

**INFORMATION SHARING AGREEMENT**  
**For**  
**CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)**  
**Between**  
**STATE OF WASHINGTON**  
**DEPARTMENT OF HEALTH**  
**And**

**Kittitas County Public Health Department**

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

**CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION**

	<b>INFORMATION RECIPIENT</b>	<b>INFORMATION PROVIDER</b>
<b>Organization Name</b>	Kittitas County Public Health Department	Washington State Department of Health (DOH)
<b>Business Contact Name</b>	Candi Blackford	Katrina Wynkoop Simmons
Title	Business contact	BRFSS Coordinator
Address	507 N. Nanum Street, Suite 102 Ellensburg, WA 98926	PO Box 47814, Olympia, WA 98504-7814
Telephone #	(509) 962-7515	360-236-4322
Email Address	<a href="mailto:candi.blackford@co.kittitas.wa.us">candi.blackford@co.kittitas.wa.us</a>	<a href="mailto:Katrina.Simmons@doh.wa.gov">Katrina.Simmons@doh.wa.gov</a>
Fax #	509.962.7581	360-753-4135
<b>IT Security Contact</b>	Duke Senter	Sharie McCafferty
Title	IT security contact	DOH IT Security Officer
Address	205 W 5 <sup>th</sup> Ave Ellensburg WA 98926	PO Box 49704
Telephone #	(509) 962-7510	360-236-4432 (office) 360-236-2290 (emergency)
Email Address	<a href="mailto:duke.senter@co.kittitas.wa.us">duke.senter@co.kittitas.wa.us</a>	<a href="mailto:sharie.mccafferty@doh.wa.gov">sharie.mccafferty@doh.wa.gov</a>
<b>Privacy Contact Name</b>	Candi Blackford	Kathy Stout
Title	Privacy contact	DOH Privacy Officer
Address	507 N. Nanum Street, Suite 102 Ellensburg, WA 98926	PO Box 49704
Telephone #	(509) 962-7515	360-236-4221
Email Address	<a href="mailto:candi.blackford@co.kittitas.wa.us">candi.blackford@co.kittitas.wa.us</a>	<a href="mailto:kathy.stout@doh.wa.gov">kathy.stout@doh.wa.gov</a>

## **DEFINITIONS:**

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.

Health Care Information means The state Health Care Information Act, RCW 70.02., states in pertinent part, “ ‘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)

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, regulations or contractual agreements. Violations may result in enhanced legal sanctions.

## **PURPOSE AND AUTHORITY/SCOPE OF AGREEMENT**

PURPOSE (include a description of how the data will be used and any provisions for re-disclosure)

Statement of purpose: Kittitas County Public Health Department will use BRFSS survey data only to examine health risk and protective factors, and other variables measured by the survey. These analyses will be used to inform policy and program development at the local level.

Re-disclosure: We will not disclose the data except as the law requires, the agreement permits, or with specific prior written permission by the Secretary of the Department of Health or designee.

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

STATUTORY AUTHORITY TO SHARE INFORMATION

DOH statutory authority to disclose the confidential information or limited Dataset(s) identified in this agreement to the Information Recipient:  
45 CFR, part 46, Protection of Human Subjects

Information Recipient's statutory authority to receive the confidential information or limited Dataset(s) identified in this Agreement: None stated

If the purpose is for research, has an Institutional Review Board (IRB) review and approval been received?

☐ Yes ☐ No ☒ Does not apply

PERIOD OF PERFORMANCE

This Agreement shall be effective from (1/13/2010) through (1/12/2012).

DESCRIPTION OF INFORMATION

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

Washington State Annual BRFSS data files from 2008 forward as released. See WA BRFSS Codebook 2008.doc (attached) for a list of data elements.

The information described in this section is:

- ☐ Restricted Confidential Information  
☐ Confidential Information  
☒ Potentially identifiable information

Any reference to information in this Agreement shall be the information as described in this Section.

## 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
- ☐ Other: (describe the methods for access/transfer)

Note: DOH IT Security Officer must approve "Other" prior to Agreement execution. IT 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 \_\_\_\_\_ (date)
- ☒ Repetitive: frequency or dates: Annually, as files are released
- ☐ As available within the period of performance stated in Section III.D.

### OTHER PROVISIONS

None.

## USE OF INFORMATION

The Information Recipient agrees to strictly limit use of information obtained or created under this Agreement to the purposes stated in the 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.

## SAFEGUARDING INFORMATION

### CONFIDENTIALITY

Information Recipient agrees to:

- limit access and use of the information:
  - To the minimum amount of information
  - The fewest people
  - For the least amount of time required to do the work.
- Assure that all people with access to the information understand their responsibilities regarding it.



- Assure 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.

#### SECURITY

The Information Recipient assures that its security practices and safeguards meet Washington State Information Services Board (ISB) IT Security Standards:  
<http://isb.wa.gov/policies/security.aspx>.

- For the purposes of this Agreement, compliance with the HIPAA Security Standards meets the ISB IT Security Standards.

