

**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 (DOH) 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	Washington State Department of Health (DOH)
<b>Business Contact Name</b>	Dennis Worsham	Martha Skiles
Title	Department Director	Sr. Epidemiologist
Address	3020 Rucker Ave., Ste. 306, Everett, WA 98201	111 Israel Rd. S.E. Tumwater, WA 98501
Telephone #	425.339.8687	360-236-3506
Email Address	<a href="mailto:Dennis.Worsham@co.snohomish.wa.us">Dennis.Worsham@co.snohomish.wa.us</a>	<a href="mailto:martha.skiles@doh.wa.gov">martha.skiles@doh.wa.gov</a>
<b>IT Security Contact</b>	Jim Kamp	John Weeks
Title	Business Analyst	Chief Information Security Officer
Address	3020 Rucker Ave., Ste. 306, Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425.339.8689	360-999-3454
Email Address	<a href="mailto:Jim.Kamp@co.snohomish.wa.us">Jim.Kamp@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	Evan Gaffey
Title	Public & Privacy Records Officer	Acting DOH Chief Privacy Officer
Address	3020 Rucker Ave., Ste. 306, Everett, WA 98201	P. O. Box 47890 Olympia, WA 98504-7890
Telephone #	425.339.8641	(360) 236-4437
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.

**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.

**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.

**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 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 DOE through 12/31/2026.

**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



Lacey Harper

Lacey Harper (Sep 25, 2023 09:32 PDT)

Signature

Signature

WA Department of Health Contracts Office

Lacey Harper

Print Name

Print Name

09/25/2023

09/25/2023

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 limited Washington PRAMS (Pregnancy Risk Assessment Monitoring System) datasets for Phase 8: 2016 through 2022 (when it becomes available) and Phase 9: 2023 through 2027 (when it becomes available) will be provided for public health assessment only. Data will include a county level indicator for Snohomish County Health Department.

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 analyzed and the findings reported to policymakers to keep them informed about emerging public health issues and to track the progress of various public health programs.

Parties shall use the information described in this Agreement solely for the purpose stated this Agreement.

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 A shall be effective from through\_\_\_\_\_.

**3. DESCRIPTION OF DATA**

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

**Database Name(s):** *Pregnancy Risk Assessment Monitoring System (PRAMS) Public Use Dataset*

**Data Elements being provided:** *See Appendix E – PRAMS 2020 Public Use Variables*

The limited Washington PRAMS (Pregnancy Risk Assessment Monitoring System) datasets for Phase 8: 2016 through 2022 (when it becomes available) and Phase 9: 2023 through 2027 (when it becomes available) will be provided for public health assessment only. Data will include a county level indicator for Snohomish County Health Department.

The information described in this section is:

- Restricted Confidential Information (Category 4)
- Confidential Information (Category 3)
- Potentially identifiable information (Category 3)
- Internal [public information requiring authorized access] (Category 2)
- Public Information (Category 1)

Any reference to data/information in this Agreement shall be the data/information as described in this Exhibit.

**4. STATUTORY AUTHORITY TO SHARE INFORMATION**

**DOH statutory authority** to obtain and disclose the confidential information or limited Dataset(s) identified in this Exhibit to the Information Recipient:

- RCW 43.20.050 – Powers and duties of state board of health**
- RCW 43.70.050 – Collection, use, and accessibility of health-related data**
- RCW 70.02.050 – Disclosure without patient’s authorization**
- RCW 42.48 - Disclosure for scientific merit, governed by IRB approval**

**5. ACCESS TO INFORMATION**

**METHOD OF ACCESS/TRANSFER**

- DOH Web Application (indicate application name):
- Washington State Managed File Transfer Service (mft.wa.gov)
- Encrypted CD/DVD or other storage device
- Health Information Exchange (HIE)\*\*
- Other: (describe the methods for access/transfer)\*\*

**\*\*NOTE:** DOH Chief Information Security Officer must approve prior to Agreement execution. DOH Chief Information Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

FREQUENCY OF ACCESS/TRANSFER

- One time: DOH shall deliver information by \_\_\_\_\_ (insert date)
- Repetitive: frequency or dates \_\_\_\_\_ (insert dates if applicable)
- As available within the period of performance stated in Section 2.

