SNOHOMISH COUNTY COUNCIL
SNOHOMISH COUNTY, WASHINGTON

ORDINANCE NO. 23-091

APPROVING AGREEMENT WITH WASHINGTON STATE DEPARTMENT OF
HEALTH FOR THE SHARING OF OPIOID OVERDOSE DATA

WHEREAS, the Snohomish County Health Department currently has a data sharing agreement with the Washington State Department of Health for opioid overdose data which will terminate on October 30, 2023; and

WHEREAS, the Washington State Department of Health and the Snohomish County Health Department wish to continue this partnership; and

WHEREAS, the Snohomish County Health Department needs access to the opioid overdose data for programmatic work; and

WHEREAS, drug overdose is a persistent public health problem for Washington State residents, and it is imperative for public health partners to know how this public health problem is impacting their communities; and

WHEREAS, the County Council held a public hearing on _____, 2023, to consider approving a data sharing agreement with the Washington State Department of Health for opioid overdose data and to authorize the Snohomish County Executive to enter into such agreement in substantially the form attached as Exhibit A.

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 between Snohomish County and the Washington State Department of Health for opioid overdose data in substantially the form attached hereto as Exhibit A.

PASSED this ___ day of _____, 2023.

SNOHOMISH COUNTY COUNCIL
Snohomish County, Washington

_____
Council Chair

1   ATTEST:
2
3   _____
4   Deputy Clerk of the Council
5
6   ( )   APPROVED
7   ( )   EMERGENCY
8   ( )   VETOED
9
10   DATE: _____
11
12
13   _____
14   County Executive
15   ATTEST:
16
17   _____
18
19   Approved as to form only:
20   _signature_   09-01-2023
21   _____
22   Deputy Prosecuting Attorney
23
24

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

Snohomish County ("Information Recipient")

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	Sarah de Jong	Cynthia Karlsson
Title	Executive Assistant	Rapid Health Information Network program manager
Address	3020 Rucker Ave Suite 306 Everett, WA 98201	1610 NE 150th St. MS: K17-9 Shoreline, WA 98155-9701
Telephone #	425-339-8652	(360) 995-3051
Email Address	SHD-Contracts@co.snohomish.wa.us	cynthia.karlsson@doh.wa.gov
IT Security Contact	Jim Kamp	John Weeks
Title	Business Management Analyst	Chief Information Security Officer
Address	3020 Rucker Ave Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8689	360-999-3454
Email Address	Jim.Kamp@co.snohomish.wa.us	Security@doh.wa.gov
Privacy Contact Name	Jannah Abdul-Qadir	Michael Paul
Title	Privacy and Public Records 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 provider means any individual or entity that provides data to the RHINO program. This includes all participating hospitals, clinics, and providers.

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.

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.

Health Information Exchange (HIE) means the statewide hub that provides technical services to support the secure exchange of health information between HIE participants.

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

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

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

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 with the identity of the person or persons to whom the data or records pertain. Research data or records with direct identifiers removed, but which retain indirect identifiers, are still considered identifiable.

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

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

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

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

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

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

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

GENERAL TERMS AND CONDITIONS

I. USE OF INFORMATION

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. SAFEGUARDING INFORMATION

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 OICIO 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. Once Data is accessed by the Receiving Party, this DSA is binding as to the confidentiality, use and disposition of all Data received as a result of access, unless otherwise agreed in writing.

DOH may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party, if DOH has a reasonable basis to believe that the Receiving Party has: (1)

failed to perform under any provision of this DSA; (2) violated any law, regulation, rule, or ordinance applicable to this DSA; and/or (3) otherwise breached any provision or condition of this DSA. If it is later determined that the Receiving Party was not in default, the termination shall be considered a termination for convenience.

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 date of execution through 10/31/2024.

SPECIAL TERMS AND CONDITIONS

XXI. The information recipient shall:

a. Not utilize the information obtained through this agreement for purposes of research activities as defined in RCW 42.48.010 unless reviewed by Washington State Institutional Review Board (WSIRB), execution of a Confidentiality Agreement for the research project, and approval from the data provider.

b. Not publish or otherwise disclose any data which may directly or indirectly identify an individual. Furthermore, the information recipient shall not publish the identity of a data provider (hospital, clinic, or provider) except with the consent of the data provider.

c. Not attempt to determine the identity of persons whose information is included in the data set or use the data in any manner that identifies individuals or their families.

d. Not attempt to obtain additional information about a patient or their visit from a patient's electronic medical record except for purposes agreed upon by the data provider (hospital, clinic, or provider) and the information recipient.

e. Except as required by state or federal law, not provide or otherwise utilize data obtained through this agreement for purposes of regulatory action or law enforcement against a data provider (hospital, clinic, or provider) or individual.