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.

The Information Recipient agrees to notify the DOH IT Security Officer within two (2) business days of any suspected or actual confidentiality or security breach.

Note: The DOH IT 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.

#### BREACH NOTIFICATION

The Information Recipient shall notify the DOH IT Security Officer within two (2) business days of any suspected or actual breach of security or confidentiality of information covered by the Agreement.

#### **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 of the Information Recipient received the request
  - DOH records the Information Recipient believes are responsive to the request and the
  - Identity of the requestor, if known.

### 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. Other citation:

Washington State Department of Health, Center for health Statistics, Behavioral Risk Factor Surveillance System, supported in part by Centers for Disease Control and Prevention Cooperative Agreement number \_\_\_\_\_ (year)<sup>1</sup>

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

### 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.

### 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

<sup>1</sup> See Appendix D for a list of Cooperative Agreement numbers and years.

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 amended, 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):

#### **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

#### **CAUSE FOR IMMEDIATE TERMINATION**

The Information Recipient acknowledges that unauthorized use or disclosure of the Information or any other violation of section VI may result in the immediate termination of this Agreement.

#### **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.

### **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.

### **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 contract work. 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.

### **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.

### **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.

### **LIMITATION OF AUTHORITY**

Only the Authorized Signator for (DOH) (delegation to be made prior to action) 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 Signator for DOH.

### **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.

### **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 research papers, reports, presentations or publications, URLs of web publications
- to the attention of:  
Katrina Wynkoop Simmons, BRFSS Coordinator

Center for Health Statistics, 101 Israel Rd SE, Tumwater, WA 98501

or

Center for Health Statistics, PO Box 47814, Olympia, WA 98504-7814

### **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.

### **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.

### **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.

### **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.

### **ALL WRITINGS CONTAINED HEREIN**

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

IN WITNESS WHEREOF, the parties have executed this Agreement.

**INFORMATION PROVIDER**

Christie Spice, State Registrar and Director  
Center for Health Statistics  
State of Washington Department of Health


  
Signature

  
Date

**INFORMATION RECIPIENT**

Candi Blackford, Business and privacy contact  
Kittitas County Public Health Dept

  
Signature

  
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 in section III of 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 section III of the Agreement, and 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)**

F. **SIGNATURE**

Name: Amy Diaz  
(Print or Type)

Signature: Amy Diaz Date: 3/1/10

[Make additional copies for other staff who will have contact with identified or potentially identified data.]



## APPENDIX B

### DATA SECURITY REQUIREMENTS

#### **Protection of Data**

The Information Recipient agrees to store data on one or more of the following media and protect the data as described:

##### **A. Hard disk drives**

Data stored on local workstation hard disks: The data must be encrypted as described under F. data storage on portable devices or media. Access to the data will be 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 require administrator reset.

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
- Are changed at least every 120 days.

##### **B. Network server disks**

Data stored on hard disks mounted on network servers and made available through shared folders:

1. Access to the data will be 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.
  - a. 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 require administrator reset.
2. Data on disks mounted on such servers must be located in a secured computer area, which is accessible only to authorized personnel with access controlled through use of a key, card key, combination lock, or comparable mechanism.
3. If the servers are not located in a secured computer area or if the data is classified as Confidential or Restricted Confidential, it must be encrypted as described under F. data storage on portable devices or media.

**C. Optical discs (CDs or DVDs) in local workstation optical disc drives**

Data provided on optical discs must be encrypted as described under F. data storage on portable devices or media. 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.

**D. Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**

Data provided on optical discs must be encrypted as described under F. data storage on portable devices or media.

1. Access to data on these discs will be 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 require administrator reset.
3. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

**E. Access via remote terminal/workstation over the State Governmental Network (SGN) or the Internet**

1. When data is transferred between the Information Provider and the Information Recipient, access to the data will be controlled by the Information Provider, who will issue authentication credentials. Information Recipient will notify the Information Provider immediately whenever:
  - An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Information Recipient
  - Whenever a person's duties change such that the person no longer requires access to perform work for this agreement.
2. The data shall 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. If so authorized secure encryption protocols and multi-factor authentication mechanisms such as; hardware or software tokens, smart cards, digital certificates and biometrics, must be used. During transmission the data must be encrypted 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.

**F. Data storage on portable devices or media**

1. Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.

2. Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).
3. The data shall not be stored by the Information Recipient on portable devices or media unless specifically authorized within the terms of this Agreement. If so authorized, the data shall be given the following protections:
  - Use industry standard encryption mechanisms validated by the National Institute of Standards and Technologies (NIST).
  - Encrypt the data with a key length of at least 128 bits
  - Control access to devices with a unique user ID and Complex Password or stronger authentication method such as a physical token or biometrics. Whenever technically possible accounts must lock after 5 unsuccessful access attempts and require administrator reset.
  - Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 10 minutes.
  - Physically protect the portable device(s) and/or media by
    - Keeping them in locked storage when not in use
    - Using check-in/check-out procedures when they are shared, and
    - Taking frequent inventories

When being transported outside of a secure area, portable devices and media with data provided under this agreement must be under the physical control of Information Recipient staff with authorization to access the data.

