615 Sheridan Street
Port Townsend, WA 98368
www.JeffersonCountyPublicHealth.org
Consent Agenda

JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA REQUEST

TO: **Board of County Commissioners**
Mark McCauley, County Administrator

FROM: Apple Martine, Jefferson County Public Health Director
Ocean Mason, Jefferson County Public Health Communicable Disease Team Lead

DATE: April 21, 2025

SUBJECT: Agenda item – Data Sharing Agreement Between Jefferson County Public Health and Washington State Department of Health - upon signature until 12/31/2029

STATEMENT OF ISSUE:

Jefferson County Public Health (JCPH) seeks Board approval of a Data Sharing Agreement (DSA) with the Washington State Department of Health (DOH). This agreement provides the framework for secure, lawful access and use of sensitive data within the state's syringe services program (SSP) data system (REDCap). The DSA ensures JCPH can input, store, and access potentially identifiable and confidential information essential to its harm reduction and public health programming. The agreement spans from the date of execution through December 31, 2029.

ANALYSIS/STRATEGIC GOALS/PROS and CONS:

This agreement strengthens JCPH's harm reduction efforts by enabling secure access to the state SSP data system, supporting more coordinated, data-informed care. It enhances public health surveillance, improves client services, and aligns with JCPH's strategic goals. While it requires diligent compliance with security protocols, the benefits—expanded data capacity, confidentiality safeguards, and stronger public health response—far outweigh the administrative burden.

FISCAL IMPACT/COST BENEFIT ANALYSIS:

There is no charge for this service. There is no fiscal impact.

RECOMMENDATION:

JCPH management requests approval of this Data Sharing Agreement from upon signature until 12/31/2029 or terminated by either party.

REVIEWED BY:

Mark McCauley, County Administrator — Date: 4/17/25

Community Health
Developmental Disabilities
360-385-9400
360-385-9401 (f)

Environmental Public Health
360-385-9444
(f) 360-379-4487

Clear Form

CONTRACT REVIEW FORM

(INSTRUCTIONS ARE ON THE NEXT PAGE)

CONTRACT WITH: Washington State Department of Health Contract No: AD-25-018

Contract For: Data Share: Syringe Services Term: 1/1/2025-12/31/2029

COUNTY DEPARTMENT:	Jefferson County Public Health
Contact Person:	ocean mason
Contact Phone:	360-379-4480
Contact email:	omason@co.jefferson.wa.us

AMOUNT: n/a

Revenue: _____

Expenditure: _____

Matching Funds Required: _____

Sources(s) of Matching Funds _____

Fund # _____

Munis Org/Obj _____

PROCESS:

- ☐ **Exempt from Bid Process**
- ☐ **Cooperative Purchase**
- ☐ **Competitive Sealed Bid**
- ☐ **Small Works Roster**
- ☐ **Vendor List Bid**
- ☐ **RFP or RFQ**
- ☐ **Other:** _____

APPROVAL STEPS:

STEP 1: DEPARTMENT CERTIFIES COMPLIANCE WITH JCC 3.55.080 AND CHAPTER 42.23 RCW.

CERTIFIED: ☐ **N/A:** ■ Signature April 15, 2025 Date

STEP 2: DEPARTMENT CERTIFIES THE PERSON PROPOSED FOR CONTRACTING WITH THE COUNTY (CONTRACTOR) HAS NOT BEEN DEBARRED BY ANY FEDERAL, STATE, OR LOCAL AGENCY.

CERTIFIED: ☐ **N/A:** ■ Signature April 15, 2025 Date

STEP 3: RISK MANAGEMENT REVIEW (will be added electronically through Laserfiche):

Electronically approved by Risk Management on 4/16/2025.

STEP 4: PROSECUTING ATTORNEY REVIEW (will be added electronically through Laserfiche):

Electronically approved as to form by PAO on 4/16/2025.
State data share agreement.

STEP 5: DEPARTMENT MAKES REVISIONS & RESUBMITS TO RISK MANAGEMENT AND PROSECUTING ATTORNEY(IF REQUIRED).