**6. REIMBURSEMENT TO DOH**

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

Billing Procedure

- Information Recipient agrees to pay DOH by check or account transfer within 30 calendar days of receiving the DOH invoice.
- Upon expiration of the Agreement, any payment not already made shall be submitted within 30 days after the expiration date or the end of the fiscal year, which is earlier.

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

- \$ \_\_\_\_\_
- No charge.

**7. DATA DISPOSITION**

Unless otherwise directed in writing by the DOH Business Contact, at the end of this Agreement, or at the discretion and direction of DOH, the Information Recipient shall:

- Immediately destroy all copies of any data provided under this Agreement after it has been used for the purposes specified in the Agreement . Acceptable methods of destruction are described in Appendix B. Upon completion, the Information Recipient shall submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.
- Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes

specified in the Agreement, along with the attached Certification of Data Disposition (Appendix C)

Retain the data for the purposes stated herein for a period of time not to exceed \_\_ one year after termination of this agreement, unless superseded by another agreement for the same purpose. \_ (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 reports, press releases, web pages, and any publications of PRAMS data to the attention of: Linda Lohdefinck, PRAMS Coordinator, Office of Family and Community Health Improvement, PO Box 47835, Olympia, WA 98504-7835 (Linda.Lohdefinck@doh.wa.gov or WAPRAMS@doh.wa.gov) .

## 9. ALL WRITINGS CONTAINED HEREIN

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

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

**INFORMATION PROVIDER**

State of Washington Department of Health



\_\_\_\_\_  
Signature

WA Department of Health Contracts Office

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

09/25/2023

\_\_\_\_\_  
Date

**INFORMATION RECIPIENT**

Snohomish County



Lacey Harper (Sep 25, 2023 09:32 PDT)

\_\_\_\_\_  
Signature

Lacey Harper

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

09/25/2023

\_\_\_\_\_  
Date

**APPENDIX A**

**USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION**

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it. Below are key elements:

A. **CONFIDENTIAL INFORMATION**

Confidential information is information federal and state law protects from public disclosure. Examples of confidential information are social security numbers, and healthcare information that is identifiable to a specific person under RCW 70.02. The general public disclosure law identifying exemptions is RCW 42.56.

B. **ACCESS AND USE OF CONFIDENTIAL INFORMATION**

1. Access to confidential information must be limited to people whose work specifically requires that access to the information.
2. Use of confidential information is limited to purposes specified elsewhere in this Agreement.

C. **DISCLOSURE OF CONFIDENTIAL INFORMATION**

1. An Information Recipient may disclose an individual's confidential information received or created under this Agreement to that individual or that individual's personal representative consistent with law.
2. An Information Recipient may disclose an individual's confidential information, received or created under this Agreement only as permitted under the **Re-Disclosure of Information** section of the Agreement, and as state and federal laws allow.

D. **CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE**

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

E. **ADDITIONAL DATA USE RESTRICTIONS: (if necessary)**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_



## APPENDIX B

### DATA SECURITY REQUIREMENTS

#### Protection of Data

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

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

#### A. Passwords

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

#### B. Hard Disk Drives / Solid State Drives – Data stored on workstation drives:

1. The data must be encrypted as described under section *F. Data storage on mobile devices or portable storage media*. Encryption is not required when Potentially Identifiable Information is stored temporarily on local workstation Hard Disk Drives/Solid State Drives. Temporary storage is thirty (30) days or less.
2. Access to the data is restricted to authorized users by requiring logon to the local workstation using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

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

**C. Network server and storage area networks (SAN)**

1. Access to the data is restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network.
2. Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.
3. The data are located in a secured computer area, which is accessible only by authorized personnel with access controlled through use of a key, card key, or comparable mechanism.
4. If the servers or storage area networks are not located in a secured computer area **or** if the data is classified as Confidential or Restricted it must be encrypted as described under F. Data storage on mobile devices or portable storage media.

**D. Optical discs (CDs or DVDs)**

1. Optical discs containing the data must be encrypted as described under F. Data storage on mobile devices or portable storage media.
2. When not in use for the purpose of this Agreement, such discs must be locked in a drawer, cabinet or other physically secured container to which only authorized users have the key, combination or mechanism required to access the contents of the container.