XXII.   The Information Recipient may:

a. Adhering to the DOH Small Numbers Publishing Guidelines (Appendix D) and RHINO Data Best Practices (Appendix E), and without including direct or indirect identifiers, publish, redisclose, or release aggregated data in order to protect public health.

b. Link data obtained through this Agreement with data from other sources, in order to identify, characterize, and/or solve a health problem, or evaluate the success of a health program. Any linked dataset containing data elements obtained through this agreement are subject to the terms of this Agreement, similar agreements governing linked datasets, and all state and federal laws that govern any included datasets.

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

Snohomish County

_____
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.

Washington Department of Health supports local health jurisdictions (LHJs) and tribes in their disease and injury surveillance and control activities by providing timely access to data. ESSENCE data is some of the most timely information available, with over 90% of emergency departments reporting visits within 24 hours. LHJs and tribes use this information to identify and respond quickly to public health threats such as novel pathogens, as well as track injury and health condition trends, evaluate interventions implemented, and use ESSENCE data within their statutory authority to provide quality public health services. Additionally, Washington Department of Health must provide local health jurisdictions and tribes access to the healthcare encounter data for their jurisdiction by statute (RCW 43.70.057).

Washington Department of Health will provide the requestor with ESSENCE access for identified users so that they may perform their duties of public health disease monitoring and control.

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 date of execution through 10/31/2024.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:

The Information Provider will provide access to the CDC National Syndromic Surveillance Program (NSSP) Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE) platform for a limited number of authorized users employed or contracted by the Information Recipient. User accounts will be established and managed by the Information Provider.

Authorized users will, upon execution of this Agreement and receipt of signed confidentiality agreements (Appendix A) from each authorized user, have access to the complete dataset contained within ESSENCE for the Information Recipient's jurisdiction. For example, an authorized user employed by a local health jurisdiction (LHJ) will have access to all ESSENCE data reported by facilities located in that jurisdiction, and all ESSENCE data for residents of that jurisdiction. An authorized user employed by a hospital will have access only to data from that hospital.

Authorized users have the ability to interact with and analyze the data within the ESSENCE platform. Additionally, authorized users have the ability download partial or complete datasets from the platform for additional analysis outside of the ESSENCE platform.

Data elements which may be found in ESSENCE for each record (visit) include:
- Facility name
- Facility type
- Admission reason code
- Patient's chief complaint(s) – original and processed entries
- Patients discharge diagnosis(es)
- Patient's Date of Birth
- Patient's age
- Visit/Admission date and time
- Discharge date and time
- Date and time of death (if applicable)
- Patient's medical record number
- Zip code city, county, and state of patient residence
- Discharge disposition
- Patient's sex
- Patient's race
- Patient's ethnicity
- Facility zip code
- Procedure code
- Initial Temperature
- Initial ED acuity assessment
- Onset date
- Clinical Impression

- Problem list
- Medication list
- Initial pulse oximetry
- Initial systolic and diastolic blood pressures
- Height
- Weight
- Body mass Index
- Pregnancy status
- Smoking status
- Travel history
- Visit type
- Mode of arrival
- Clinical Impression
- Triage notes
- Insurance coverage
- Insurance company ID
- Discharge instructions
- Various administrative and system data elements

It is important to note that, while the above listed data elements may exist in the ESSENCE platform, the elements included for each individual record may vary. This is a result of variances in data submission among facilities.