STEP 6: CONTRACTOR SIGNS

STEP 7: SUBMIT TO BOCC FOR APPROVAL

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

This Agreement documents the conditions under which Washington DOH shares confidential information or limited Dataset(s) with other entities.

CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION

	INFORMATION RECIPIENT	INFORMATION PROVIDER
Organization Name	Washington State Department of Health (DOH)	Jefferson County Public Health
Business Contact Name	Rachel Amiya	Ocean Mason
Title	Assessment Unit Manager	Public Health Nurse
Address	101 Israel Rd SE	615 Sheridan Street, Port Townsend, WA 98368
Telephone #		360-379-4480
Email Address	Rachel.amiya@doh.wa.gov	omason@co.jefferson.wa.us
IT Security Contact	John Weeks	Mikey Forville
Title	Chief Information Security Officer	Network Foreman
Address	PO Box 47890 Olympia, WA 98504-7890	1820 Jefferson Street, Port Townsend, WA 98368
Telephone #	360-999-3454	360-385-9209
Email Address	Security@doh.wa.gov	mforville@co.jefferson.wa.us
Privacy Contact Name	Michael Paul	Veronica Shaw
Title	DOH Chief Privacy Officer	Deputy Director
Address	P. O. Box 47890 Olympia, WA 98504-7890	615 Sheridan Street, Port Townsend, WA 98368
Telephone #	(564) 669-9692	360-385-9409
Email Address	Privacy.officer@doh.wa.gov	veronica@co.jefferson.wa.us

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.

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) 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 information provider.

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 information provider 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 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 the information provider 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 Information Provider 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 Information Provider, 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.

IX. DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the Information Provider 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. 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.

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. Information Provider and the Information Recipient shall cooperate in the defense of tort lawsuits, when possible.

XII. 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.

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 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.

XVI. 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.

XVII. 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.

XVIII. PERIOD OF PERFORMANCE

This **Agreement** shall be effective from 1/1/2025 through 12/31/2029.

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

INFORMATION PROVIDER

Jefferson County Public Health
Board of County Commissioners
Jefferson County, Washington

Signature

Heidi Eisenhour, Chair
Print Name

Date

INFORMATION RECIPIENT

State of Washington Department of Health

Signature

Print Name

Date

Approved as to form only:

Philip C. Hunsucker
Chief Civil Deputy Prosecuting Attorney

04/16/2025
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 purpose of this agreement is to provide protections and a framework for appropriate for data stored by syringe services programs (SSP's) within DOH's SSP data system. Syringe Services are programs operated by a variety of organizations (to date local governments, not for profit entities) which provide harm reduction supplies, including syringes, to the communities they inhabit. The DOH's SSP data system is designed as a tool to assist state-funded SSP's in collecting and storing data. It is accessed via browser and is intended to be used by SSP staff to enter and develop reports describing program data. The DOH requires minimal aggregate data to be stored in the SSP data system as a requirement for funding, but allows SSP's to store a variety of data in order to meet their program needs. This can include personally identifiable information which could cause significant harm if it were released. This agreement encompasses data that the SSP's store in the data system beyond the minimum funding reporting requirements (CLH31013). The data reported to DOH in the system to meet the minimum funding reporting requirements can be used without restriction.

The DOH may use the data in the system to

-To monitor and evaluate program outcomes to inform decisions on resource planning and allocation.
-Characterize trends in drug use and harm reduction service utilization in Washington state
-To identify novel public health concerns related to syringe service programs

Is the purpose of this agreement for human subjects research that requires Washington State Institutional Review Board (WSIRB) approval?

☐ Yes ☒ No

If yes, has a WSIRB review and approval been received? If yes, please provide copy of approval. If No, attach exception letter.

