DATA SHARING AGREEMENT
FOR DATASET(S)
BETWEEN
STATE OF WASHINGTON DEPARTMENT OF HEALTH
AND
SNOHOMISH COUNTY HEALTH DISTRICT

PARTIES: This Agreement is made between the Washington State Department of Health, Center for Health Statistics (Department) and Snohomish County Health District (Information Recipient).

PURPOSE: This Agreement documents the conditions under which the Department shares data with the Information Recipient. This Agreement documents the conditions under which the Information Recipient is approved to receive and use the data.

STATUTORY AUTHORITY:
Chapter 70.58A RCW, Vital Statistics, grants the Department statutory authority to obtain and disclose vital records data identified in this Agreement to the Information Recipient, and chapter 70.58A RCW grants the Information Recipient the authority to receive the vital records data identified in this Agreement.

PERIOD OF PERFORMANCE: This Agreement shall be effective from: date of execution through 2/28/2026.

CONTACT INFORMATION FOR INFORMATION RECIPIENT AND THE DEPARTMENT:

	INFORMATION RECIPIENT	THE DEPARTMENT
Organization Name		Washington State Department of Health
Business Contact Name		Katitza Holthaus
Title		Policy Analyst
Address		P.O. Box 47814 Olympia, WA 98504-7814
Telephone #		(360) 236-4311
Email Address		Katitza.holthaus@doh.wa.gov
Data User Contact Name		Data Sharing Coordinator
Title		
Address		P.O. Box 47814 Olympia, WA 98504-7814
Telephone #		CHS.DataRequests@doh.wa.gov
Email Address		
IT Security Contact Name		Tracy Auldredge
Title		DOH Chief Information Security Officer
Address		PO Box 47890 Olympia, WA 98504-7890
Telephone #		(360) 236-4432
Email Address		security@doh.wa.gov
Privacy Contact Name		Shannon Goudy
Title		DOH Privacy Officer
Address		P. O. Box 47890 Olympia, WA 98504-7890
Telephone #		(360) 236-4012
Email Address		Privacy.officer@doh.wa.gov

DEFINITIONS:

Authorized user is an Information Recipient's employee(s), agent(s), assign(s), representative(s), independent contractor(s), or other person(s) or entity authorized by the Department to access, use, or disclose information through this Agreement. All authorized user(s) must sign an Appendix A.

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.

Commercial purpose means a business activity by any form of business enterprise intended to generate revenue or financial benefit, including non-profit business activity.

Data means a data file containing multiple records.

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.

De-identified dataset(s) or limited dataset(s) contains potentially identifiable information.

Direct identifier means a single data element that identifies an individual person. Direct identifiers include information in accordance with Chapter 246-492 WAC.

Direct patient identifier means information that identifies a patient. Direct patient identifiers include information in accordance with WAC 246-455-085.

Disclosure means to permit access to or release, transfer, or any other form of communication of information by any means including oral, written, or electronic, to any party except the Department or the Information Recipient within this Agreement.

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.

Government agencies include Washington state boards, commissions, committees, departments, educational institutions, or other Washington state agencies which are created by or pursuant to statute, other than courts and the legislature; Washington county or city agencies, U.S. federal agencies.

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.

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

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

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

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

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

Indirect identifiers means a single data element that on its own does not identify an individual person, but when combined with other indirect identifiers can be used to identify an individual person. Indirect identifiers include information in accordance with Chapter 246-492 WAC.

Indirect patient identifier means information that may identify a patient when combined with other information. Identification of a specific patient is more likely when a file contains a group of ten or fewer similar hospitalizations. Indirect patient identifiers include information in accordance with WAC 246-455-085.

Normal business hours means the state business hours of Monday through Friday from 8:00 a.m. to 5:00 p.m. PST excluding state holidays.

Potentially identifiable information means data that contains indirect identifiers or indirect patient identifiers.

Public health purpose means a purpose that seeks to support or evaluate public health activities which include, but are not limited to, health surveillance; identifying population health trends; health assessments; implementing educational programs; program evaluation;

developing and implementing policies; determining needs for access to services and administering services; creating emergency response plans; promoting healthy lifestyles; and preventing, detecting, and responding to infectious diseases, injury, and chronic and inheritable conditions. Public health purpose does not include research as defined in this section.