#### **G. Backup Media**

Data may be backed up as part of Information Recipient's normal backup process provided that it is encrypted and the process includes secure storage and transport.

#### **H. Paper documents**

Any paper records must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

#### **Data Segregation**

1. Data provided under this agreement 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 data, which it is commingled with the data provided under this agreement, must be protected as described in this exhibit

### **I. Data Disposition**

If data destruction is required by the Agreement, the data shall be destroyed using one or more of the following methods:

<b>Data stored on:</b>	<b>Will be destroyed by:</b>
Server or workstation hard disks	<p>Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, or</p> <p>Degaussing sufficiently to ensure that the data cannot be reconstructed, or</p> <p>Physically destroying the disk , or</p> <p>Delete the data and physically and logically secure data storage systems that continue to be used for the storage of confidential data to prevent any future access to stored information. One or more of the preceding methods must be performed before transfer or surplus of the systems or media containing the data.</p>
Paper documents with confidential data	<p>On-site shredding, pulping, or incineration, or</p> <p>Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of data will be protected.</p>
Paper documents containing confidential information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
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

**J. Notification of Compromise or Potential Compromise**

The compromise or potential compromise of the data must be reported to the DOH IT Security Officer within two (2) business days of discovery.

# 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 # BRFSS-2-024, Section C, item B, Disposition of Information, have been fulfilled as indicated above.

### SIGNATURE

Name: \_\_\_\_\_  
(Print or Type)

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

## Appendix D

**CDC Cooperative Agreement Numbers****CDC Cooperative Agreement Numbers for  
Questionnaire Years 1987-2003**U58/CCU002118-*number (year)*

Cooperative Agreement Number	Questionnaire Year
1	1987
2	1988
3	1989
4	1990
5	1991
6	1992
7	1993
8	1994
9	1995
10	1996
11	1997
12	1998
13	1999
14	2000
15	2001
16	2002
17	2003

**CDC Cooperative Agreement Numbers for  
Questionnaire Years 2004- 2008**U58/CCU022819-*number (year)*

Cooperative Agreement Number	Questionnaire Year
1	2004
2	2005
3	2006
4	2007
5	2008

**CDC Cooperative Agreement Numbers for  
Questionnaire Years 2009- 2013**U58/DP001996-*number (year)*

Cooperative Agreement Number	Questionnaire Year
1	2009
2	2010
3	2011
4	2012
5	2013

Kittitas County  
Review Form  
Grants & Contract Agreement



Today's Date 03/03/10	Agenda Date
Fund/Department 116 Public Health Department	

**Contract/Grant Information**

Contract /Grant Agency: Information Sharing Agreement for Confidential Information or Limited Dataset between the State Of Washington Department of Health and Kittitas County Public Health Department	
Period Begin Date: Upon Signature	Period End Date: N/A
Total Grant/Contract Amount: N/A	
Grant/Contract Number:	
Contract/Grant Summary: The purpose of this agreement documents the conditions under which the Washington State Department of Health shares confidential information or limited Dataset with other entities.	

**Recommendation for Board of Health and Board of Health Review on \_\_\_\_\_**

Department Head Signature: <u><i>Ashley Bambuck</i></u> Administrator	Date: <u>3/4/10</u>
---	---------------------

**Kittitas County Prosecutor, Auditor, and Board of Health Review and Comment:**

APPROVED AS TO FORM:

<u><i>[Signature]</i></u> Signature of Prosecutor's Office	<u>4/23/10</u> Date
<u><i>Dawn Mohn</i></u> Signature of Auditor's Office	<u>4/29/10</u> Date
<u><i>[Signature]</i></u> Signature of Board of Health member	<u>5-20-10</u> Date

**Financial Information**

Total Amount \$N/A	State Funds \$	Federal Funds \$
Percentage County Funds	Matching Funds \$	CFDA#
	In-Kind \$ Explain	



Is Equipment being purchased?	Who owns equipment?
New Personnel being hired?	Contact HR hiring – reporting requirements
Future impacts or liability to Kittitas County:	

### Budget Information

Budget Amendment Needed?	Yes <input type="checkbox"/> attach budget form	No <input type="checkbox"/> Why not
New Division Created?		
Revenue Code		

### Pass Through Information

Agency to Pass Through	
Amount to Pass Through	\$
Sub-Contract Approved	Date:

### Prosecutor Review

Has the Prosecutor reviewed this agreement?	Yes <input type="checkbox"/> No <input type="checkbox"/>
---	--

### County Departments Impacted

Auditor	Facilities Maintenance
Information Services	Human Resource
Prosecutor	Treasurer

### Submitted

Signature:	Date:
Department: Public Health	

### Assignment of Tracking Information

Auditor's Office	
Human Resource	
Prosecutor's Office	
Who Signed the grant application	

Reviewer	Date
----------	------