☐ Yes ☒ No

2. PERIOD OF PERFORMANCE

This **Exhibit** shall have the same period of performance as the **Agreement** unless otherwise noted below:

Exhibit ___ shall be effective from 1/1/2025 through 12/31/2029.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:
Database Name(s): *REDCap SSP Database*
Data Elements being provided:

See Appendix E

The information described in this section is:

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

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

4. STATUTORY AUTHORITY TO SHARE INFORMATION

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

RCW 43.70.050 (2) – Collection, use, and accessibility of health-related data
RCW 43.70.070(2) - Duties of department—Analysis of health services.
RCW 43.70.130(2) and (10) - Powers and duties of secretary—General.

5. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

- ☐ DOH Web Application (indicate application name):
- ☐ Washington State Secure File Transfer Service (sft.wa.gov)
- ☐ Encrypted CD/DVD or other storage device
- ☐ Health Information Exchange (HIE)**
- ☒ Other: Redcap SSP Data System

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

FREQUENCY OF ACCESS/TRANSFER

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

6. REIMBURSEMENT TO DOH

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

Billing Procedure

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

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

☐ $_____
☒ No charge.

7. DATA DISPOSITION

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

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

☐ Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes

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

☐ Retain the data for the purposes stated herein for a period of time not to exceed _____ (*e.g., one year, etc.*), after which Information Recipient shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☒ Other (Describe): Information Recipient will retain the data for 2 years, after which Information Recipient will destroy all identifiers (names, dates of birth, unique identifiers, addresses, phone numbers, other contact information) and will retain the data in de-identified form.

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 _____ (insert list of items)____
  to the attention of: __(insert name of DOH employee) __
  at ___(insert address to which material is sent)____ .

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

Jefferson County Public Health
Board of County Commissioners
Jefferson County, Washington

_____
Signature

Heidi Eisenhour, Chair
Print Name

_____
Date

INFORMATION RECIPIENT

State of Washington Department of Health

_____
Signature

Print Name

_____
Date

APPENDIX A

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

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

A. CONFIDENTIAL INFORMATION

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

B. ACCESS AND USE OF CONFIDENTIAL INFORMATION

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

C. DISCLOSURE OF CONFIDENTIAL INFORMATION

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

D. CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE

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

E. ADDITIONAL DATA USE RESTRICTIONS: (if necessary)

Signature: _____

Date: _____

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%).

APPENDIX E

LIST OF DATA ELEMENTS BEING PROVIDED

Form	Question	Field Type
registration	Record ID	text
registration	First 2 letters of last name	text
registration	First letter of first name	text
registration	First letter of mother's first name	text
registration	2 digit day of the month you were born	text
registration	Unique ID	text
registration	tiebreaker field for duplicate unique ID's	text
registration	Notes or messages for all staff:	notes
ssp_intake	SSP Intake Date	text
ssp_intake	Intake Site	dropdown
ssp_intake	Provider name	dropdown
ssp_intake	How do you identify your gender?	checkbox
ssp_intake	What is your age?	radio
ssp_intake	Race/ethnicity	checkbox
ssp_intake	In the last 30 days, where did you sleep most frequently?	radio
ssp_intake	Zip code (if applicable)	text
ssp_intake	Are you exchanging today for yourself, others, or both?	checkbox
ssp_intake	In the last 7 days, which drugs have you used?	checkbox
ssp_intake	What do you consider to be your primary drug?	radio
ssp_intake	On a typical day, how many times do you inject (if at all)?	radio
ssp_intake	On a typical day, how many smoking sessions do you have (if at all)?	radio
ssp_intake	Routes of administration in past 30 days	checkbox
ssp_intake	In the last 30 days, have you had to do any of the following because you didn't have a new, sterile syringe?	checkbox
ssp_intake	In the last 30 days, have you had to do any of the following because you didn't have access to smoking supplies (e.g. pipe, foil, tooter)	checkbox
ssp_intake	Health behavior in the past 90 days:	checkbox
ssp_intake	Do you currently have health insurance?	yesno
ssp_intake	What type of health insurance do you have?	checkbox
ssp_intake	How did you hear about us?	dropdown
ssp_intake	Notes	notes
ssp_encounter	Encounter date	text
ssp_encounter	Site name	dropdown
ssp_encounter	Provider	dropdown
ssp_encounter	Delivery zip code	text
ssp_encounter	First encounter?	checkbox
ssp_encounter	How many people are you exchanging or getting supplies for today?	radio
ssp_encounter	In the past 30 days, have you shared needles/works?	yesno
ssp_encounter	In the past 30 days, have you reused syringes?	yesno

