<div align="center">

SNOHOMISH COUNTY COUNCIL
SNOHOMISH COUNTY, WASHINGTON

ORDINANCE NO. 25-007

APPROVING DATA SHARING AGREEMENT WITH WASHINGTON STATE
DEPARTMENT OF HEALTH AND PROVIDING AUTHORITY TO APPROVE ANY
FUTURE AMENDMENTS

</div>

WHEREAS, Snohomish County, acting through its Health Department, needs access to the Washington State Department of Health (DOH) Ryan White HIV/AIDS Program (RWHAP) datasets; and

WHEREAS, the Snohomish County Health Department will collect RWHAP data to be entered into the Washington State DOH's Electronic Client Management System which will be used to support and facilitate health interventions; and

WHEREAS, the County's Health Department will use the RWHAP datasets to monitor health outcomes and adherence to treatment regimens, including tracking trends for public health indicators and preparing reports on specific public health issues; and

WHEREAS, the parties wish to enter into a data sharing agreement for RWHAP datasets and anticipate future amendments to the data sharing agreement; and

WHEREAS, the County Council held a public hearing on _____ to consider approval of the data sharing agreement with the Washington State Department of Health for Ryan White HIV/AIDS Program datasets and to authorize the Snohomish County Executive, or designee, to enter into such agreement in substantially the form attached as Exhibit A, and further to grant the Snohomish County Executive authority to enter into future amendments to the agreement;

NOW, THEREFORE, BE IT ORDAINED:

Section 1. The County Council hereby adopts the foregoing recitals as findings of fact and conclusions as if set forth in full herein.

Section 2. The County Council hereby approves and authorizes the County Executive, or designee, to execute the data sharing agreement with the Washington State Department of Health in substantially the form attached as Exhibit A.

Section 3. The County Council hereby authorizes the County Executive, or designee, to execute all subsequent amendments to the data sharing agreement with the Washington State Department of Health.

1   PASSED this _____ day of _____, 2025.
2
3
4   SNOHOMISH COUNTY COUNCIL
5   Snohomish County, Washington
6
7
8   _____
9   Council Chair
10   ATTEST:
11
12
13   _____
14   Deputy Clerk of the Council
15
16   ( ) APPROVED
17   ( ) EMERGENCY
18   ( ) VETOED
19
20   DATE: _____
21
22
23   _____
24   County Executive
25   ATTEST:
26
27
28   _____
29
30   Approved as to form only:
31
32
33   _____
34   Deputy Prosecuting Attorney
35

DATA SHARING AGREEMENT
For
CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)
Between
STATE OF WASHINGTON
DEPARTMENT OF HEALTH
And
Snohomish County
CLH29554

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	Snohomish County	Washington State Department of Health (DOH)
Business Contact Name	Dennis Worsham	Elizabeth Crutsinger-Perry
Title	Department Director	Director
Address	3020 Rucker Ave, Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8687	(360) 236-3440
Email Address	dennis.worsham@co.snohomish.wa.us	elizabeth.crutsinger-perry@doh.wa.gov
IT Security Contact	Doug Cavit	John Weeks
Title	IT Security Officer	Chief Information Security Officer
Address	3000 Rockefeller Ave, Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-312-0660	360-999-3454
Email Address	doug.cavit@co.snohomish.wa.us	Security@doh.wa.gov
Privacy Contact Name	Jannah Abdul-Qadir	Michael Paul
Title	Public records and Privacy Officer	DOH Chief Privacy Officer
Address	3020 Rucker Ave, Everett, WA 98201	P. O. Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8641	(564) 669-9692
Email Address	Jannah.Abdul-Qadir@co.snohomish.wa.us	Privacy.officer@doh.wa.gov

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 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.

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.

Exceed authorized access is defined by the Computer Fraud and Abuse Act (CFAA) *codified at* 18 U.S.C. §1030 to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."

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 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.

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.

Information Provider represents the Washington State Department of Health

Information Recipient represents the HRSA and/or Syndemic subrecipients, also known as the "contractor".

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

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.

