1 SNOHOMISH COUNTY COUNCIL
2 SNOHOMISH COUNTY, WASHINGTON
3
4 ORDINANCE NO. 24-090
5
6 APPROVING DATA SHARING AGREEMENT WITH STATE OF WASHINGTON
7 DEPARTMENT OF HEALTH FOR THE REFUGEE HEALTH PROMOTION PROGRAM
8
9 WHEREAS, Snohomish County, through its Health Department, wishes to enter
10 into a data sharing agreement with State of Washington Department of Health (DOH) to
11 outline the conditions that require the Health Department to submit required Refugee
12 Health Promotion (RHP) program data to DOH; and
13
14 WHEREAS, the goal of the RHP program, funded by the Office of Refugee
15 Resettlement (ORR), is to promote the health and well-being of refugees and other
16 ORR eligible communities; and
17
18 WHEREAS, the Snohomish County Health Department must share collected
19 data with DOH in order to fulfill ORR reporting requirements and receive funding
20 provided through the DOH Consolidated Contract; and
21
22 WHEREAS, data sharing between agencies are core public health services that
23 the Snohomish County Health Department performs; and
24
25 WHEREAS, the County Council held a public hearing on December 11, 2024, to
26 consider approving the data sharing agreement with State of Washington Department of
27 Health and to authorize the Snohomish County Executive to enter into such agreement
28 in substantially the form attached as Exhibit A;
29
30 NOW, THEREFORE, BE IT ORDAINED:
31
32 Section 1. The County Council hereby adopts the foregoing recitals as findings of
33 fact and conclusions as if set forth in full herein.
34
35 Section 2. The County Council hereby authorizes the County Executive, or
36 designee, to execute the data sharing agreement between Snohomish County and
37 State of Washington Department of Health in substantially the form attached hereto as
38 Exhibit A.
39
40
41 PASSED this 11th day of December, 2024.
42
43
44

SNOHOMISH COUNTY COUNCIL
Snohomish County, Washington

_____
Council Chair

ATTEST:

_____
Deputy Clerk of the Council

(X) APPROVED
( ) EMERGENCY
( ) VETOED

DATE: _____December 11, 2024_____

_____
County Executive

ATTEST:

_Melissa Geraghty_____

Approved as to form only:

Guadamud, Rebecca
Digitally signed by Guadamud, Rebecca
Date: 2024.09.16 15:12:08 -07'00'

_____
Deputy Prosecuting Attorney

DATA SHARING AGREEMENT
For
CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)
Between
STATE OF WASHINGTON
DEPARTMENT OF HEALTH
And
SNOHOMISH COUNTY

This Agreement documents the conditions under which the Washington State Department of Health (DOH) shares confidential information or limited Dataset(s) with other entities.

CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION

	INFORMATION RECIPIENT	INFORMATION PROVIDER
Organization Name	Washington State Department of Health (DOH)	Snohomish County
Business Contact Name	Jasmine Matheson	Katie Curtis
Title	Refugee and Immigrant Health Program Manager	Prevention Services Director
Address	1610 NE 150th Street Shoreline, WA 98155	3020 Rucker Ave., Ste. 203, Everett, WA 98201
Telephone #	360-490-7300	425-339-8711
Email Address	Jasmine.Matheson@doh.wa.gov	Katie.curtis@co.snohomish.wa.us
IT Security Contact	John Weeks	Jim Kamp
Title	Chief Information Security Officer	Business Analyst
Address	PO Box 47890 Olympia, WA 98504-7890	3020 Rucker Ave., Ste. 306, Everett, WA 98201
Telephone #	360-999-3454	425-339-8689
Email Address	Security@doh.wa.gov	Jim.Kamp@co.snohomish.wa.us
Privacy Contact Name	Michael Paul	Jannah Abdul-Qadir
Title	DOH Chief Privacy Officer	Public & Privacy Records Officer
Address	P. O. Box 47890 Olympia, WA 98504-7890	3020 Rucker Ave., Ste. 306, Everett, WA 98201
Telephone #	(564) 669-9692	425-339-8641
Email Address	Privacy.officer@doh.wa.gov	Jannah.Abdul-Qadir@co.snohomish.wa.us

DEFINITIONS

Authorized user means a Provider's employees, agents, assigns, representatives, independent contractors, or other persons or entities authorized by the data provider 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 media with information recorded on it, such as CDs/DVDs, computers 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.