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:

    RCW 43.20.050 – Powers and duties of state board of health
    RCW 43.70.050 – Collection, use, and accessibility of health-related data

RCW 70.02.050 – Disclosure without patient's authorization
RCW 43.70.057 - Hospital emergency room patient care information—Data collection,
maintenance, analysis, and dissemination—Rules
RCW 43.70.130 – Powers and duties of secretary—General.
45 CFR Part 160 – General Administrative Requirements
45 CFR Part 162 – Administrative Requirements
Patient Protection and Affordable Care Act of 2010

Information Recipient's statutory authority to receive the confidential information or limited
Dataset(s) identified in this Exhibit

WAC 246-101-505 - Duties of the local health officer or the local health department
WAC 246-101-610 - Handling of case reports and medical information
United States Federal Indian Law
Indian Self Determination Act 1975

5. **ACCESS TO INFORMATION**

   METHOD OF ACCESS/TRANSFER

   ☐ DOH Web Application (indicate application name):
   ☐ Washington State Secure File Transfer Service (sft.wa.gov)
   ☐ Encrypted CD/DVD or other storage device
   ☐ Health Information Exchange (HIE)**
   ☒ Other: Authorized users will access the data through the CDC NSSP ESSENCE platform

   **<u>NOTE</u>: 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): Authorized users have the ability to download (copy) partial or complete datasets from the platform. Upon request by DOH program staff, at the end of the Agreement term, or when no longer needed, the Information Recipient shall destroy all copies of any data provided under this Agreement. Acceptable methods of destruction are described in Appendix B.

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 all papers, presentations, reports, or publications developed using data obtained under this agreement to the attention of: the RHINO program at RHINO@doh.wa.gov.

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

State of Washington Department of Health

_____
Signature

_____
Print Name

_____
Date

INFORMATION RECIPIENT

Snohomish County

_____
Signature

_____
Print Name

_____
Date

<u>EXHIBIT II</u>

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.

    Drug overdose is a persistent public health problem for Washingtonians. It is imperative for public health partners to know how this public health problem is impacting their communities. To maintain visibility on the drug overdose concern, the Information Provider has created a dashboard displaying a synopsis of the data for drug overdose. The Information Provider will give the Information Recipient access to this dashboard once this DSA is signed.

    The Information Recipient agrees not to remove data from the dashboard to use in a public facing product. The dashboard provided by the Information Provider is strictly for keeping the Information Recipient abreast of what is happening in the community to facilitate proper community guidance and public health work. The Information Recipient agrees to reach out to the Information Provider if raw data is needed for another purpose. The Information Provider acknowledges that the dashboard contains small numbers but expects the Information Recipient to adhere to the small number policy attached to this DSA and to only use the dashboard data in ways consistent with this DSA.

    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 date of execution through 10/31/2024.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:
Database Name(s): *RHINO ESSENCE*
Data Elements being provided:
Access to the opioid dashboard. The following variables are part of the dashboard:

   Age, residential county, visit date, race, ethnicity, sex, drug category.
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:

RCW 43.20.050 – Powers and duties of state board of health
RCW 43.70.050 – Collection, use, and accessibility of health-related data
RCW 70.02.050 – Disclosure without patient's authorization
RCW 43.70.057 - Hospital emergency room patient care information—Data collection, maintenance, analysis, and dissemination—Rules

Information Recipient's statutory authority to receive the confidential information or limited Dataset(s) identified in this Exhibit:
RCW 43.70.057 - Hospital emergency room patient care information—Data collection, maintenance, analysis, and dissemination—Rules

5. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

- ☒ DOH Web Application (indicate application name): DOH Opioid Dashboard
- ☐ Washington State Secure File Transfer Service (sft.wa.gov)
- ☐ 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

☐   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): Authorized users have the ability to download (copy) partial or complete datasets from the platform. Upon request by DOH program staff, at the end of the Agreement term, or when no longer needed, the Information Recipient shall destroy all copies of any data provided under this Agreement. Acceptable methods of destruction are described in Appendix B.

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 all papers, presentations, reports, or publications developed using data obtained under this agreement to the attention of: the RHINO program at rhino@doh.wa.gov.