Remote Access: Shall mean providing secured access to a DOH application, computer, or other network resources from a remote site, which is controlled through DOH and/or the Washington State Department of Consolidated Technical Services (CTS) managed secure gateways.

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.

Virtual Private Network Service (VPN)*:* shall mean a private data network that makes use of the public telecommunication infrastructure, maintaining privacy with a tunneling protocol and security procedures.

GENERAL TERMS AND CONDITIONS

I.   <u>USE OF INFORMATION</u>

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

II.   <u>SAFEGUARDING INFORMATION</u>

A. CONFIDENTIALITY

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

B. SECURITY

The Information Recipient 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 Recipient agrees to adhere to the Data Security Requirements in Appendix B. The Information Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient believes are responsive to the request and the identity of the requestor, if known.

IV. ATTRIBUTION REGARDING INFORMATION

Information Recipient agrees to cite "Washington State Department of Health" 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 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.

VIII. CONFLICT OF INTEREST

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

Terminate the right of the Information Recipient 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 Recipient, 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 Recipient as it could pursue in the event of a breach of the Agreement by the Information Recipient. 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.

IX.   DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the DOH and the Information Recipient 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 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.

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

During the course of this contract, the information recipient may inadvertently become aware of information unrelated to this agreement. Information recipient will treat such information respectfully, recognizing DOH 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.

XI.   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.

XII.   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 Recipient shall cooperate in the defense of tort lawsuits, when possible.

XIII.   **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.

XIV.   **RIGHT OF INSPECTION**

The Information Recipient shall provide the DOH and other authorized entities the right of access to its facilities at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Agreement on behalf of the DOH.

 XV.   **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.

XVI.   **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.

XVII.   **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.

XVIII.   **WAIVER OF DEFAULT**

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.

XIX. **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.

XX. **PERIOD OF PERFORMANCE**

This **Agreement** shall be effective from **July 1, 2024,** through **June 30, 2029**. If the contract is amended to extend past this original end date, this Agreement will reflect the end date in the amended contract.

SPECIAL TERMS AND CONDITIONS

XXI. List special terms and conditions imposed for this specific Agreement.

The Information Recipient must complete and sign the "Remote Access Agreement" (Appendix E) prior to gaining access to the Electronic Client Management System (ECMS).

Information Recipients are permitted to enter and access data in the Electronic Client Management System (ECMS) during the time outlined in their contracts and with the consent of the client.

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

INFORMATION PROVIDER

State of Washington Department of Health

_____
Signature

_____
Print Name

_____
Date

INFORMATION RECIPIENT

_____
Signature

_____
Print Name

_____
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.

    As encouraged by the U.S. Department of Health and Human Services - Health Resources and Services Administration HIV/AIDS Bureau (HRSA), establishing data-sharing agreements with other RWHAP recipients, RWHAP subrecipients, and federal programs reduces the burden in eligibility and eligibility confirmation procedures. Information Recipients, also referred to as contracted partners/service providers, are contractually required to obtain client consent to release/share the client's protected health information (PHI), referred to as a Release of Information.

    The Release of Information (ROI) establishes the client's consent and authorization to release the client's specific protected health information to entities designated in the ROI. The ROI must be signed by the client and maintained by the Information Recipient. Protected health information (PHI) is protected under Federal and State laws and cannot be disclosed without the client's written consent unless otherwise permitted or required by law. Clients retain the right to revoke their consent, and thus their ROI, at any time by submitting a written request, except where actions have already been taken based on the previously given consent.

    A client chart (profile record) is created in the Electronic Client Management System (ECMS) data system after the Release of Information (ROI) is obtained by the Information Recipient (contracted partner/service provider). The Information Recipient is contractually required to maintain and document an active ROI in the data system to enroll and maintain service eligibility for state and local funded HIV/HIV-related programs.

    The Information Recipient must comply with all federal laws regarding the protection of health information. Clients have the right to have personal information safeguarded. Partners are obligated to protect this right.