ssp_encounter	Syringes returned	text
ssp_encounter	Sharps containers returned	text
ssp_encounter	Syringes returned	checkbox
ssp_encounter	Were any supply items requested but unavailable?	checkbox
ssp_encounter	Unavailable supplies	checkbox
ssp_encounter	Basic needs provided	checkbox
ssp_encounter	Syringes distributed	text
ssp_encounter	HRT kit	text
ssp_encounter	Boofing kit	text
ssp_encounter	Snorting kit	text
ssp_encounter	Plan B	text
ssp_encounter	Pregnancy tests	text
ssp_encounter	Bubbles/meth pipe	text
ssp_encounter	Stem/crack pipe	text
ssp_encounter	Hammer pipe	text
ssp_encounter	Foil	text
ssp_encounter	Mouthpiece	text
ssp_encounter	Chore/brillo	text
ssp_encounter	External condoms	text
ssp_encounter	Lube	text
ssp_encounter	Internal condoms distributed	text
ssp_encounter	Dental dams	text
ssp_encounter	Fentanyl test strips	text
ssp_encounter	Xylazine test strips	text
ssp_encounter	Wound care kit	text
ssp_encounter	Hygiene kit	text
ssp_encounter	Biohazard bin (1 quart)	text
ssp_encounter	Biohazard bin (2 gallon)	text
ssp_encounter	Nasal naloxone kits	text
ssp_encounter	Injectable naloxone kits	text
ssp_encounter	Naloxone kits (any type)	text
ssp_encounter	Naloxone training provided?	checkbox
ssp_encounter	Have you used naloxone since your last visit?	checkbox
ssp_encounter	How many overdoses have you responded to since your last visit to this ssp?	text
ssp_encounter	How many overdoses have you successfully reversed since your last visit to this ssp?	text
ssp_encounter	For the most recent reversal, how many doses were administered?	text
ssp_encounter	What type of naloxone was used?	checkbox
ssp_encounter	Where did the overdose occur?	radio
ssp_encounter	What happened to the person that overdosed after they were given naloxone?	radio
ssp_encounter	Did you receive the naloxone kit that was used from this SSP?	radio
ssp_encounter	Routes of administration in past 30 days	checkbox

ssp_encounter	In the last 30 days, have you had to do any of the following because you didn't have a new, sterile syringe?	checkbox
ssp_encounter	Education provided	checkbox
ssp_encounter	Services provided	checkbox
ssp_encounter	Referrals	checkbox
ssp_encounter	Referrals: Infectious disease testing type	checkbox
ssp_encounter	Referrals: Infectious disease treatment type	checkbox
ssp_encounter	Referred facility name(s)	text
ssp_encounter	Notes	notes
hrcn_participant_profile	Enrollment Date	text
hrcn_participant_profile	Consent and confidentiality form signed	checkbox
hrcn_participant_profile	Active in Harm Reduction Care Navigation?	checkbox
hrcn_participant_profile	First name	text
hrcn_participant_profile	Last name	text
hrcn_participant_profile	(optional) What do you like to be called? (Nickname/Alias)	text
hrcn_participant_profile	Date of Birth	text
hrcn_participant_profile	Gender Identity	checkbox
hrcn_participant_profile	Race/Ethnicity	checkbox
hrcn_participant_profile	Other Race/Ethnicity	text
hrcn_participant_profile	Housing status	radio
hrcn_participant_profile	Do you have health insurance?	checkbox
hrcn_participant_profile	Other health insurance	text
hrcn_participant_profile	Health Insurance information (e.g., ID number, Medicaid MCO, etc.)	notes
hrcn_participant_profile	Permission to contact via:	checkbox
hrcn_participant_profile	Phone number(s)	notes
hrcn_participant_profile	Address and/or places we can find you	notes
hrcn_participant_profile	Alternate Contact(s)	notes
hrcn_participant_profile	Notes:	notes

