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

This Agreement documents the conditions under which the Washington State Department of Health 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, through its Health Department	Washington State Department of Health (DOH)
Business Contact Name	Pamela Aguilar	Michelle Campbell
Title	Interim Department Director/ Department Deputy Director	Chief Data Officer
Address	3020 Rucker Ave, Suite 306, Everett, WA 98201	P.O. Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-5200	360-236-4241
Email Address	SHD-Contracts@co.snohomish.wa.us	michelle.campbell@doh.wa.gov
IT Security Contact	Doug Cavit	John Weeks
Title	County Information Security Officer	Chief Information Security Officer
Address	3000 Rockefeller Ave, Everett, WA 98201	P.O. 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	Mike Paul
Title	Public & Privacy Records Officer	DOH Chief Privacy Officer
Address	3020 Rucker Ave, Suite 306, Everett, WA 98201	P.O. Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8641	564-669-9692
Email Address	jannah.abdulqadir@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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GENERAL TERMS AND CONDITIONS

I. **USE OF INFORMATION**

The Information Recipient 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 Washington Technology Solutions (WaTech) security standard's: Asset Management Policy | WaTech; Physical and Environmental Protection Policy | WaTech; Network Security Standard | WaTech; Mobile Device Security Standard | WaTech; Remote Access Standard | WaTech.

For the purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates meets WaTech security standards in SEC-08 "Data Sharing Policy" and SEC-01 through SEC-13 "WaTech Policies".

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 the paragraph 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 date of execution through 12/31/2029.

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

INFORMATION PROVIDER		**INFORMATION RECIPIENT**
State of Washington Department of Health		Snohomish County
Signature		Signature
Print Name		Print Name
Date		Date

EXHIBIT I

1. PURPOSE AND JUSTIFICATION FOR SHARING THE DATA

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

The Child Wellness Survey is funded by Foundational Public Health Services to collect information on the health, development, and wellbeing of young children and their families.

Under RCW 43.70.130 the department is tasked with investigating and studying factors related to the preservation, promotion, and improvement of the health of the people. Under RCW 43.70.040 the department may undertake studies, research, and analysis necessary to carry out the department's responsibilities. The Child Wellness Survey (CWS) is a special study done to study and investigate factors related to the preservation, promotion, and improvement of the health of children.

The purpose of the Child Wellness Survey (CWS) is to collect Washington-based population survey data on indicators of wellbeing among infants, children, and families that can inform programs and policies. Per RCW 43.70.050, these data will be shared for appropriate use in alignment with all relevant protections as outlined in Appendix A. RCW 43.70.515(3)(iv) also permits DOH to provide critical data to public health programs statewide to support their foundational work.

CWS data will be used to support ongoing surveillance and policy and program evaluation efforts related to infant, child, and family wellbeing. Policy development may also be informed using these data.

The CWS was determined by the Washington State Institutional Review Board (WSIRB) to be exempt from full WSIRB review. The sharing of a full dataset with state, Tribal, and local public health partners does not require further WSIRB review.

The Snohomish County Health Department will use the CWS data for general exploratory analysis of Snohomish County's sample and all variables to understand the baseline data. The Health Department anticipates creating a small summary report to give to our child and family health team to inform their programming work. The data will be used to supplement and continue epidemiology programmatic work on child and family health topics.

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

Exhibit I shall be effective from DOE through 12/31/2029.

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.

Child Wellness Survey and all data elements as described in Appendix A.

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

Data elements and details are listed in Appendix A

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 43.70.050 (2) and (5) – Collection, use, and accessibility of health-related data
RCW 43.70.512 Public health system-Foundational public health service Intent
RCW 43.70.515(3)(iv) Foundational Public Health Services-Funding
RCW 43.70.040(3) Secretary's powers-Rule-making authority-Report to the legislature
RCW 43.70.130(2) Powers and duties of Secretary-General

5. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

☐ DOH Web Application (indicate application name):
☒ Washington State Secure File Transfer Service (mft.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 __1/31/2026__
☐ Repetitive: frequency or dates _____
☐ 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 All reports using CWS data to the attention of: Population Survey Team cepea@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		**INFORMATION RECIPIENT**
State of Washington Department of Health		Snohomish County
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:

1. "Identifiable information" means any data element, or combinations of such data elements, that could be used to identify an individual child or respondent who participated in the Survey (such as age, race, sex);or presentations of data that could identify individual either of them.
   Families participating in the survey were assured privacy of their responses. It is the intention of this agreement to permit sharing of individual-level Survey data while ensuring anonymity of families.

2. "Survey" and "Survey data" refer to the Child Wellness Survey data [0-5 years old] and [2024]. For the 2024 survey, only data for 0-5-year-olds are available.