**E. Access over the Internet or the State Governmental Network (SGN).**

1. When the data is transmitted between DOH and the Information Recipient, access is controlled by the DOH, who will issue authentication credentials.
2. Information Recipient will notify DOH immediately whenever:
  - a) An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Information Recipient;
  - b) Whenever a person's duties change such that the person no longer requires access to perform work for this Contract.

3. The data must not be transferred or accessed over the Internet by the Information Recipient in any other manner unless specifically authorized within the terms of the Agreement.
  - a) If so authorized the data must be encrypted during transmissions using a key length of at least 128 bits. Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required.
  - b) Authentication must occur using a unique user ID and Complex Password (of at least 10 characters). 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 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 J, Disposition of Information, have been fulfilled as indicated above.

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

\_\_\_\_\_  
Date

## APPENDIX D

### **DOH SMALL NUMBERS GUIDELINES**

- Aggregate data so that the need for suppression is minimal. Suppress all non-zero counts which are less than ten.
- Suppress rates or proportions derived from those suppressed counts.
- Assure that suppressed cells cannot be recalculated through subtraction, by using secondary suppression as necessary. Survey data from surveys in which 80% or more of the eligible population is surveyed should be treated as non-survey data.
- When a survey includes less than 80% of the eligible population, and the respondents are unequally weighted, so that cell sample sizes cannot be directly calculated from the weighted survey estimates, then there is no suppression requirement for the weighted survey estimates.
- When a survey includes less than 80% of the eligible population, but the respondents are equally weighted, then survey estimates based on fewer than 10 respondents should be “top-coded” (estimates of less than 5% or greater than 95% should be presented as 0-5% or 95-100%).

### **ADDITIONAL DATASET SPECIFIC SMALL NUMBERS REQUIREMENTS**

Information Recipient agrees not to:

- Publish results at the county level if the total number of respondents in dataset for the county is less than 50.
- Publish results if the number of participants in each analysis is at less than 30.

## APPENDIX E

PRAMS 2021 Limited Dataset Variables

1	abcond1-abcond6	44	delivery_method_final	87	intensive_care
2	abnormal_conditions_none	45	diabetes	88	labchar1-labchar7
3	abnormal_conditions_unknown	46	down_confirm	89	labons1-labons3
4	anencephaly	47	down_pending	90	labor_onset_none
5	anesthesia	48	down_syndrome	91	labor_onset_unknown
6	antibiotics	49	downsflg	92	last_live_birth_year
7	apgar_10	50	ecv_failed	93	last_prenatal_visit_year
8	apgar_5	51	ecv_success	94	limb_defect
9	assist_vent	52	facility_type	95	malf1-malf7
10	assist_vent_6	53	father_birthplace_cntry_wa_code	96	married_2016
11	assisted_reproduction	54	father_birthplace_state	97	mat_labor_characteristics_none
12	attempt_forceps	55	father_calculated_age	98	mat_labor_characteristics_unk
13	attempt_vacuum	56	father_educ_8th_grade_or_less	99	maternal_morbidity_none
14	attendant_class	57	father_education	100	maternal_morbidity_unknown
15	augmentation	58	father_hispanic	101	maternal_transfusion
16	birth_hr	59	Variable Name	102	meconium_stain
17	birth_order	60	father_race_summary_code	103	minfect1-minfect7
18	birth_weight_grams	61	fertility_treatment	104	mmorbid1-mmorbid5
19	birthplace_state_nchs_code	62	fetal_intolerance	105	mother_birthplace_cntry_wa_code
20	calculated_gestation	63	fetal_presentation	106	mother_birthplace_state
21	cephaflg	64	gastroschisis	107	mother_calculated_age
22	certifier_class	65	gestation_calculated_flag	108	mother_educ_8th_grade_or_less
23	certyear	66	gestation_estimate	109	mother_education
24	cervical_cerclage	67	gestational_diabetes	110	mother_height_feet
25	child_antibiotics	68	gestational_hypertention	111	mother_height_inches
26	child_injury	69	gonorrhea	112	mother_hispanic
27	child_seizure	70	group_b_strep	113	mother_marital_status
28	child_transfer	71	head_circumference	114	mother_months_at_residence
29	chlamydia	72	hep_b	115	mother_race_summary_code
30	chorioamnionitis	73	hep_c	116	mother_residence_state_nchs_code
31	cigarettes_smoked_1st_tri	74	herpes	117	mother_transfer
32	Variable Name	75	hiv	118	mother_weight_at_delivery
33	cigarettes_smoked_2nd_tri	76	hyperflg	119	mother_weight_gain
34	cigarettes_smoked_3_months_prior	77	hypertension_eclampsia	120	mother_weight_prior
35	cigarettes_smoked_3rd_tri	78	hypospadias	121	mother_years_at_residence
36	cleft_lip	79	hysterectomy	122	mrf1-mrf6
37	cleft_palate	80	induction	123	Variable Name
38	cnty_res	81	infections_none	124	msb
39	congenital_anomaly_none	82	infections_other	125	nchs_month_prenatal_care_began
40	congenital_anomaly_unknown	83	infections_other_specify	126	nicu_admission
41	congenital_heart	84	Variable Name	127	non_vertex_presentation
42	congenital_hernia	85	infections_unknown	128	num_prev_cesarean
43	delivery_method_calculation	86	intended_facility	129	number_prenatal_visits