hrcn_form_uploads	Form Type	dropdown
hrcn_form_uploads	Form description	text
hrcn_form_uploads	Upload File	file
hrcn_goals	Goal Label	text
hrcn_goals	Goal start date	text
hrcn_goals	Summary	notes
hrcn_goals	Resources	notes
hrcn_goals	Barriers	notes
hrcn_goals	action step #1	notes
hrcn_goals	action step #2	notes
hrcn_goals	action step #3	notes
hrcn_goals	action step #4	notes
hrcn_goals	action step #5	notes
hrcn_goals	Role/responsibility #1	notes
hrcn_goals	Role/responsibility #2	notes
hrcn_goals	Role/responsibility #3	notes
hrcn_goals	Role/responsibility #4	notes
hrcn_goals	Role/responsibility #5	notes
hrcn_goals	Action item goal completion date	text
hrcn_goals	Action item goal completion date	text
hrcn_goals	Action item goal completion date	text
hrcn_goals	Action item goal completion date	text
hrcn_goals	Action item goal completion date	text
hrcn_goals	Goal Notes	notes
hrcn_goals	Date goal completed	text
hrcn_encounter	Date	text
hrcn_encounter	Encounter Duration	dropdown
hrcn_encounter	Contact Method	radio
hrcn_encounter	Other Contact Method	text
hrcn_encounter	Where was encounter initiated?	radio
hrcn_encounter	Other encounter location	text
hrcn_encounter	Did you make contact with the client?	radio
hrcn_encounter	Encounter Type	checkbox
hrcn_encounter	Services directly provided by SSP staff or Care Navigator	checkbox
hrcn_encounter	Housing Services	checkbox
hrcn_encounter	Infectious disease	checkbox
hrcn_encounter	HCV Services	checkbox
hrcn_encounter	HCV Testing	checkbox
hrcn_encounter	HIV Services	checkbox
hrcn_encounter	HIV Testing	checkbox
hrcn_encounter	Other HIV Test	text
hrcn_encounter	Other STI	checkbox

hrcn_encounter	Chlamydia Services	checkbox
hrcn_encounter	Gonorrhea Services	checkbox
hrcn_encounter	Syphilis Services	checkbox
hrcn_encounter	Public Benefits	checkbox
hrcn_encounter	Substance Use Treatment	checkbox
hrcn_encounter	MOUD	checkbox
hrcn_encounter	Data	notes
hrcn_encounter	Assessment	notes
hrcn_encounter	Plan	notes
hrcn_referral	Referral date	text
hrcn_referral	External Referral Organization/Agency	text
hrcn_referral	Referral category	dropdown
hrcn_referral	Housing Services	checkbox
hrcn_referral	Infectious disease	checkbox
hrcn_referral	HCV Services	checkbox
hrcn_referral	HCV Testing	checkbox
hrcn_referral	HIV Services	checkbox
hrcn_referral	HIV Testing	checkbox
hrcn_referral	Other HIV Test	text
hrcn_referral	Other STI	checkbox
hrcn_referral	Chlamydia Services	checkbox
hrcn_referral	Gonorrhea Services	checkbox
hrcn_referral	Syphilis Services	checkbox
hrcn_referral	Public Benefits	checkbox
hrcn_referral	Substance Use Treatment	checkbox
hrcn_referral	MOUD	checkbox
hrcn_referral	Referral notes	notes
hrcn_referral	Linkage successful?	yesno
hrcn_referral	Linkage date	text
hrcn_referral	Linkage notes	notes
hrcn_test_results	Date	text
hrcn_test_results	Test Result Source	checkbox
hrcn_test_results	Test	radio
hrcn_test_results	Test other type	text
hrcn_test_results	Type of Test (eg, brand)	text
hrcn_test_results	Test Result	radio
hrcn_test_results	Notes	notes