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program that is considered research for other purposes. The Department's human subjects' research that involves data through intervention or interaction with the individual, or identifiable private and/or confidential information should follow the Department's Human Research Review Policy 03.001.

State holidays means New Year's Day, Martin Luther King Jr. Day, President's Day, Memorial Day, Labor Day, Independence Day, Veterans' Day, Thanksgiving day, the day after Thanksgiving day, and Christmas. Note: When January 1, 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.

Writing includes handwriting, typewriting, printing, photocopying, emailing, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated.

GENERAL TERMS AND CONDITIONS:

I. USE OF INFORMATION

The Information Recipient agrees it will only use information obtained or created under this Agreement consistent with the Exhibit(s) of this Agreement.

The ownership of all information received by the Information Recipient under this Agreement remains with the Department, and is not transferred to the Information Recipient.

The Information Recipient understands and agrees that the parties shall construe this Agreement to provide the maximum protection allowed by law of the confidentiality of the information transferred pursuant to this Agreement.

II. SAFEGUARDING INFORMATION

The Information Recipient agrees to do all of the following:

- Comply with all state and federal laws and regulations surrounding the protection and confidentiality of the information.

- Limit access and use of the information:
    - To the minimum amount of information.
    - To the purpose identified within the Exhibit(s) only.
    - For the least amount of time required to do the work.
    - Only to Authorized Users.

- Assure that all Authorized Users with access to the data:
    - Understand their responsibilities regarding use of and access to the data provided by the Department pursuant to this Agreement,
    - Agree to abide by the terms of the "Use and Disclosure of Confidential Information Form" (Appendix A), and
    - Sign and date the "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the data.

- All signed Appendix A forms must be maintained by the Information Recipient during the duration of the Agreement and for one year following the expiration of this Agreement. Information Recipient must provide the Department with any or all Appendix A forms immediately upon demand by the Department.

- A complete and up to date list of Authorized Users must be maintained by the Information Recipient at all times during the duration of this Agreement, and must be provided to the Department immediately upon demand.

  Notify the Department when Authorized Users or the contacts listed in this Agreement are no longer affiliated with the Information Recipient or are no longer authorized to access information provided under this Agreement.

- Comply with all Data Security requirements outlined in Appendix B.

- Follow DOH small numbers guidelines, as well as dataset specific small numbers requirements, covered in Appendix D.

- Unless otherwise agreed to in writing in this Agreement, or at the discretion and direction of the Department, 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 Department's Data Sharing

Coordinator within 30 calendar days of the end of this Agreement. Failure to submit an Appendix C may result in the Information Recipient's inability to receive future data.

- In the event of a breach of the terms of this Agreement, or for any other reason, the Department may by written notice require the Information Recipient to immediately destroy all copies of any data provided under this 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 Department's Data Sharing Coordinator within 30 calendar days of the date the notice was sent to the Information Recipient. Failure to submit an Appendix C may result in the Information Recipient's inability to receive future data.

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

III. RE-DISCLOSURE OF INFORMATION

Information Recipient is prohibited from disclosing in any manner all or part of the information provided under this Agreement, unless the Department has agreed otherwise in writing in the Exhibit(s).

If the Information Recipient must comply with state or federal public record disclosure or freedom of information 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 Department's Privacy Officer of the request ten (10) business days prior to disclosing to the requestor. The notice must:

- Be in writing, and
- Include a copy of the request or some other writing that shows the:
    - Date the Information Recipient received the request; and
      The Department 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. AGREEMENT ALTERATIONS AND AMENDMENTS

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

VI. CAUSE FOR TERMINATION

The Information Recipient acknowledges that unauthorized use or disclosure of the data/information or any other violation of this Agreement may be guilty of a misdemeanor, will result in the immediate termination of this Agreement, and result in denial of data/information in the future.

VII. CONFLICT OF INTEREST

The Department 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 Department 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 Department, 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 (VI) above, the Department 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 Department provided for in this section are in addition to any other rights and remedies provided by law. Any determination made by the Department under this clause shall be an issue and may be reviewed as provided in the "disputes" clause of this Agreement.