    The **Purpose** of this agreement is to support the Washington State Department of Health (**Information Provider**) in its public health authority to collect data from HRSA and/or Syndemic subrecipients/contractors and support/facilitate health interventions. Data is collected (entered) by the **Information Recipient (HRSA and/or Syndemic funded entity)** into Washington State DOH's Electronic Client Management System (ECMS). This integrated data system is used to collect and monitor information for the purpose of:
    *   Improving health outcomes
    *   Improving service coordination across contracted partners
    *   Complying with program requirements
    *   Improving quality and efficiency of services
    *   Identifying service gaps and tracking client wellness and outcomes
    *   Facilitating program evaluation of program effectiveness

- Reducing challenges grant recipients, subrecipients, and project sponsors face in data integration
- Decreasing duplication of data entry
- Decreasing barriers to accessing and retaining care
- Improving information for resource planning and allocation

Data will be used by the **Information Provider (WA State DOH)** to:
- Monitor and evaluate health outcomes, program compliance, and performance metrics
- Meet federal and state grant requirements, in both compliance and reporting
- Inform decisions on resource planning and allocation

Data will be used by the **Information Recipient** to serve clients according to its contract with DOH. Information Recipient will use data to:
- Monitor health outcomes, performance measures, and adherence to treatment regimens.
- Coordinate services across grant recipients, subrecipients, and project sponsors
- Ensure access to care and services
- For HIV Client Services, comply with the Ryan White grant reporting requirements outlined by HRSA and meet the requirements outlined in the statutes and rule included the Authority to Share section of this document.

Notwithstanding any other provision, the scope of this agreement shall:
- Be limited to information stored in the Electronic Client Management System (ECMS).
- Be limited to the access to the Electronic Client Management System (ECMS), and shall not affect any other program, process, or activity of Washington State Department of Health

The data in the Electronic Client Management System (ECMS) must be used to comply with the purpose of this Agreement and provide the maximum protection of the information that the law allows.

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 shall be effective from _____ through _____.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement: **Database Name(s):** *provide the name(s) of databases here.*

Washington State Department of Health's Electronic Client Management System (ECMS), currently called Provide® Enterprise

Data Elements being provided: *provide all data elements to be shared here. Attachments are not recommended.*

Information Recipients must have informed consent established with client(s) to enter data on behalf of the client into the Electronic Client Management System (ECMS).

The Information Recipient agrees to enter the data elements described in detail in the Information Recipients' contract held with WA DOH and/or with their grant recipient(s) and/or project/partner sponsor(s).

Demographic Data	☐ First and Last Name
	☐ Year of birth
	☐ Ethnicity
	☐ Hispanic subgroup
	☐ Race
	☐ Asian subgroup
	☐ Native Hawaiian or Pacific Islander (NHPI) subgroup
	☐ Gender
	☐ Sex at birth
	☐ Health coverage
	☐ Housing status
	☐ Housing status collection date
	☐ Federal poverty level percent
	☐ HIV/AIDS status
	☐ Risk factors
	☐ Vital status HIV diagnosis year
	☐ New client

	☐ Received services previous year ☐ Residential & Mailing address
Clinical Data	☐ Data First outpatient/ambulatory health service visit date ☐ Outpatient ambulatory health service visits and dates ☐ CD4 counts and dates ☐ Viral load counts and dates ☐ Prescribed ART ☐ Date of first positive HIV test/ HIV/AIDS diagnosis date ☐ Date of OAHS visit after first positive HIV test ☐ Date of Medical Appointment ☐ Health coverage status ☐ Medications ☐ Premiums
Enrollment data	☐ Client demographic elements ☐ Client clinical data elements ☐ Proof of residency ☐ Proof of income ☐ Proof of identity ☐ Health Coverage ☐ Release of information (ROI) ☐ Last Eligibility Confirmation Date ☐ Enrollment status ☐ Disenrollment Reason ☐ HIV/AIDS Status ☐ Insurance assistance enrollment (start date & status) ☐ Insurance assistance type ☐ Medication assistance enrollment (start date & status) ☐ Medication assistance types ☐ Medication transaction records ☐ Premium assistance transaction records ☐ HOPWA Program Enrollment ☐ HOPWA Housing Assistance ☐ HOPWA – TBRA/FBH Housing Units ☐ HOPWA – TBRA/FBH Rent Responsibility

