

**IT 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**

	<b>INFORMATION RECIPIENT</b>	<b>INFORMATION PROVIDER</b>
Organization Name	Snohomish County, through its Health Department	Washington State Department of Health (DOH)
<b>Business Contact Name</b>	Hollianne Bruce	Jessica Marcinkevage
Title	Lead Epidemiologist	Interim State Epidemiologist for Policy and Practice
Address	3020 Rucker Ave, Ste 208, Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-5213	
Email Address	<a href="mailto:hollianne.bruce@co.snohomish.wa.us">hollianne.bruce@co.snohomish.wa.us</a>	<a href="mailto:CEPEA@doh.wa.gov">CEPEA@doh.wa.gov</a>
<b>IT Security Contact</b>	Doug Cavit	John Weeks
Title	County Information Security Officer	Chief Information Security Officer
Address	3000 Rockefeller Ave, Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-312-0660	360-999-3454
Email Address	<a href="mailto:doug.cavit@co.snohomish.wa.us">doug.cavit@co.snohomish.wa.us</a>	<a href="mailto:Security@doh.wa.gov">Security@doh.wa.gov</a>
<b>Privacy Contact Name</b>	Jannah Abdul-Qadir	Mike Paul
Title	Public & Privacy Records Officer	DOH Chief Privacy Officer
Address	3020 Rucker Ave, Ste 308, Everett, WA 98201	P. O. Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8641	564-669-9692
Email Address	<a href="mailto:jannah.abdul-qadir@co.snohomish.wa.us">jannah.abdul-qadir@co.snohomish.wa.us</a>	<a href="mailto:Privacy.officer@doh.wa.gov">Privacy.officer@doh.wa.gov</a>

## **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.

**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** Days of the week excluding weekends and state holidays; namely, New Year's Day, Martin Luther King Jr. Day, President's Day, Memorial Day, Juneteenth, Labor Day, Independence Day, Veterans' Day, Thanksgiving day, the day after Thanksgiving day, and Christmas. Note: When January 1, June 19, July 4, November 11, or December 25 falls on Saturday, the preceding Friday is observed as the legal holiday. If these days fall on Sunday, the following Monday is the observed holiday.

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

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

### B. SECURITY

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

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

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

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

#### C. BREACH NOTIFICATION

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

### III. **RE-DISCLOSURE OF INFORMATION**

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

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

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

### IV. **ATTRIBUTION REGARDING INFORMATION**

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

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

### V. **OTHER PROVISIONS**

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

**VI. AGREEMENT ALTERATIONS AND AMENDMENTS**

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

**VII. CAUSE FOR IMMEDIATE TERMINATION**

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

**VIII. CONFLICT OF INTEREST**

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

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

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

**IX. DISPUTES**

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

- Be in writing and state the disputed issues, and
- State the relative positions of the parties, and
- State the information recipient's name, address, and his/her department agreement number, and

- Be mailed to the DOH contracts and procurement unit, P. O. Box 47905, Olympia, WA 98504-7905 within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue which he/she now disputes.

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

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

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

**XI. GOVERNANCE**

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

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

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

**XII. HOLD HARMLESS**

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

**XIII. LIMITATION OF AUTHORITY**

Only the Authorized Signatory for DOH shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of the DOH. No alteration, modification, or waiver of any clause or condition of

this Agreement is effective or binding unless made in writing and signed by the Authorized Signatory for DOH.

**XIV. RIGHT OF INSPECTION**

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

**XV. SEVERABILITY**

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

**XVI. SURVIVORSHIP**

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

**XVII. TERMINATION**

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

**XVIII. WAIVER OF DEFAULT**

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

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

**XIX. ALL WRITINGS CONTAINED HEREIN**

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



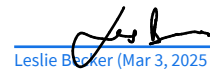
**XX. PERIOD OF PERFORMANCE**

This **Agreement** shall be effective from March 16, 2025 through March 15, 2029.

