage of Confidential or Restricted information to prevent any future access to stored information. One or more of the preceding methods is performed before transfer or surplus of the systems or media containing the data.
Paper documents with Confidential or Restricted information	On-site shredding, pulping, or incineration, or Recycling through a contracted firm provided the Contract with the recycler is certified for the secure destruction of confidential information.
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a course abrasive.
Magnetic tape	Degaussing, incinerating or crosscut shredding.
Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data. Physically destroying the disk. Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.

K. Notification of Compromise or Potential Compromise

The compromise or potential compromise of the data is reported to DOH as required in Section II.C.

APPENDIX C

CERTIFICATION OF DATA DISPOSITION

Date of Disposition _____

☐ All copies of any Datasets related to agreement DOH#_____ have been deleted from all data storage systems. These data storage systems continue to be used for the storage of confidential data and are physically and logically secured to prevent any future access to stored information. Before transfer or surplus, all data will be eradicated from these data storage systems to effectively prevent any future access to previously stored information.

☐ All copies of any Datasets related to agreement DOH#_____ have been eradicated from all data storage systems to effectively prevent any future access to the previously stored information.

☐ All materials and computer media containing any data related to agreement DOH #_____ have been physically destroyed to prevent any future use of the materials and media.

☐ All paper copies of the information related to agreement DOH #_____ have been destroyed on-site by cross cut shredding.

☐ All copies of any Datasets related to agreement DOH #_____ that have not been disposed of in a manner described above, have been returned to DOH.

☐ Other

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in agreement DOH # _____, Section J, Disposition of Information, have been fulfilled as indicated above.

_____ _____

Signature of data recipient Date

APPENDIX D

DOH SMALL NUMBERS GUIDELINES

- Aggregate data so that the need for suppression is minimal. Suppress all non-zero counts which are less than ten.

- Suppress rates or proportions derived from those suppressed counts.

- Assure that suppressed cells cannot be recalculated through subtraction, by using secondary suppression as necessary. Survey data from surveys in which 80% or more of the eligible population is surveyed should be treated as non-survey data.

- When a survey includes less than 80% of the eligible population, and the respondents are unequally weighted, so that cell sample sizes cannot be directly calculated from the weighted survey estimates, then there is no suppression requirement for the weighted survey estimates.

- When a survey includes less than 80% of the eligible population, but the respondents are equally weighted, then survey estimates based on fewer than 10 respondents should be "top-coded" (estimates of less than 5% or greater than 95% should be presented as 0-5% or 95-100%).

ATTACHMENT A

Information Provider will provide a unique identifier to HVSA funded clients and use this identifier to designate data for clients consistently by funding code, as designated by DOH.

All data for HVSA clients served by Information Provider will be shared with DOH by one of the following protocols.

1. Local Program Generation and Transfer of Data for programs not utilizing approved database. Information Provider will:
    a) Export all client data in Excel (.xls) or Txt (.txt) tables. When providing multiple tables, tables must include unique client identifiers to link the tables together into a complete data set
    b) Restrict data to only HVSA reportable clients.
    c) Data will be shared using a method approved by DOH.

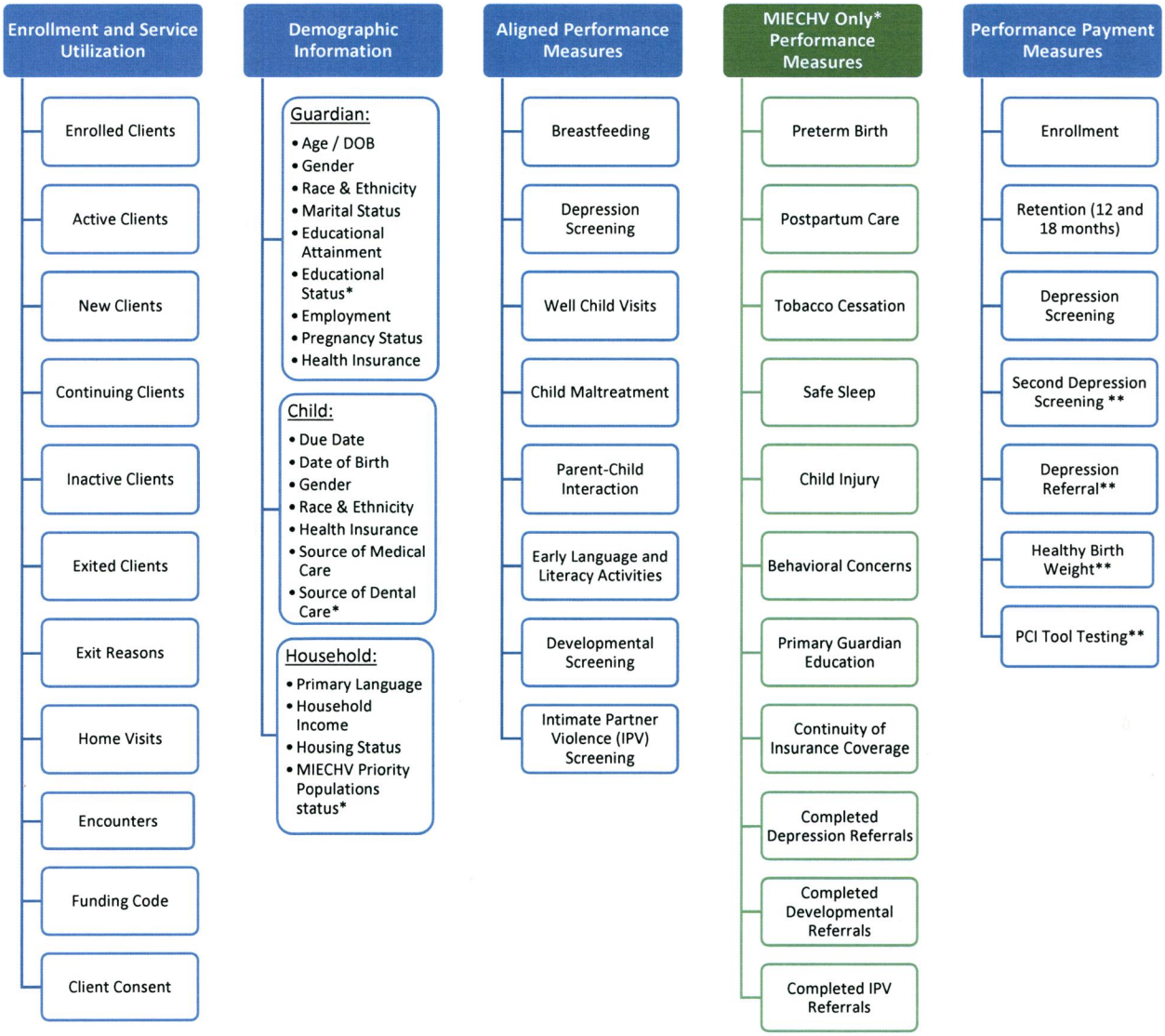
2. Direct Transfer of Program Data from national service organization's data system
   DCYF and DOH have entered into data sharing agreement with the national service organizations and national data systems to receive all Information Provider data entered into the national data systems.

Schedule of Data Provision

Data transfers will occur minimally on a monthly basis unless otherwise approved by DOH. Programs are expected to (1) keep client data updated within five to seven business data of data collection and within five to seven business days of end of prior month and (2) help DOH address data quality and interpretation concerns as needed to accurately reflect client served.

ATTACHMENT B

HVSA Aligned, MIECHV, and Performance Payment Measures & Data Elements



*Required for MIECHV-funded programs only

**PBC measures dependent on Model