VIII. DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the Information Recipient and the Department and it cannot be resolved between the two parties, 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:

1. Be in writing and state the disputed issues, and
2. State the relative positions of the parties, and
3. State the information recipient's name, address, and his/her department agreement number, and
4. Be mailed to the DOH contracts and procurement unit, P.O. Box 47905, Olympia, WA 98504-7905 within thirty (30) calendar days after the party

could reasonably be expected to have knowledge of the issue which he/she now disputes.

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

IX. EXPOSURE TO THE DEPARTMENT'S BUSINESS INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO THIS AGREEMENT

During the course of this Agreement, the Information Recipient may inadvertently become aware of information unrelated to this Agreement. Information Recipient will disregard such information and not use it, recognizing the Department 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.

X. 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:

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

XI. 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. The Department and the Information Recipient shall cooperate in the defense of tort lawsuits, when possible.

XII. LIMITATION OF AUTHORITY

Only an authorized signatory in the Contracts and Procurement Unit for the Department 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 Department. No alteration, modification, or waiver of any clause or condition of this Agreement is effective or binding unless made in writing and signed by an authorized signatory in the Contracts and Procurement Unit for the Department.

XIII. 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.

XIV. 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.

XV. TERMINATION

Either party may terminate this Agreement for any reason upon 30 days prior written notification to the other party. The Department may terminate this Agreement, effective immediately if it finds that the Information Recipient has used or disclosed data in any manner that violates the terms of this Agreement, or its attachments, or appendices. 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. Termination of this Agreement does not extinguish the Information Recipient's obligation to delete any data or information received by following and submitting an Appendix C.

XVI. WAIVER OF DEFAULT

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

XVII. ALL WRITINGS CONTAINED HEREIN

This Agreement and attached Exhibit(s) and Appendices 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) and Appendices shall be deemed to exist or to bind any of the parties hereto.

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

THE DEPARTMENT

State of Washington Department of Health	Snohomish County Health District
Signature	Signature
Print Name	Print Name
Date	Date

EXHIBIT 1

APPROVED SCOPE OF DEATH DATA

1. PURPOSE OF DATA AUTHORIZED BY THE DEPARTMENT

To release death data to requesting entities as permitted by WAC 246-492-300(9). The Department authorizes the local deputy registrar to release only the following information:

- Decedent's name
- Date of death
- Date of birth
- Date filed
- Age of decedent
- Gender of decedent
- Decedent's residence city and state
- County of death

The local deputy registrar may not release any cause or manner of death information.

Death data may only be in the format of the EDRS Registrar Line Listing report, EDRS Obituary List report, or a spreadsheet manually created using information from EDRS or WHALES. This Agreement does not grant the local deputy registrar authority to permit access to EDRS or WHALES to other entities.

The local deputy registrar must require the entity receiving the death data to sign a data sharing agreement with the local deputy registrar. The local deputy registrar is responsible for maintaining current and valid data sharing agreements with the receiving entity.

The Information Recipient is permitted to contact individuals. ☐ Yes ☒ No

If yes: Contacting individuals that is authorized by the Department.

The data is permitted to be linked with other information. ☒ Yes ☐ No

If yes: Linking authorized by the Department.

The Department permits the local deputy registrar the authority to allow receiving entities under the Agreement with the local deputy registrar to link the data that is received. The Department recognizes the data is used by numerous local government agencies and organizations to maintain programs and services.

The data is permitted to be re-disclosed. ☒ Yes ☐ No

If yes: Re-disclosure that is authorized by the Department.

The Department authorizes the local deputy registrar to release only the following information:

- Decedent's name
- Date of death
- Date of birth
- Date filed
- Age of decedent
- Gender of decedent
- Decedent's residence city and state
- County of death

The local deputy registrar may not release any cause or manner of death information.

2. DESCRIPTION OF DATA

The Department will make available the following information under this Agreement:

☐ WA Death Annual Statistical
☐ WA Death Cause of Death Literals
☐ WA Death Names
☐ WA Death Geocode
☒ Custom: data elements listed above.

The information described in this section is:

☐ Restricted Confidential Information (Category 4)
☒ Potentially Identifiable/Confidential 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.