DOH means the Washington State Department of Health.

DSHS means the Washington State Department of Social and Health Services.

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 contain*s* 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.

Information Provider, as used in the Special Terms and Conditions of this Agreement, means the entity that is disclosing their Data for use by the Data Recipient for completion of this contract.

Information Recipient, as used in the Special Terms and Conditions of this Agreement, means the entity that is receiving the Data from the Data Provider for purposes of completion of this contract.

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

LHJ means Local Health Jurisdiction.

ORIA means the Washington State Department of Social and Health Services, Office of Refugee and Immigrant Assistance.

ORR, as used in the Special Terms and Conditions of this Agreement, means the U.S. Department of Health and Human Services, Administration for Children & Families, Office of Refugee Resettlement.

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.

RADS means refugee Arrivals Data System managed by ORR.

Refugee means a person who is unable to return to his/her home country because of persecution, or a well-founded fear of persecution due to his/her race, religion, nationality, membership in a particular social group, or political opinion. For purposes of this Contract, the term "refugee" also refers to ORR-eligible populations, such as asylees, victims of human

trafficking, Amerasians, Cuban-Haitian entrants, Iraqi and Afghan Special Immigrants, Afghan and Ukrainian Humanitarian parolees and others.

Refugee Health Promotion Provider means DSHS and/or DOH contracted service providers and/or sub-recipients providing Refugee Health Promotion program and services, a federally funded program administered by ORR.

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.

GENERAL TERMS AND CONDITIONS

I.   USE OF INFORMATION

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

II.   SAFEGUARDING INFORMATION

A.   CONFIDENTIALITY

Information Provider agrees to:

- Follow DOH small numbers of 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 Information Provider acknowledges the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

B. SECURITY

The Information Provider 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 OCIO standard 141.10 "Securing Information Technology Assets."

The Information Provider agrees to adhere to the Data Security Requirements in Appendix B. The Information Provider 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 Information Provider 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**

Information Provider 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 Information Provider 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: the Information Provider will notify the DOH Privacy Officer 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 the Information Recipient received the request; and
    - The DOH records that the Information Provider believes are responsive to the request and the identity of the requestor, if known.

IV.   **ATTRIBUTION REGARDING INFORMATION**

Information Recipient agrees to cite Snohomish County Health Department or other citation as specified, as the source of the information subject of this Agreement in all text, tables and references in reports, presentations and scientific papers.

Information Recipient agrees to cite its organizational name as the source of interpretations, calculations or manipulations of the information subject of this Agreement.

V.   **OTHER PROVISIONS**

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

VI.   **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.

VII.   **CAUSE FOR IMMEDIATE TERMINATION**

The Information Recipient and Information Provider acknowledge 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.

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 recipient's and 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. **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.

X. **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.

XI. **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 the 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.

XII. **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.

XIII. **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.

XIV.   <u>**TERMINATION**</u>

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.

XV.   <u>**WAIVER OF DEFAULT**</u>

This Agreement, or any term or condition, may be modified only by a written amendment signed by the Information Provider and the Information Recipient. 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 the Information Recipient.

XVI.   **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.

XVII.   **PERIOD OF PERFORMANCE**

This **Agreement** shall be effective from 9/1/2024 through 9/30/2026.

SPECIAL TERMS AND CONDITIONS

XVIII.

Refugee Health Promotion Providers subcontracted by DOH shall submit required data per DSHS-DOH IAR under contract GVS28843-1, including client demographic information, program engagement data, and program evaluation data. DOH shall manage and maintain client-centered demographic and program engagement data and will share with DSHS the data as requested by ORR on the ORR-6 report or other required reports.