Ryan White Services and/or Syndemic Services data	☐ Progress Logs and Services Provided
	    o Create Date
	    o Create By
	    o Status
	    o Service Category
	    o Service Type
	    o Brief Description
	    o Full Description
	☐ Medical Appointments
	☐ CD4 and/or Viral Load test dates and results

Care Plan data	☐ Comprehensive Assessment - Relevant areas of concern, including but not limited to the following domains: Medical, Other Core Services, Support Services, Sexual Health, Quality of Life, and Domestic Violence
	    o Create Date
	    o Complete Date
	☐ Individual Service Plans (ISP)
	☐ Individual Service Plan Goals
	☐ Acuity Assessment
	☐ Ryan White Housing Plan
	☐ HOPWA Assessment
	☐ PAHR intake, screening, and follow-up assessments

Syndemic Integrative Testing	☐ Demographic data (see above) ☐ HIV test dates and results ☐ STI/STD test dates and results ☐ Referrals ☐ Linkage to Care ☐ Risk Factors ☐ Testing Provider name and site ☐ PrEP usage ☐ Screened for social/behavioral/risk reduction and enrollment services
Syndemic Anonymous Services & Anonymous Integrative Testing	☐ Condom distribution, Reach & Light touch efforts. ☐ HIV test dates and results ☐ STI/STD test dates and results ☐ Referrals ☐ Linkage to Care

☐ **Data Classification**	
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 Recipient:

Collection:

RCW 70.02.050 – Disclosure without patient's authorization

Add any program specific RCWs that allows the data to be shared here:

- RCW 70.02 Medical Records—Health Care Information Access and Disclosure
- RCW 70.02.030 Patient authorization of disclosure—Health care information—Requirement to provide free copy to patient appealing denial of social security benefits.

    RCW 70.24.400 Funding for office on AIDS—Center for AIDS education—Department's duties for awarding grants.

    WAC 246-08-390 (7) Acquisition, security, retention, disclosure and destruction of health information.

Information Recipient's statutory authority to receive the confidential information or limited Dataset(s) identified in this Exhibit—
- RCW 70.02.290 Use/destructions of health care information by certain state and

local agencies

WAC 246-08-390(7) Acquisition, security, retention, disclosure and destruction of health information.

RCW 70.24.400 Funding for office on AIDS—Center for AIDS education—Department's duties for awarding grants.

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: Electronic Client Management System (ECMS) and/or DOH Managed File Transfer (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 _____ (insert dates if applicable)
- ☒ As available within the period of performance stated in Section 2.

6. **REIMBURSEMENT TO DOH**

Payment for services to create and provide the information is based on the actual expenses DOH incurs, including charges for research assistance when applicable.

Billing Procedure

- Information Recipient agrees to pay DOH by check or account transfer within 30 calendar days of receiving the DOH invoice.

- Upon expiration of the Agreement, any payment not already made shall be submitted within 30 days after the expiration date or the end of the fiscal year, which is earlier.

Charges for the services to create and provide the information are:

☐ $_____

☒   No charge.

7. 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):

8. RIGHTS IN INFORMATION

Information Recipient 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 _____ (<u>insert list of items</u>) ____
  to the attention of: __(<u>insert name of DOH employee</u>) __
  at ___(<u>insert address to which material is sent</u>)____ .

9. 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**
State of Washington Department of Health	
Signature	Signature
Print Name	Print Name
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.   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 ***Re-Disclosure of Information*** section of the Agreement, and as state and federal laws allow.

D.   CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE
        An Information Recipient's unauthorized use or disclosure of confidential information is the basis for the Information Provider immediately terminating the Agreement. The Information Recipient 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 Recipient 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 Recipient, access is controlled by the DOH, who will issue authentication credentials.

   2. Information Recipient 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 Recipient 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 Recipient'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 Recipient, 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. 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#HSP29546 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# HSP29546 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 # HSP29546 have been physically destroyed to prevent any future use of the materials and media.

☐　All paper copies of the information related to agreement DOH # HSP29546 have been destroyed on-site by cross cut shredding.