**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

  
Leslie Becker (Mar 3, 2025 08:17 PST)

Signature

**Leslie Becker**

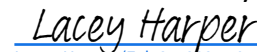
Print Name

**03/03/2025**

Date

**INFORMATION RECIPIENT**

Snohomish County

  
Lacey Harper (Feb 25, 2025 10:13 PST)

Signature

**Lacey Harper**

Print Name

**02/25/2025**

Date

## **EXHIBIT I**

### **1. PURPOSE AND JUSTIFICATION FOR SHARING THE DATA**

The Healthy Youth Survey (HYS) is a multi-agency collaborative research study conducted under the authority of RCW 69.50.540 (1)(b)(i)(B). DOH and partner agencies are obligated to collect, analyze, and report on survey results at least every two years. The HYS collects information from 6th-12th graders in Washington on a range of health indicators that can inform programs and policies related to adolescent health. Per RCW 43.70.050, these data will be shared for appropriate use in alignment with all relevant protections as outlined in Appendix A.

HYS data will be used to support ongoing surveillance and policy and program evaluation efforts related to adolescent wellbeing. Policy development may also be informed using these data.

The HYS has been approved by the Washington State Institutional Review Board (WSIRB). The WSIRB authorizes DOH to release a full dataset to state, Tribal, and local public health partners using the data to support surveillance and evaluation without further WSIRB review.

Data will be used for on-going assessment activities, including tracking trends for public health indicators, preparing reports on specific public health issues, and responding to requests for data from the public and other public agencies. Data are analysed and the findings reported to Snohomish County leaderships, policy-makers, and other community partners to keep them informed about emerging public health issues and to track the progress of various public health programs.

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 \_\_\_\_\_ through \_\_\_\_\_.

### 3. DESCRIPTION OF DATA

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

Healthy Youth Survey and all data elements as described 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 – Collection, use, and accessibility of health-related data**  
**RCW 69.50.540 (1)(b)(i)(B) – Authority for conducting the Healthy Youth Survey**

### 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 \_\_\_\_\_ (insert date)
- ☒ Repetitive: Between March 1, 2026 and March 15, 2029\_\_\_\_
- ☐ 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 HYS data       to the attention of: Healthy Youth Survey Principal Investigator at [Healthy.Youth@doh.wa.gov](mailto:Healthy.Youth@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

  
Leslie Becker (Mar 3, 2025 08:17 PST)  
 Signature

Leslie Becker


Print Name

03/03/2025

Date

**INFORMATION RECIPIENT**

Snohomish County

  
Lacey Harper (Feb 25, 2025 10:13 PST)  
 Signature

Lacey Harper

Print Name

02/25/2025

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 student who participated in the Survey (such as grade, age, race, sex); presentations of data that could identify individual students; and, in cases in which a school principal has not given permission for school-identified presentations, individual schools or grade levels within a school.

Students participating in the survey and their parents were promised complete anonymity of student survey responses. It is the intention of this agreement to permit disclosure of individual-level Survey data while ensuring anonymity of students.

2. "Survey" and "Survey" data refer to the Washington State Healthy Youth Survey 2002-2027.

The Healthy Youth Survey Planning Committee has requested that the Department of Health (DOH, Data Provider) handle disclosure of individual-level data containing only indirect identifiers from the Healthy Youth Survey 2002-2027 (hereinafter referred to as "Survey") to local health departments and universities. WSIRB approval or exempt determination are not needed for this data sharing agreement.

NOW THEREFORE, IT IS AGREED AS FOLLOWS:

1. For access to school identifiers, Snohomish County Health Department shall obtain written permission from the principals of *each* school for which Snohomish County Health Department will report data in such a way that the school can be identified and written permission from the superintendent of each school district for which Snohomish County Health Department will report data in such a way that the school district can be identified. School principal/superintendent permission will not be necessary to use the data to compose groups of schools (e.g., north and south areas of the county) as long as data are not reported in such a way that schools or school districts can be identified. Generally, if there are at least 3 schools and 3 school districts at a geographical level for which data are being reported, the schools and school districts are not identifiable. However, there may be exceptions in which they would be identifiable. For example, if the report includes thresholds that all of the schools in a grouping meet (for example, if all schools or school districts in a grouping have especially high or low levels of risk on a particular measure) then the information for those schools or school districts is identifiable, and school principal or superintendent permissions will be obtained.
2. DOH will disclose to Snohomish County Health Department individual-level Healthy Youth Survey data for 2002-2027 survey cycles for the following geographic area(s): All of Washington State. DOH will disclose all data elements including any geographic identifiers such as the identifiers of the schools participating in the Survey in Snohomish County. Geographic identifiers will not be provided for schools outside of Snohomish County. Snohomish County Department of Health will also maintain access to prior years' data in accordance with their prior DSAs. The Data Provider shall transfer Survey data using a secure file transfer method.
3. Snohomish County Department of Health (Data Recipient) will:
  - a) use Survey data only to examine the use of alcohol, tobacco and other drugs, and risk and protective factors, and other variables measured by the survey, among public

school students. These analyses will be used to inform policy and program development at the local level;