3. USE OF INFORMATION

The Information Recipient agrees and understands that, unless stated otherwise in this Exhibit, it is not permitted to:

- Use the information received under this Agreement for any commercial purposes.
- Sell the information to another individual or organization.
- Share or give information received under this Agreement with anyone not authorized by the Department or for any reason beyond the purposes stated in this Exhibit.

4. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

☒ DOH Web Application (indicate application name): EDRS or WHALES

☐ DOH Y: Drive (Internal DOH only)
☐ Washington State Secure File Transfer Service (sft.wa.gov)
☐ Health Information Exchange (HIE)**
☐ Other: (describe the methods for access/transfer)**

**Note: The Department's Chief Information Security Officer must approve prior to Agreement execution. The Department's Chief Information Security Officer will send approval/denial directly to the Department's Contracts Office and Business Contact.

FREQUENCY OF ACCESS/TRANSFER
☐ Repetitive: frequency _____
☒ As available or requested.

5. REIMBURSEMENT TO DOH
There is no fee charged to the Information Recipient by the Department for the information under this Agreement.

6. RIGHTS IN INFORMATION
Information Recipient agrees to provide, if requested, copies for review by the Department of any research papers or reports prepared as a result of access to Department information under this Agreement prior to publishing or distributing. If requested, submit the copies of any research papers or reports to the Department's Business Contact listed in this Agreement.

In no event shall the Department 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 Department disclaims 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.

APPENDIX A

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

Persons with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it. The Information Recipient must maintain this form. All persons provided with access to information provided pursuant to this Agreement must understand and agree to abide by the following:

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 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 when state or federal law allows or requires disclosure.

D. CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE

An Information Recipient's unauthorized use or disclosure of confidential information is the basis for the Department immediately terminating the Agreement. The Information Recipient may also be subject to administrative, civil and criminal penalties identified in law.

E. ADDITIONAL DATA USE RESTRICTIONS: (if necessary)

Signature: _____ Date: _____

Print Name: _____ Title: _____

APPENDIX B

DATA SECURITY REQUIREMENTS

The Department's Chief Information Security Officer must approve any changes to this section prior to Agreement execution; he/she will send approval/denial directly to the Department's Contracts Office and Business Contact.

The Information Recipient agrees:

- Its security practices and safeguards comply with Washington State Office of the Chief Information Officer (OCIO) security standard 141.10 *Securing Information Technology Assets*.
- Compliance with the HIPAA Security Standard and all subsequent updates meets OCIO standard 141.10 "Securing Information Technology Assets".
- Has taken steps necessary to prevent unauthorized access, use, or modification of the information in any form.

The Information Recipient agrees to store information received under this Agreement 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.
   - 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 disks. 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 8 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 on these mobile devices/media must not be stored in the Cloud. This includes device 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, and a completed Appendix C must be submitted to the DOH data sharing coordinator. Failure to submit an Appendix C may result in the Information Recipient's inability to receive future data.

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 Breach or Potential Breach**

The Information Recipient shall notify the Department's Chief Information Security Officer at security@doh.wa.gov and the Department's Business Contact within one (1) business day of any suspected or actual breach of security or confidentiality of information covered by the Agreement.

APPENDIX C

CERTIFICATION OF DATA DISPOSITION

Date of Disposition: Select date

Check all that apply:

☐ All copies of any datasets related to Agreement DOH#_____ have been destroyed from all data storage systems currently under or previously under control of the Information Recipient identified in Agreement DOH#_____ to effectively prevent any future access to the previously stored information.

☐ All materials and media currently under or previously under control of the Information Recipient identified in Agreement DOH#_____ 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 currently under or previously under control of the Information Recipient identified in Agreement DOH#_____ related to agreement DOH#_____ have been destroyed on-site by cross cut shredding.

☐ Other (provide details in an attachment to this document).

The Information 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. The person signing below indicated, by signing, that they have the authority to sign on behalf of the Information Recipient, if the Information Recipient is an organization.

Sign here _____ Select date _____

Signature of Information Recipient Date

Sign here _____

Print Name

APPENDIX D

DOH SMALL NUMBERS PUBLISHING 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%).