130	obproc1-obproc4	177	hi_num	224	momcig
131	obstet_proc_none	178	inf_live	225	momlbs
132	obstet_proc_unknown	179	inf_wmom	226	momsmoke
133	omphalocele	180	infq_age_mod	227	pob
134	operation	181	ins_num	228	trans
135	other_chrom	182	kessner	229	batch
136	other_chrom_confirm	183	kotelchuck	230	modeprt
137	other_chrom_pending	184	lga	231	cell
138	other_preg_outcomes	185	macrosomia	232	inqx
139	other_preg_outcomes_month	186	mat_age_naphsis	233	nest_yr
140	other_preg_outcomes_year	187	mom_bmi	234	sam_yrs
141	packs_smoked_1st_tri	188	mom_bmi_bc	235	sament
142	packs_smoked_2nd_tri	189	mom_bmig	236	stratumc
143	packs_smoked_3_months_prior	190	mom_bmig_bc	237	sud_nest
144	packs_smoked_3rd_tri	191	mom_bmig_qx_rev	238	totcnt
145	perineal_laceration	192	mom_mtrs	239	wtanal
146	plurality	193	mom_wt	240	wtone
147	poor_preg_outcomes	194	nchs_urb_rur2	241	wththree
148	precipitous_labor	195	nohosp_b	242	wtwo
149	Variable Name	196	pg_tdap8_dk	243	age1517
150	prepreg_diabetes	197	pgwtgn8_dk	244	age4
151	prepreg_hypertension	198	Variable Name	245	age5
152	preterm_births	199	pgwtgnu8_dk	246	age6
153	previous_cesarean	200	pnc_1trm	247	agetn
154	prior_live_births_deceased	201	pnc_vst_naphsis	248	dadrace
155	prior_live_births_living	202	pnc_wks	249	ed2
156	prolonged_labor	203	pncno	250	father_year_of_birth
157	risk_factors_none	204	pp_depress	251	fpc
158	risk_factors_unknown	205	pp_num	252	lbw
159	ruptured_membranes	206	pre_lb_naphsis	253	married
160	ruptured_uterus	207	qx_phase	254	momrace
161	sex	208	sga_10	255	mother_year_of_birth
162	source_of_payment	209	sga_2sd	256	pgint3
163	steroids	210	smk63b_a	257	race_dad
164	surfactant	211	smk63l_a	258	race_mom
165	syphilis	212	smk6c_nw	259	Variable Name
166	tocolysis	213	smk6c_pg	260	race7
167	vaginal_bleeding	214	smk6c_pp	261	sex_num
168	wic	215	smk6nw_a	262	stratumy
169	bc_yrllb	216	strs_t_g	263	vlbw
170	bf5weeks	217	strs_tt3	264	ashk_jew
171	drk83b_a	218	brstfed	265	br_ovcnr
172	Variable Name	219	defect	266	brcnr_2side
173	drk83l_a	220	infer_tr	267	brcnr_aunt
174	drk8c_pg	221	mat_deg	268	brcnr_bro
175	gest_wk_naphsis	222	mm_nomd	269	brcnr_cous
176	gram_naphsis	223	Variable Name	270	brcnr_d_dad