☐　All copies of any Datasets related to agreement DOH # HSP29546 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 # HSP29546, Section J, Disposition of Information, have been fulfilled as indicated above.

_____　　　_____
Signature of data recipient　　　　　　　　　　　　　　Date

APPENDIX D

<u>DOH SMALL NUMBERS GUIDELINES</u>

K. 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.

- 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%).

ADDITIONAL DATASET SPECIFIC SMALL NUMBERS REQUIREMENTS

- Dataset specific small numbers requirements (delete if not needed).

APPENDIX E

Remote Access Agreement

Name and Address of Information Recipient:

    Information Recipient signature authority

    Name: Snohomish County

    Address: 3020 Rucker Ave, Everett, WA 98201

Scope of Remote Access Agreement:

This REMOTE ACCESS Agreement (Agreement) is entered into by and between Harborview Medical Center (Information Recipient), and Washington State Department of Health (DOH), and is effective as of date of execution of the above Data Sharing Agreement. This agreement outlines the terms and conditions under which the Information Provider will provide Remote Access Service to Information Recipient.

The REMOTE ACCESS service will provide a secure means for Information Recipient to access Washington State Department of Health's the Electronic Client Management System (ECMS).

This agreement defines REMOTE ACCESS requirements for the Information Recipient to access DOH's Electronic Client Management System (ECMS) as defined under this Agreement.

1. **Terms**

The terms of this Agreement shall be in effect upon the date of execution by both parties and shall remain in full force until the end of the above Data Sharing Agreement, or terminated by either party , or until the Information Recipient's remote access is terminated.

Information Recipient acknowledges and understands the provision of REMOTE ACCESS is dependent on third-party providers. Information Provider shall not be held liable for actions or inactions of such third-party providers.

2. **Information Recipient Requirements**

A. Security Patch Updates and Anti-virus Software:
Information Recipient agrees to maintain security patch updates at current levels and to implement and maintain comprehensive anti-virus/malware protection (including upgrades and patches) consistent with industry standards and Washington State IT Security Standards, on all devices used by Information Recipient under this Agreement.

B. Information Recipient agrees to refrain from the following:
   a. Use of the REMOTE ACCESS service for any unlawful purpose
   b. Transmission of any content that is obscene pornographic, libelous, invasive of privacy rights, or advocates violence, bigotry, or bias based on race, color, religion, ancestry, national origin, gender orientation, or physical or mental disability.
   c. Accessing any data and/or networks to which Information Recipient does not have prior authorization to access
   d. Altering, tampering, or otherwise modifying the REMOTE ACCESS service, or the software or hardware used to provide the REMOTE ACCESS.
   e. Providing access to the REMOTE ACCESS service for others not affiliated with Information Recipient.
   f. Use of the REMOTE ACCESS for means other than performing a purpose reasonably related to contract referenced in this agreement.
   g. Impersonating any person or entity, including, but not limited to, an Agency or Washington State official, falsely state or otherwise misrepresent your affiliation with an Agency or the State of Washington.
   h. Modifying, publishing, transmitting, transferring or selling, reproducing, creating derivative works from, distributing, performing, linking, displaying or in any way exploiting any content from any Information Provider database
   i. Use or attempted use of the REMOTE ACCESS service after termination of this Agreement Uploading, posting, E-mailing, otherwise transmitting, or posting links to any material that contains software viruses, worms, Trojan horses, time bombs, trap doors or any other computer code, files or programs or repetitive requests for information designed to interrupt, destroy or limit the functionality of any Agency computer software or hardware, telecommunications equipment,

or Agency data or to diminish the quality of, interfere with the performance of, or impair the functionality of the REMOTE ACCESS service.

j. Use of the REMOTE ACCESS to connect a LAN or other network to Agency's network

k. Use of any mechanism to enable the number of Authorized Information Recipient concurrently accessing the service to exceed the number of concurrent logons provided for in the Agreement.

l. Use of any mechanism to enable the Information Recipient to exceed authorized access beyond the scope of this remote access security Agreement or the terms of the Information Recipient's contract with the Information Provider

m. Tapering, corrupting, altering, or modifying in any respect, the information or any data, instructions, commands or programs stored/contained in or on the site

n. Acting in any way to provide an electronic hub or switch allowing third parties to access to the REMOTE ACCESS service via Internet or any other method

3. Security Authentication Appliance

If REMOTE ACCESS will be provided through a Virtual Private Network (VPN), Information Recipient may be required to install VPN client software and/or obtain a SecureID token issued by DOH. Information Recipient must return all DOH-supplied software and/or hardware upon termination of REMOTE ACCESS services.