3. "Dataset" refers to the data file that will be provided to the recipient.

a. "Limited" dataset refers to the dataset that include the individual-level data from the statistical sample (state sample) and the non-probability sample WITHOUT any other geographic identifiers.
b. "Full" dataset refers to the dataset that include individual-level data from the statistical sample (state sample) and the non-probability sample WITH regions' identified. County identifiers and zipcode will not be shared.

NOW THEREFORE, IT IS AGREED AS FOLLOWS:

1. DOH will disclose to **Snohomish County** a **full analytic dataset with identifiers for geographic region** for the 2024 CWS data for 0-5 years old. Data Provider shall transfer Survey data using a secure file transfer method.

2. Each CWS data recipient from the **Snohomish County** shall follow all DOH- and CWS-specific small numbers requirements and suppressions listed in Appendix D to maintain confidentiality.

Signed by all data users:

Signature _____ Date _____

Print Name Suzy An

Signature _____ Date _____

Print Name Ashley Thapa

Signature _____ Date _____

Print Name Peter Maier

Signature _____ Date _____

Print Name Miyuki Blatt

Signature _____ Date _____

Print Name Hollianne Bruce

Signature _____ Date _____

Print Name Tyler Bonnell

Signature		Date	
Print Name	Cassidy, Brewin,		
Signature		Date	
Print Name	Kali Turner		
Signature		Date	
Print Name	Elizabeth Noonan		

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 hard disks:

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). When the data is classified as Confidential or Restricted, authentication requires secure encryption protocols and multi-factor authentication mechanisms, such as hardware or software tokens, smart cards, digital certificates or biometrics.

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

F. Data storage on mobile devices or portable storage media

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

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

3. The data must not be stored by 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 wipe or be rendered unusable after no more than 10 failed access attempts.
    d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactivity activity period of 3 minutes or less.
    e) The data must not be stored in the Cloud. This includes backups.

    f) The devices/ media must be physically protected by:
        - Storing them in a secured and locked environment when not in use;
        - Using check-in/check-out procedures when they are shared; and
        - Taking frequent inventories.

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

G. Backup Media

The data may be backed up as part of 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

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

K. Notification of Compromise or Potential Compromise

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

APPENDIX C

CERTIFICATION OF DATA DISPOSITION

Date of Disposition _____

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

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

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

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

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

☐ Other

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in agreement DOH # _____, Section C, item B 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 CWS-SPECIFIC SMALL NUMBERS REQUIREMENTS

To maintain confidentiality, CWS data recipients shall:

1. Use CWS data for statistical analyses only.
2. Follow the DOH Small Numbers standards (Guidelines for Working With Small Numbers) and additional CWS data reporting restrictions **(see #3)**
3. Report or publish findings in a manner that does not permit identification of survey participants and adheres to the CWS suppression rules. These include:
    a. Do not publish results if the number of respondents is less than 40
    b. Flag all results where the Relative Standard Error (RSE) is between 25% and 30%
    c. Do not publish results if RSE is greater than 30%
    d. Do not publish findings if cell size is less than 10 in your crosstab analysis
    e. Only use weighted data for analysis and reporting
4. Report data use (presentations, reports, manuscripts, etc.) by December 30th annually (you will be notified when it is time to report).

CWS data recipient <u>will not</u>:

1. Redistribute or share dataset with anyone else.
2. Attempt to link CWS data to other data sources with the purpose of identifying individuals or creating individual-level linked records.

APPENDIX E

Tribal Data Sovereignty Principles

These Tribal Data Sovereignty Principles were drafted in partnership with WA Tribes based on the Governor's Indian Health Advisory Council's Principles. These principles are included in our data sharing agreements at DOH as a reflection of our commitment to uphold these principles and our government-to-government relations with Tribes.

Tribal data sovereignty asserts the rights of Tribal Nations to govern the collection, ownership, and application of their own data, this derives from Tribes' inherent right to govern their peoples, lands, and resources. To uphold Tribal Data Sovereignty principles, DOH may sign Tribe-specific Data Sharing Agreements, which include provisions for data sharing and consent for data use via a Tribal Nation Data Use Form.

By signing this agreement, the Information Recipient acknowledges the sovereignty of the Tribal Nations outlined in these principles.

1. **Inherent Authority to Manage Data.** Tribes hold the sovereign authority to manage the collection, ownership, application and interpretation of their own data even when it is collected by federal, state, or local governments and/or other third parties.

2. **Ownership of and Authority Over Tribal Data.** Tribes retain an ownership interest in data and authority even when the Tribe's data are located in a state, federal or other datasets. This interest remains when the Tribe's data are aggregated with other data.