271	brcnr_d_mom	318	vacbarr_efmom	365	drgp_cbd
272	brcnr_dad	319	vacbarr_elig	366	drgp_ccn
273	brcnr_m_dad	320	vacbarr_hcwno	367	drgp_dep
274	brcnr_m_mom	321	vacbarr_info	368	drgp_hrn
275	brcnr_mom	322	vacbarr_tran	369	drgp_huf
276	brcnr_naunt	323	vacbarr_vacbp	370	drgp_k2
277	brcnr_nbro	324	work_none	371	drgp_lsd
278	brcnr_ncous	325	wrk_hlter	372	drgp_mj
279	brcnr_nsis	326	wrk_medcr	373	drgp_mth
280	brcnr_nuncle	327	wrk_nopubl	374	drgp_nal
281	brcnr_sis	328	wrk_publ	375	drgp_spd
282	brcnr_uncle	329	dp_hcwppr	376	drgp_tnq
283	brcnr_young	330	dp_mat	377	pphrm_inf
284	cnr_couns	331	dp_ppr_cod	378	pphrm_mom
285	coun_brcnr	332	dp_ppr_fent	379	t1_pprtm_lngth
286	coun_other	333	dp_ppr_hcod	380	t1_pprtm_lngtu
287	coun_ovcnr	334	dp_ppr_hmor	381	t2_pprtm_lngth
288	couns_reason	335	dp_ppr_mor	382	t2_pprtm_lngtu
289	ovcnr_aunt	336	dp_ppr_ocod	383	t3_pprtm_lngth
290	ovcnr_cous	337	dp_ppr_omor	384	t3_pprtm_lngtu
291	ovcnr_d_mom	338	dp_ppr_tra	385	ask_abus
292	ovcnr_m_mom	339	dp_pprcut	386	ask_bdef
293	ovcnr_mom	340	dp_pprcuthlp	387	ask_bf
294	ovcnr_naunt	341	dp_pprcuttbl	388	ask_dprs
295	ovcnr_ncous	342	dp_pprlc_den	389	ask_drug
296	ovcnr_nsis	343	dp_pprlc_dr	390	ask_hivt
297	ovcnr_sis	344	dp_pprlc_er	391	ask_labr
298	dp_covac	345	dp_pprlc_fam	392	ask_meds
299	hcw_ofrvac	346	dp_pprlc_nrx	393	ask_merc
300	hcw_recvac	347	dp_pprlc_ob	394	ask_ppbc
301	hcw_refvac	348	dp_pprlc_oth	395	bc_now4
302	hcw_tlkvac	349	dp_pprlc_rx	396	bc_when4
303	infcovac	350	dp_pprus_emo	397	bcb_husb
304	pp_covac	351	dp_pprus_hgh	398	bcb_nsex
305	vacbar_altmet	352	Variable Name	399	bcb_oth
306	vacbar_noben	353	dp_pprus_hok	400	bcb_pay
307	vacbar_norsk	354	dp_pprus_inj	401	bcb_pnow
308	vacbar_oth	355	dp_pprus_injbp	402	bcb_preg
309	vacbar_prot	356	dp_pprus_oth	403	bcb_side
310	vacbar_serill	357	dp_pprus_rlx	404	bcb_tube
311	vacbarr_alrg	358	dp_pprus_slp	405	bcb_want
312	vacbarr_alwd	359	dp_pruse_acet	406	bcp_cond
313	vacbarr_appt	360	dp_pruse_asp	407	bcp_impl
314	vacbarr_avail	361	dp_pruse_ibu	408	bcp_iud
315	vacbarr_cov	362	dp_pruse_nap	409	bcp_nsex
316	vacbarr_devtm	363	drgp_add	410	bcp_oth
317	vacbarr_efinf	364	drgp_anx	411	bcp_pill