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

State of Washington Department of Health

_____
Signature

_____
Print Name

_____
Date

INFORMATION RECIPIENT
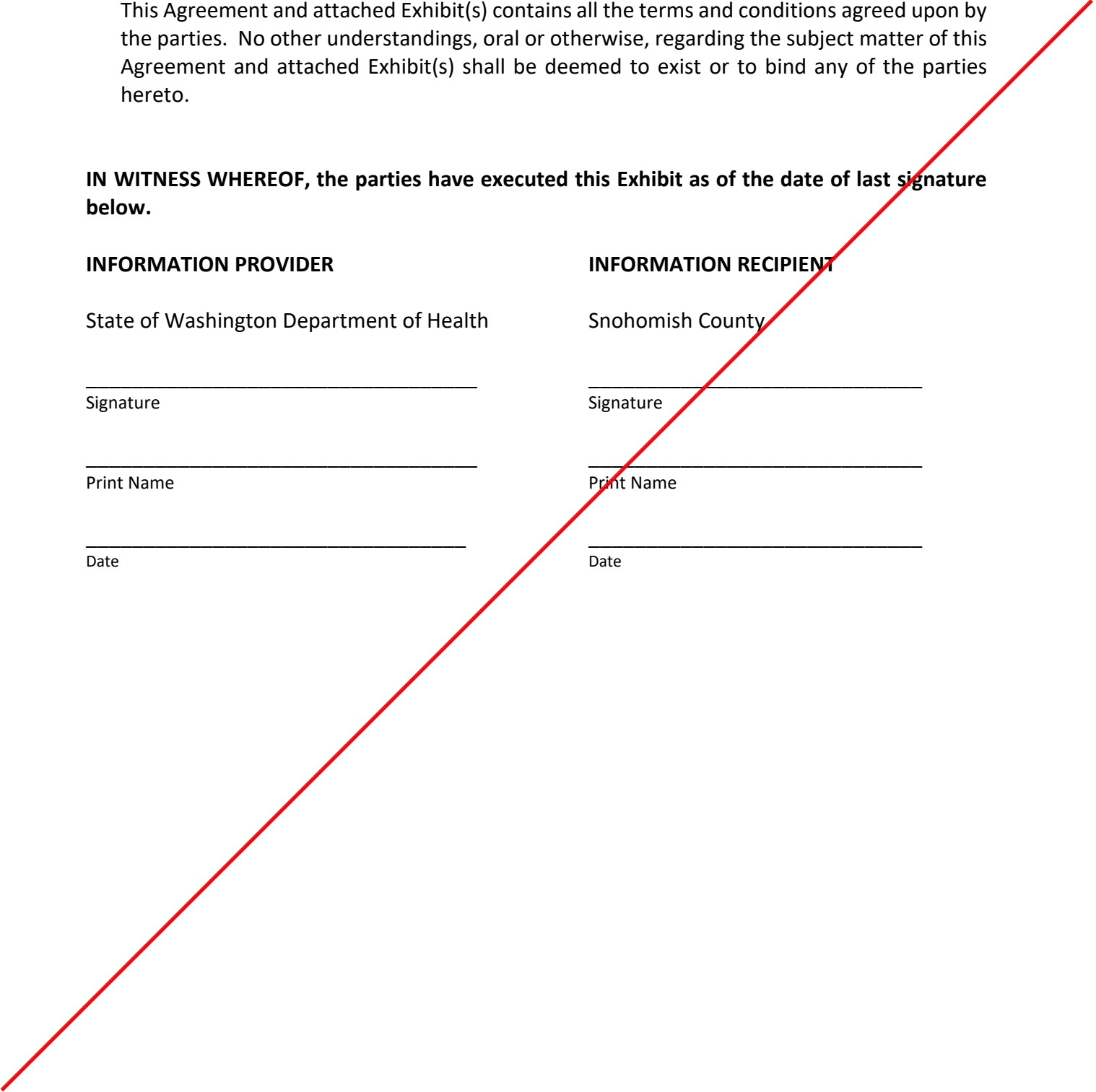
Snohomish County

_____
Signature

_____
Print Name

_____
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:_____

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

Every person (e.g., employee or agent) with access to the information must sign and date the "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.

The Information Recipient must retain a copy of the signed and dated form for each user as long as required in Data Disposition Section.

The Information Recipient must forward a copy of the signed and dated form for each user to the RHINO program at RHINO@doh.wa.gov to obtain access credentials for new users.

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
      2.   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: ESSENCE User Code of Conduct

System Monitoring —As an authorized user, you understand and acknowledge that your use of this system will be monitored for system management and to ensure protection against unauthorized access or use. Unauthorized access or use may subject a user to administrative, civil, criminal, or other adverse action to the extent allowed by law.

Warnings, Alerts, and Anomalies —Syndromic surveillance systems emphasize the use of statistical alerting algorithms to help users determine where to focus additional attention. Time series visualization and statistical alerts alone are generally insufficient for issuing public alerts or warnings. Users typically "drill down" to these data to assess the distribution of affected emergency department (ED) visits (or other events captured by the syndromic surveillance system) and may use additional variables such as person, place, or time and other clinical assessments. Analyses may include quality checks to confirm data are complete and accurate.