- b) maintain all Survey data in a secure, locked location, or in password protected computer files, at all times when not in use;
- c) restrict access to Survey data to persons who specifically require access in the performance of their assigned duties. Prior to making Survey data available, all staff requiring access will be informed of the use and disclosure requirements and staff shall read and sign this agreement prior to access. Snohomish County Department of Health shall submit the signed agreement to DOH.
- d) Report or publish findings in a manner that does not permit identification of students who participated in the Survey, which includes the following:
  - i. Report or publish simple frequencies only if there are 15 or more valid surveys, and
  - ii. Report or publish cross tabs only if there are at least 5 valid responses per cell at the state level or 10 per cell at the sub-state level.

4. Snohomish County Health Department will not:

- a) attempt to identify any individual student who participated in the Survey or use the Survey data for any personal reasons;
- b) release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons identifiable Survey information;
- c) copy, duplicate or otherwise retain Survey data provided or created under this Agreement for any use after the stated purposes have been accomplished.
- d) transmit any Survey data across any electronic network or medium unless the individual records have been securely encrypted.
- e) use Survey data for any purposes other than those described in their request to DOH.

Signed by all data users:

Signature \_\_\_\_\_ Date \_\_\_\_\_

Print Name \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

Print Name \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_



## APPENDIX B

### DATA SECURITY REQUIREMENTS

#### Protection of Data

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

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

#### A. Passwords

1. Passwords must always be encrypted. When stored outside of the authentication mechanism, passwords must be in a secured environment that is separate from the data and protected in the same manner as the data. For example passwords stored on mobile devices or portable storage devices must be protected as described under section F. Data storage on mobile devices or portable storage media.
2. Complex Passwords are:
  - At least 8 characters in length.
  - Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
  - Do not contain the user's name, user ID or any form of their full name.
  - Do not consist of a single complete dictionary word but can include a passphrase.
  - Do not consist of personal information (e.g., birthdates, pets' names, addresses, etc.).
  - Are unique and not reused across multiple systems and accounts.
  - Changed at least every 120 days.

#### B. Hard disk drives – 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 disks

Using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data, or

Degaussing sufficiently to ensure that the data cannot be reconstructed, or

Physically destroying the disk , or

Delete the data and physically and logically secure data storage systems that continue to be used for the storage of Confidential or Restricted information to prevent any future access to stored information. One or more of the preceding methods is performed before transfer or surplus of the systems or media containing the data.

Paper documents with Confidential or Restricted information

On-site shredding, pulping, or incineration, or

Recycling through a contracted firm provided the Contract with the recycler is certified for the secure destruction of confidential information.

Optical discs (e.g. CDs or DVDs)

Incineration, shredding, or completely defacing the readable surface with a course abrasive.

Magnetic tape

Degaussing, incinerating or crosscut shredding.

Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)

Using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data.

Physically destroying the disk.

Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.

**K. Notification of Compromise or Potential Compromise**

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

**APPENDIX C****CERTIFICATION OF DATA DISPOSITION**

Date of Disposition \_\_\_\_\_

- ☐ All copies of any Datasets related to agreement DOH#\_\_\_\_\_ have been deleted from all data storage systems. These data storage systems continue to be used for the storage of confidential data and are physically and logically secured to prevent any future access to stored information. Before transfer or surplus, all data will be eradicated from these data storage systems to effectively prevent any future access to previously stored information.
- ☐ All copies of any Datasets related to agreement DOH#\_\_\_\_\_ have been eradicated from all data storage systems to effectively prevent any future access to the previously stored information.
- ☐ All materials and computer media containing any data related to agreement DOH #\_\_\_\_\_ have been physically destroyed to prevent any future use of the materials and media.
- ☐ All paper copies of the information related to agreement DOH #\_\_\_\_\_ have been destroyed on-site by cross cut shredding.
- ☐ All copies of any Datasets related to agreement DOH #\_\_\_\_\_ that have not been disposed of in a manner described above, have been returned to DOH.
- ☐ Other

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

\_\_\_\_\_  
Signature of data recipient\_\_\_\_\_  
Date