3. **Informed Consent.** Tribes have the right to informed consent on how their data, including protected health information about Tribal members, are used or shared with third parties.

4. **Equitable Access to Data.** Tribes have the right to exercise their Tribal data sovereignty and must have the same or enhanced access to state data as other public health jurisdictions to effectively carry out their governmental duties.

5. **Partnership.** The agency will make reasonable efforts to collaborate with Tribes, as equal partners, as outlined in the RCW 43.376.020 (Government-to-government relationships—State agency duties) and DOH Collaboration & Consultation guidance, and other Tribal data initiatives.

6. **Privacy and Security Protections.** DOH will work collaboratively with Tribes and use required administrative, technical and physical security practices to protect Tribal data and the confidentiality of Tribal data.

7. **Tribal Sovereignty and Third-Party Relationships.** DOH respects the sovereign rights of Tribes to enter into other agreements or collaborate with third parties as they deem appropriate.

8. **Tribal Data Sovereignty and Third-Party Accountability.** DOH will ensure third-party accountability for adherence to these principles, any applicable privacy laws, and Tribal expectations for the appropriate use of Tribal data.

APPENDIX F
PHSKC – DOH Data User Agreement (verbatim)

DUA purpose:

This DUA permits DOH to:

a. use King County's 2023 Best Start for Kids Health survey (BSFKHS) data to generate CWS state estimates, and
b. re-share BSFKHS data with CWS data users who sign this Data Sharing Agreement with DOH.

******Please DO NOT sign the signature block below. The below section is for reference ONLY.******

Data Use Agreement
between
Public Health – Seattle & King County ("Covered Entity")
And
Washington State Department of Health **("Data User")**

The effective date of this agreement is: NA

A. Public Health agrees to provide Data User with a Limited Data Set, which means that all direct patient identifiers have been removed, except those indirect identifiers which are allowed in a limited data set.

This information is provided to the Data User in order to:

Combine King County results from the Best Starts for Kids Health Survey (BSKHS) with results for The Child Wellness Survey (CWS) to produce state-wide estimates. The CWS is a new statewide population-based survey that will focus on collecting information on child development and early experiences, parent-child interactions, basic needs, parent support, community support and family strength.

The survey closely mirrors King County's BSKHS with minor modifications for a few questions and/or responses to meet statewide needs. WSIRB determined that CWS is classified as a project to support surveillance and evaluation and hence does not require further reviewed by WSIRB.

The CWS does not include King County residents as PHSKC administers BSKHS for King County residents. Therefore, the 2023 Best Starts for Kids Survey data will be appended to the 2024 Child Wellness Survey data to be able to generate state and regional -level estimates of key indicators that will help inform policy and public health decision-making. Future BSKHS survey data may also be combined with CWS data.

Approved, indirect identifiers from this appended dataset will be disseminated to LHJs, Tribal-, and other approved partners by DOH in accordance with a data sharing agreement process and appropriate internal review. Each entity will sign a data sharing agreement with DOH that will outline which, if any, indirect identifiers they receive. DOH will provide either a limited CWS dataset with no geographic identifiers or a dataset with geographic identifiers (region names) included

either for all geographies or a subset of geographies. The school district variable from BSFKS dataset will not be shared and is only intended for DOH internal use to support future collaboration between the surveys.

Under RCW 43.70.050 the Data User is tasked with collecting and evaluating population based health related data for identify high priority health issues that require study or evaluation. One of these is evaluation of specific population groups to identify needed changes in health practices and services. The Child Wellness and BSKHS survey will provide the Data User with data to understand the needs of families in Washington including access to childcare, healthcare services, basic needs and other similar topics. Under RCW 43.70.040, the Data User is granted authority to undertake studies, research, and analysis necessary to carry out the duties of the Data User. This project would be considered a study and analysis of a population group.

B. The Limited Data Set may only be used for the purposes of research, public health authority activities, or healthcare operations.

If this information is provided for the Data User to conduct research, please list the study title:

N/A

C. The identifiable elements that are allowed in a Limited Data Set and that will be included in data set are as follows:

Individually Identifiable Data Elements allowed in a limited data set	**Element included in this set**
State, county, city, precinct and five digit zip code	County, Region, School District
Admission, discharge & service dates Birth date Date of death Age (including age 90 or over)	Age

All other direct identifiers will be removed.

D. The Data User agrees to the following with respect to the Limited Data Set(s) provided by the Best Starts for Kids Health Survey Program of Public Health.