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

INFORMATION PROVIDER	**INFORMATION RECIPIENT**
Snohomish County	**State of Washington Department of Health**

Lacey Harper

Leslie Becker (Sep 16, 2024 08:35 PDT)

Signature	Signature
Lacey Harper	Leslie Becker
Print Name	Print Name
Executive Director	Chief of Innovation & Technology
Title	Title
Dec 16, 2024	Sep 16, 2024
Date	Date

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.

Under RCW 74.74.030 and RCW 74.74.040 the Department of Social and Health services (DSHS) is required to support the economic and social integration and basic needs of immigrants and refugees. DSHS is also required to coordinate with local, state, and federal agencies and other stakeholders to fulfill the duties outlined in RCW 74.74. To accomplish this, DSHS is partnering with the Department of Health (DOH) and permitting them to subcontract with other partners. Please see contract GVS28843-1 for additional details.

The goal of the Refugee Health Promotion (RHP) program, funded by the Office of Refugee Resettlement (ORR), is to promote the health and well-being of refugees and other ORR-eligible communities. RHP focuses on three key service types: 1) providing opportunities to increase health literacy, 2) coordinating health care, and 3) organizing wellness groups. Through an intra-agency agreement, contract number GVS28843-1, Department of Social and Health Services (DSHS) is partnering with Washington State Department of Health (DOH) to provide RHP services to ORR-eligible communities. DOH will subcontract with Local Health Jurisdictions (LHJs) to provide services focused on health literacy and health navigation through community health workers. LHJs have longstanding relationships and connections with local communities, with many having existing community health workers. Community health workers have strong connections with the communities they serve which ensures trust when collecting client demographic data. For those same reasons, LHJs may choose to subcontract with Community Based Organizations to recruit community health workers. The LHJs shall ensure that the subcontractors follow the terms and conditions in this Agreement and Exhibit.

Pursuant to Contract Number CLH 31027, as amended, DOH has contracted with Information Provider, an LHJ, to provide the RHP program services. The purpose of this data sharing agreement is to outline the conditions that require the Information Provider to submit required RHP program data to DOH. LHJs must share collected data with DOH in order to fulfill ORR reporting requirements and receive funding. Per federal regulation, ORR-funded programs may only be administered to eligible recipients. Eligibility information must be submitted as a condition of funding. Participating LHJs will need to submit monthly client demographic data and program participation data in a Monthly Caseload Report (MCR). LHJs applied to receive this funding with the knowledge and acceptance of federal funding requirements.

Required client demographic data includes alien number, first name, middle name, last name, date of birth, gender, immigration status, country of origin, zip code, city, county, and date of eligibility for ORR services. In addition to fulfilling federal reporting requirements, this data will be used to validate that each participant is eligible to receive

RHP services. The program participation data includes start and end dates of service, as well as type of service received. This data will also support program monitoring activities that will inform future decision making regarding RHP services.

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

☐ Yes ☒ **No**

If yes, has a WSIRB 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 I shall be effective from 09/01/2024 through 09/30/2026.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:
Database Name(s): Excel Spreadsheet templates provided by WA DOH
Data Elements being provided:

Data Field	Description
Client Demographics	
Alien Number	Individual's unique seven-, eight-, or nine-digit number assigned by the Department of Homeland Security
Last Name	Individual's last name
First Name	Individual's first name
Middle Name	Individual's middle name
Date of Birth	Individual's date of birth
Immigration Status	Immigration status at the time the individual enrolls and/or receives RHP services
Gender	Reported gender
Country of Origin	Individual's nationality or country of origin
Zip Code	Individual's zip code of residence
City	Individual's city of residence
County	Individual's county of residence