412	bcp_ptrg	459	ces_pos	506	inshcex
413	bcp_pull	460	ces_prev	507	insihs
414	bcp_rhyt	461	ces_prob	508	insmed
415	bcp_sht3	462	ces_size	509	insmil
416	bcp_tube	463	ces_time	510	insnone
417	bcp_vase	464	dds_acpt8	511	insoth
418	bf5ever	465	dds_cln	512	inspar
419	bf5lngth	466	dds_cost8	513	Variable Name
420	bf5lngtu	467	dds_medi8	514	inswork8
421	bf5still	468	dds_ntwt8	515	language
422	bfc5diff	469	dds_safe8	516	lth_hosp
423	bfc5home	470	del6how	517	mdob_mth
424	bfc5illm	471	drk_2yrs	518	mdob_yr4
425	bfc5jaun	472	drk8_3b	519	mh_pgdx8
426	bfc5milk	473	drk8_3l	520	mh_ppdpr
427	bfc5oth	474	ecig_3b	521	mh_ppint
428	bfc5sat	475	ecig_3l	522	mom_cm
429	bfc5sore	476	flubby	523	mom_feet
430	bfc5stop	477	flunor	524	mom_inch
431	Variable Name	478	fluoth	525	mom_lbkg
432	bfc5wt	479	flupreg	526	morb_bp8
433	bfc8husb	480	flushot	527	nbc_get
434	bfc8schl	481	fluside	528	nbc_husb
435	bfc8work	482	flutlk	529	nbc_mem
436	bfinf_bdr	483	fluwno	530	nbc_mind
437	bfinf_dr	484	fluwrk	531	nbc_oth
438	bfinf_fam	485	hdp_angr	532	nbc_side
439	bfinf_grp	486	hdp_ctrl	533	nbc_ster
440	bfinf_hot	487	hdp_saf	534	nbc_time
441	bfinf_nur	488	hdp_sex	535	pab_xhus
442	bfinf_oth	489	hi_hcex	536	pab6hus
443	bfinf_spc	490	hi_ihs	537	pad_xhus
444	bfp_ins	491	hi_medic	538	pad6hus
445	bfp_ms	492	hi_milit	539	pbc_cond
446	bfp_oth	493	hi_none	540	pbc_impl
447	bfp_race	494	hi_oth	541	pbc_iud
448	bfp_wgt	495	hi_par	542	pbc_map
449	bpg_deprs8	496	hi_work8	543	pbc_oth
450	bpg_diab8	497	hth_anx	544	pbc_pill
451	bpg_hbp8	498	hth_asma	545	pbc_ptrg
452	ces_comp	499	hth_thyr	546	pbc_pull
453	ces_dgr	500	idob_mth	547	pbc_rhyt
454	ces_due	501	idob_yr4	548	pbc_sht3
455	ces_ind	502	inc_ndep	549	pg_gdb8
456	ces_nvag	503	income8	550	pg_tdap8
457	ces_oth	504	inflive5	551	pgintent
458	ces_plan	505	infwmom5	552	pgwtgn8

553	pgwtgnu8	584	sleepown	615	strs_job
554	pnc_1st	585	sleeppos	616	strs_mov
555	pnc_1stu	586	slp_chr	617	strs_pay
556	pot_b4	587	slp_crb8	618	strs_pg
557	pot_pg	588	slp_mat8	619	strs_wrk
558	pot_pp	589	slp_nblk	620	strshome
559	pp_ihs	590	slp_npad	621	tlk_cigs
560	pp_medic	591	slp_room	622	tlk_etoh
561	pp_milit	592	Variable Name	623	tlk_wt
562	pp_none	593	slp_sak	624	tod_mth
563	pp_oth	594	slp_swg	625	tod_yr4
564	pp8_hcex	595	slp_toypil	626	typ_bc
565	pp8_nopnc	596	slp2back	627	typ_dds
566	pp8_par	597	slp2crb	628	typ_doct
567	pp8_work	598	slp2myrm	629	typ_illn
568	ppv_chk	599	slp2ntbd	630	typ_injr
569	pre_abus	600	smk_chew	631	typ_mh
570	pre_bdef	601	smk_ecig	632	typ_obgn
571	pre_hivt	602	smk_hook	633	typ_othr
572	pre_hlth	603	smk2yrs	634	typ_what
573	pre_kids	604	smk6_3b	635	vitamin
574	pre_mhdp	605	smk6_3l	636	vpp_abus
575	pre_morb	606	smk6_3n	637	vpp_bcm
576	pre_prbc	607	strs_arg	638	vpp_depr
577	pre_smk	608	strs_awy	639	vpp_diab
578	pre_sti	609	strs_bil	640	vpp_eat
579	pre_vist	610	strs_dh3	641	vpp_nsrt
580	pre_vit	611	strs_drg	642	vpp_presbc
581	pre_work	612	strs_dv3	643	vpp_smok
582	pre_wt	613	strs_fm3	644	vpp_vit
583	preg_try	614	strs_jl3	645	vpp_wait