The Data User:

1. Will not use or disclose any of the data received except to fulfill the purpose of the above referenced request. A plan for the review of applications for use of this data by local health jurisdictions, tribal, and academic partners will be discussed and pre-approved by the Data User and Assessment Public Development and Evaluation (APDE) Unit in Public Health-

Seattle & King County. The Data User will require DSAs from each data recipient to ensure that the data recipient understands DOH's criteria for data use and storage as well as PHSKC's criteria. The Data User will make a determination about:

A. Risk of disclosure of confidential and/or sensitive information: Can the analysis be conducted without compromising the confidentiality promised to BSKHS respondents?
B. Compatibility with the purpose of the survey: Is the proposed project consistent with the purposes for which the information was collected?

2. Will share a detailed plan of the different dataset versions that will be made available, and who/how/when the data recipient may be able to access the different versions that range from the limited dataset with no geographic identifiers to generate state-level estimates, to a dataset with county names identified which maybe shared after WSIRB exempt determination.

3. Will include all relevant terms, conditions and requirements set forth in this DUA in any sharing agreement with local health jurisdictions, tribal, and academic partners that includes BSKHS data.

4. Understands that it, those under its direct supervision, and those who complete an appropriate data sharing agreement with the Data User are the only parties authorized to use this information.

5. 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.

    i. Retain a copy of the signed and dated form according to organizational retention standards.

6. Will not further use or disclose the information other than as permitted by this Data Use Agreement or as otherwise required by law.

7. Will not attempt to link or permit others to attempt to link the information of persons in the data set with personally identifiable records from any other source, to learn the identity of any person represented in the data set, or to contact any individual represented in the data set.

8. Will safeguard shared data in accordance with privacy and security standards that meet or exceed those outlined in HIPAA to the extent possible as a Public Health Agency, even when the Data User (The Washington State Department of Health) is not a HIPAA-covered entity. While not bound by HIPAA regulations, DOH affirms its commitment to protecting the confidentiality, integrity, and security of the data in a manner consistent with HIPAA or stricter applicable standards.

9. Notify Covered Entity via e-mail to bsk.data@kingcounty.gov any use or disclosure of the data not provided for in this Agreement within two (2) business days of the discovery of such use or disclosure. The notification shall include the identification of the data which has

been, or is reasonably believed by the Data User to have been, accessed, acquired, or disclosed; a brief description of what happened, including the date of the use or disclosure and the date of the discovery, a brief description of what the Data User is doing to investigate the unauthorized use or disclosure, and, to protect against any further unauthorized uses or disclosures. The information shall be updated promptly and provided to the Covered Entity as requested by the Covered Entity.

10. Will ensure that any agents, including any subcontractors, to whom it provides this information, agree to the same restrictions and conditions by including this section verbatim in their Data Sharing Agreement. The Data User will keep those signed agreements in its files and make them available to Public Health upon request.

11. Will protect, defend, indemnify and hold harmless Public Health, its officers, employees, and agents, from any and all costs, claims, judgments, and/or awards of damages arising out of, or in any way resulting from, the negligent acts of the Data User in its performance and/or non-performance of its obligations under this Agreement.

12. Will comply with the Health Insurance Portability and Accountability Act of 1996 to the extent possible as a Public Health Agency, as amended, and Washington State laws regarding this information.

E. Term: This agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

F. Upon Public Health's knowledge of a material breach by Data User, Public Health shall provide an opportunity for the Data User to cure the breach or end the violation. If the Data User does not cure the breach or end the violation within ten (10) business days of receipt of written notice by Public Health, Public Health shall immediately terminate this Agreement.

G. Recipient Statutory Authority

H. RCW 43.70.050(2) Collection, use, and accessibility of health-related data
RCW 43.70.050(4)(a)(iii) Collection, use, and accessibility of health-related data
RCW 43.70.040(3) Secretary's powers-Rule-making authority-Report to the legislature
RCW 43.70.130(2) Powers and duties of secretary-General
WAC 246-101-605(2)(c) Duties-Department

I. Effect of Termination: Except as specifically provided in paragraph D, upon termination of this Agreement for any reason, the Data User shall return or destroy the Limited Data Set received from Public Health or created or received by the Data User on behalf of Public Health. This provision shall also apply to this information that is in the possession of subcontractors or agents of the Data User. The Data User shall retain no copies of the Limited Data Set.

In the event that the Data User determines that returning or destroying the Limited Data Set is not feasible, the Data User shall extend the protections of this Agreement to such information and limit further disclosures of such information to those purposes that make return or destruction infeasible, for so long as the Data User maintains such information.

FOR: Data User

Signature

Name & Title

Organization (if applicable)

Date

FOR: Public Health

Signature

Name & Title

Organization

Date

FOR: Public Health Program Overseeing DUA

Signature

Name & Title

Public Health Program Name

Date