Treatment of Confidential Information

Information Recipient acknowledges that some of the information, which may come into its possession or knowledge in connection with Information Recipient' s use of the REMOTE ACCESS service, is classified as Restricted Confidential Information. Information Recipient agrees to hold all such Confidential Information in strictest confidence and will not release or make any use of such Confidential Information for any purpose other than as permitted by in the terms of the above Data Sharing Agreement.

Information Recipient agrees to implement physical, electronic, and administrative safeguards that are consistent with the requirements in the above Information Sharing Agreement and Appendixes.

Except as permitted by the above Information Sharing Agreement, Information Recipient agrees not to collect, store, sell or distribute any Confidential Information collected or derived from its use of the REMOTE ACCESS service.

Violation of this section by Information Recipient may result in immediate termination of this Agreement, monetary damages, and/or civil and criminal penalties.

Indemnification

Information Recipient agrees to promptly defend and indemnify, and to hold harmless from, against and in respect of, and pay or reimburse for, any and all claims, demands, liabilities,

losses, damages, costs and expenses, including reasonable attorneys' fees, of the State of Washington, its employees, and other Information Recipients, arising from, relating to or in connection with an actual breach by Information Recipient of Information Recipient's obligations under this Agreement. Information Recipient further agrees to cooperate fully with the Information Provider and legal counsel in resolving any claim or dispute

Blocking of Remote Access

Information Recipient acknowledges that Information Provider or its third-party providers shall have the right to block Information Recipient's access to the REMOTE ACCESS service, in whole or in part, at any time, for any reason.

Declaration of Remote Access Service Information Recipient

Information Recipient verifies the following Information Recipient will fully represent its responsibilities as listed in this remote access security agreement and all related service contracts.

Information Recipient will notify DOH of any change in the employment status of authorized employees. This includes termination of employment, transfer to another group, or leave of absence. Additionally, Information Recipient will notify the DOH within 1 day of suspected or actual unauthorized use of the REMOTE ACCESS service.

Execution

This document constitutes the entire Agreement and supersedes all prior communication, understandings, and agreements relating to the subject matter of this Agreement, whether oral or written. Alterations to this Agreement are valid only if made in writing and signed by authorized representatives of both parties.

IN WITNESS WHEREOF, the undersigned has caused this Agreement to be executed as of the Date written below.

Information Recipient signature authority

Name: _____

Signature: _____

Title: _____

Date: _____

APPENDIX F

Example of WA State Early Intervention Program's 'Release of Information/Assignment of Benefits' documentation required for program enrollment.

Health — Washington State Department of

EARLY INTERVENTION PROGRAM (EIP) CONFIDENTIAL APPLICATION
PO Box 47841, Olympia, WA, 98504 Toll Free Phone – 1-877-376-9316 Fax – 360-664-2216

SIGNATURE PAGE: AGREEMENT, RELEASE OF INFORMATION AND ASSIGNMENT OF BENEFITS

The following agencies coordinate and verify eligibility for all applicable services, as well as treatment and care coordination with other programs related to EIP. They all adhere to the same confidentiality requirements listed below:
- Pharmacy Benefits Manager/Ramsell Corporation • Insurance Benefits Manager/Evergreen Health Insurance Program (EHIP)
- WA State Department of Employment Security (Income Verification Services) • WA State Department of Social and Health Services (Medicaid Verification)
- WA State Health Care Authority (Apple Health) • All EIP contracted Providers • System Software Vendor

By signing this document, I agree that I have read this application, certify that the information in this application is true and accurate to the best of my knowledge, and understand the following:

I have the right to:
1. Be treated with respect, consideration and honesty.
2. Receive services without discrimination on the basis of race, color, sex/gender, ethnicity, national origin, religion, age, class, or sexual orientation, as well as physical or mental ability.
3. Have my records be treated as confidential.
4. File an appeal about eligibility and coverage decisions.