To that end, users are expected to respect the role of state and local jurisdictions and their respective authority related to public health matters within their jurisdiction by

- Consulting a jurisdiction whose data you intend to access and use (including jurisdictions within your own) to discuss a finding or interpretation of these data before issuing a public statement or warning, taking public health action, or seeking further information from data providers within the other jurisdiction when that action includes disclosure of information derived in part or in whole from the other jurisdiction's data[1].

- Informing those who use your data about significant anomalies already understood or under investigation to prevent duplication of effort and unnecessary queries. This includes anomalies due to artifacts (like exercises or batched data) and those due to real local events.

Data Sharing —the design of the BioSense[2] Platform ensures that all sites contribute data toward national syndromic surveillance (with limited details at aggregate levels) while also allowing jurisdictions to control whether and how much data are shared at local and state levels. Users are expected to act responsibly by

- Assuming the risk and liability of any of their use or misuse of the BioSense Platform or data produced, including use that complies with third-party rights (i.e., downstream Data Use Agreements).

- Sharing data with other authorized users in accord with applicable agreements and laws.

- Ensuring that the use of these data is in accord with acceptable practices for ensuring the protection, confidentiality, and integrity of contents.
   DOH has established standards for the presentation of data to the public, designed to protect the confidentiality of personal data and the priavary of Washington residents. These standards require DOH staff who are preparing data for public presentation to:
   1. When possible, aggregate data so that the need for suppression is minimal.

2. Suppress all non-zero counts which are less than ten, unless they are in a category labeled "unknown."
3. Suppress rates or proportions derived from those suppressed counts.
4. Assure that suppressed cells cannot be recalculated through subtraction, by using secondary suppression as necessary.

Department of Health Agency Standards for Reporting Data with Small Numbers
- Making NO attempt to identify individuals represented in these data or data sources except as part of an authorized public health investigation follow-up and to the extent allowed by applicable law.
- Making NO attempt to use these data where prohibited by local, state, or federal law or regulation.
- Keeping usernames and passwords confidential; this system is intended for authorized users only.

Violation of Code of Conduct may result in CDC disallowing access to the BioSense Platform and associated data and tools within. By accepting this code of conduct, you acknowledge that you are an authorized user of the BioSense Platform and have read and understand the BioSense Platform Code of Conduct.

[1]Cross-jurisdictional consultation and coordination are strongly encouraged to assist in the interpretation of data and gain further information to inform effective public health action. While beneficial, this should not prevent a jurisdiction from exercising their authority to protect public health.

[2]BioSense and ESSENCE are used interchangeably.

Print Name: _____

Signature: _____

Date:_____

Email Address:_____

Phone Number:_____

Agency: _____

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

_____   _____

Signature of data recipient   Date

APPENDIX D

DOH SMALL NUMBERS GUIDELINES

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

- Suppress rates or proportions derived from those suppressed counts.

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

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

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

ADDITIONAL DATASET SPECIFIC SMALL NUMBERS REQUIREMENTS

Exceptions to the Suppression Rules:

DOH Small Numbers Publishing Guidelines allow for case-by-case exceptions in certain circumstances, so that the public may receive information when public concern is elevated and/or protective actions are warranted. Two examples of such situations are:

- In a cluster investigation, intense public interest often combines with very small numbers of cases. In order to be responsive to the community and allay fear, the Data Recipient may decide it is important to make an exception to the small numbers publishing standard while still protecting privacy.

- Similarly, in a public health emergency such as a communicable disease outbreak or other all-hazards incident, case counts may be released when the numbers are very small. This should be done in the context of an imminent public health threat, such as person to person spread of disease, where immediate action is indicated to protect public health.

When releasing small numbers to the public in the context of the above exceptions, DOH recommends limiting the amount of information shared in order to protect the identity of the person(s) involved. In these cases, DOH recommends reporting only the person's gender, decade of age, and county of residence. For minors, ages should be reported as <18.

For further guidance, please refer to Appendix F for DOH Agency Standards and Guidelines for Working with Small Numbers. This document contains recommendations and best practices for protecting the privacy of Washington residents when presenting data to the public.