Date of Eligibility	Depending on the individual's immigration status, their date of eligibility may be: Date of arrival Date when granted qualifying status
Primary Language	Individual's primary language
Program Intake	
Intake Date	Date client was initially referred to RHP program and services
Referral Source	Who referred this client to your RHP program?
Primary Need	What is this client's primary need at the time of referral?
All ORR Service Areas	
Start Date	Date when individual begins specified ORR service
End Date	Date when individual completes or is no longer participating in specified ORR service If client is still actively receiving RHP service, leave blank
Provider Notes	Optional space for provider notes
Health Education: Individual Sessions	
Number of Individual, Targeted Sessions	Number of individual, targeted health education sessions this client received this month
Health Education: Group Classes	
Number of Group Classes Attended	Number of group health education classes this client this this month
Increased Knowledge?	Did the client increase their knowledge as a result of attending health education group classes? Each program is required to measure knowledge dependent on program's curriculum and/or program's pre-specified time point for measurement
Health Care Navigation and Support	
Focus Area	What area of health care did you help your client access? The drop-down menu offers three major areas, as well as combinations of the three options.
Outcome	Did the client complete their plan of care? Plan of care and "completion of plan of care" is uniquely defined based on each program and how they offer health care navigation and care coordination. If client is still actively receiving services this month, select "Plan of Care Ongoing"
Program Exit	
Exit Date	Date client exited all RHP services offered by provider

Reason For Exit	Why did the client exit RHP services? The drop-down menu offers five options to describe reason: client moved, is no longer ORR-eligible, is lost to follow-up, completed RHP goals, or other reason.
Provider Notes	Section for RHP provider to add additional details for client's exit

Data elements that DOH will provide to DSHS:
- Client-level refugee health program data sub-contracted to Refugee Health Promotion Providers, as specified in contract between DSHS and DOH for administration of Refugee Health Screening and Refugee Health Promotion programs;
- Other refugee program-related information, used for the purposes of federal reporting and monitoring, evaluation, systems improvement and/or research.

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/Recipient:

RCW 43.70.050 – Collection, use, and accessibility of health-related data
RCW 74.74.030 – Coordination of statewide efforts
RCW 74.74.040 -- Washington state plan for refugee resettlement
RCW 43.70.040 Secretary's powers-Rule making authority-Report to the legislature
RCW 43.70.130 Powers and duties of secretary-General

5. **ACCESS TO INFORMATION**

METHOD OF ACCESS/TRANSFER

☒ DOH Web Application (indicate application name):
WA DOH secure site (e.g. MFT)
☐ Encrypted CD/DVD or other storage device
☐ Health Information Exchange (HIE)**
☐ Other: (describe the methods for access/transfer)**

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

☒ Repetitive: monthly individual report and quarterly narrative report

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 Provider 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 Provider 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 6 years (*e.g., one year, etc.*), after which Information Provider shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐ Other (Describe):

7. RIGHTS IN INFORMATION

Information Provider 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:

- Copies of _____ (insert list of items)_____
  to the attention of: ___(insert name of DOH employee) ___
  at ____(insert address to which material is sent)_____ .

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 PROVIDER	**INFORMATION RECIPIENT**
Snohomish County	**State of Washington Department of Health**
Lacey Harper	*Leslie Becker (Sep 16, 2024 08:35 PDT)*
Signature	Signature
Lacey Harper	Leslie Becker
Print Name	Print Name
Executive Director	Chief of Innovation & Technology
Title	Title
Dec 16, 2024	Sep 16, 2024
Date	Date

APPENDIX A

<u>USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION</u>

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.   An Information Recipient 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.   An Information Recipient may disclose an individual's confidential information, received or created under this Agreement only as permitted under the ***<u>Re-Disclosure of Information</u>*** section of the Agreement, and as state and federal laws allow.

D.   CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE
       An Information Provider's unauthorized use or disclosure of confidential information is the basis for the Information Recipient immediately terminating the Agreement. The Information Provider 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.

The Information Provider 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 such credentials is terminated or otherwise leaves the employ of the Information Recipient;

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 Recipient 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). <u>When the data is classified as Confidential or Restricted</u>, 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 the Information Provider 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 <u>wipe</u> 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 Information Provider'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 Information Provider, 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

<u>CERTIFICATION OF DATA DISPOSITION</u>

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 Provider 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 provider　　　　　　　　　　　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%).