I have the responsibility to:
1. Treat Department of Health staff and contracted service partners with respect, consideration and honesty.
2. Give correct, current, and complete information.
3. Respond to the Programs request(s) for information.
4. Reimburse the Program for any and all premium or benefit reimbursement payments that are paid to me in error during my enrollment.
5. Reimburse the Program if premiums are paid on my behalf for excess advance premium tax credit received as part of an Income Tax refund, if applicable.
6. File income tax forms, if applicable.
7. Update my income in the WA Healthplanfinder and with EIP if I have a Qualified Health Plan through WA Health Benefits Exchange.
8. Notify the Program, or have my Case Manager notify the Program, of any changes that affect my eligibility within 20 days. These changes include, but are not limited to: income, address, family size and health insurance coverage.
9. Apply for other services for which I may be eligible before I receive services from EIP.
10. Submit information regarding my continued eligibility for participation in the Program(s), including proof of income, proof of residency, availability of health insurance coverage, and an updated and signed version of this form with my recertification application every (6 months) as per Federal Guidelines.

I understand that:
1. The information requested on this application is for the purpose of determining my eligibility for state and federally funded services.
2. The funding is limited and may expire at any time without extended or alternate funds being available.
3. The Program will use other state and federal data systems as well as other information to verify the information I give them.
4. Upon approval, my eligibility will expire after six months. Before the conclusion of those six months, I will be required to reapply and provide updated eligibility information to continue receiving services.
5. I may have to pay a fee, called a cost share, to receive Program services.
6. If I am considered eligible for services, my information may be utilized by our contractual partners to provide Program services.
7. Eligibility approval does not mean I will receive or be enrolled in all available services. I understand each service may require additional information, and that I must provide this information for verification before enrollment into said services.
8. If I am approved for premium assistance:
   a. I will need to select EHIP as my Sponsorship Representative for a Qualified Health Plan in the WA Healthplanfinder, if applicable. By selecting EHIP as my sponsor, I authorize EHIP to communicate and share information with the WA Healthplanfinder.
   b. I must notify the Program & EHIP of any changes to my insurance coverage such as:
      i. Receiving insurance from my job, Medicaid, Medicare, partner, spouse or other source(s).
      ii. Receiving a premium statement, premium coupon or coupon book.
      iii. Receiving a late premium notice, letter or phone call.
      iv. Receiving a premium change notice or letter.
   c. I give the Program & EHIP authorization to communicate and share information about my Qualified Health Plan (QHP), Healthcare for Workers with Disabilities (HWD), Medicare Part D (PDP) or Employer Sponsored Insurance (ESI) through myself, my parent(s), my partner, my spouse's employer.
   d. I authorize and direct my health insurer to directly reimburse the Program for any unused premium payments should my insurance policy terminate or be cancelled for any reason, including but not limited to future ineligibility, voluntary termination, involuntary cancelation, termination by operation of law, or death.
   e. If I want to revoke this authorization and terminate the agreement, I must do so in writing to both insurance benefits manager and the health plan administrator.

Release of Information: I give my permission for the program to share information from this application and from subsequent documentation obtained by the program with contracted partners, case managers, and the family/friends I listed in the Authorized Representative section of this application. I give this permission for one year and 60 days from the date I sign this authorization.

Assignment of Benefits: I hereby assign to the State of Washington Department of Health any right to drug or medical benefits to which I may be entitled under any other plan of assistance or insurance from any other liable third party. I consent to the assignment of these benefits to Washington State Department of Health and I understand that the Washington State Department of Health is entitled to repayment for incorrectly provided benefits or benefits to which a third party is liable.

_____   _____
Applicant or Legal Guardian Signature **Do Not Leave Blank**   Today's Date (mm/dd/yyyy) **Do Not Leave Blank**

Client Name:_____   EIP Client ID: _____