North American Association of Central Cancer Registries
Agreement for Administering the Central Cancer Registry
Inter-Registry Resident Data Exchange
DOH DSA #: N21389

This Agreement establishes the terms and conditions for the exchange of resident cancer case information between participating member registries ("Trading Partners," collectively) of the North American Association of Central Cancer Registries ("NAACCR"). This Agreement will be executed in counterparts by each Trading Partner, with each such signed Agreement deemed to be an original, and all such counterparts together shall constitute one and the same instrument. The executed counterparts of the Agreement shall be maintained by NAACCR, but NAACCR is not a party to the Agreement.

Each Trading Partner agrees to specify in detail any additional permissions and/or restrictions affecting the use, release and re-release of its information by other Trading Partners. These specifications will be included in the Addendum, hereby incorporated into this Agreement. Each Trading Partner agrees to update and keep current all information in the Addendum by informing NAACCR in writing of any changes to law statute, regulation or policy that impact this Agreement and expressly authorizes NAACCR to provide a copy of the Trading Partner's executed counterpart (and any Addendum thereto), as may be revised or modified, to any other Trading Partner at any time.

Each Trading Partner may rescind or modify its participation in this Agreement by sending a written notice of rescission or a copy of revisions to NAACCR. Each Trading Partner acknowledges that it is its responsibility to provide written notification to NAACCR of any rescission or modification of its participation in this Agreement, including any revision of the Trading Partner's Addendum or this Agreement.

By signing this Agreement, the central cancer registry listed below agrees to become a Trading Partner in the exchange of cancer incidence data, acting as the Sending Registry and/or the Receiving Registry with regard to resident cancer data for all other Trading Partners and hereby agrees that:

1. The Sending Registry will provide all cancer registry records and information concerning diagnosis and treatment of cancer occurring in non-residents and contained in the Sending Registry to the Receiving Registry where the reported cancer cases reside, except information specifically exempt from release by the Sending Registry in accordance with the restrictions in the Addendum.
2. Information will be provided electronically, whenever practical. The latest data core edits will be run on the data by the Sending Registry, and the data shall be formatted to follow the most current NAACCR data exchange record layout, shall contain sufficient information to be used for statistical and administrative purposes, and shall be transmitted through a mutually agreed-upon secure method that ensures against inappropriate access to the information.
3. All transmittals of cancer registry records are to be made following a timetable mutually agreed upon by Trading Partners. To ensure optimum utilization of the records, Trading Partners shall make every reasonable effort to forward all cancer case reports within eighteen (18) months of the end of the diagnosis year.
4. The information exchanged under this Agreement may only be used by the Receiving Registry for purposes authorized in Paragraph 7 of this Agreement or any other purposes authorized in writing by the Sending Registry. The Receiving Registry agrees to use records containing identifiable information exchanged under this Agreement in full compliance with the terms and conditions of this Agreement and any specific conditions required by the Sending Registry in the Addendum. Identifiable information exchanged under this Agreement may not be re-released by the Receiving Registry without written permission of the Sending Registry.

   For the purpose of this Agreement, identifiable information shall be defined as in the HIPAA Privacy Rule (45 CFR 164.514).
5. Any and all data that may lead to the identification of any patient is strictly privileged and confidential, and the Receiving Registry agrees to keep all such data strictly confidential.
6. A Receiving Registry shall maintain the confidentiality of the exchanged patient identifying data and has legal protections in place under state and/or federal law to be able to protect the data from release in any manner contrary to the terms of this Agreement. Such confidentiality shall be maintained notwithstanding termination of this Agreement.

7. The cancer incidence data provided under this Agreement may be used for the following purposes and as specified by the Sending Registry for:

   a. Aggregated statistical tabulations and analyses;

   b. Linking with appropriate databases *{e.g., death certificates, hospital discharge databases, Indian Health Service, National Death Index}* as necessary for cancer registry activities intended to acquire or enhance cancer case information;

   c. Research conducted by the Receiving Registry that has been approved by the Receiving Registry's Institutional Review Board, unless otherwise specified in the Addendum; All other research, including re-release of records, requires written permission of the Sending Registry;

   d. Sharing of partially de-identified information with local and/or national public health agencies, including NAACCR and the CDC/NPCR Coordinated Call for Data, and the National Cancer Institute's Surveillance, Epidemiology, End Results (NCI/SEER) Call for Data, and for the support of public health programs, with an agreement that provides appropriate restrictions on the use and release of the shared information;

   e. Conducting linkages with and providing case information to the Breast and Cervical Cancer Control Program and Colorectal Cancer Control Program under the terms of a written Memorandum of Understanding or other means that provides for the appropriate restrictions on the use and release of the shared information;

   f. Sharing records with State Health Departments for surveillance or community health assessment activities; and

   g. Sharing of case data with other central registry entities in the Receiving Registry's state.

8. The Receiving Registry will restrict access to cancer incidence data or identifiable information on a cancer patient that was supplied by a Sending Registry under the terms of this Agreement from being released to anyone not employed in the direct operation of the Receiving Registry, except as specifically authorized within the terms of this Agreement. Employees may include those involved in the processing, administration, quality control review, and statistical surveillance of cancer incidence data.

9. All officers, agents and employees shall keep all such data strictly confidential; and that the Receiving Registry shall communicate the requirements of this Agreement to all officers, agents, and employees, shall discipline all persons who may violate the requirements of this Agreement, and shall notify the Sending Registry in writing within two working days (48 hours) of any violation of this Agreement, including full details of the violation and corrective actions to be taken.

10. The Receiving Registry will notify the Sending Registry if, in the conduct of approved research or other activities involving the Sending Registry's data, there is a breach or misuse of a cancer patient's identifying information or potentially identifying information. Should a breach or misuse take place, the Receiving Registry must notify the Sending Registry in writing within forty-eight (48) hours of the release of the data, and shall take all feasible measures to mitigate loss or damages related to such breach or misuse, including, but not limited to, bearing sole responsibility for reasonable costs, including attorneys' fees, related to mitigating the breach or misuse.

11. Any other use or release of information from records provided to the Receiving Registry that is not authorized by the terms of this Agreement requires the written permission of the Sending Registry.

12. In the event that the Receiving Registry receives a subpoena or other compulsory legal process compelling disclosure of confidential data, the Receiving Registry agrees to notify the Sending Registry within forty-eight (48) hours of receipt of the subpoena or other compulsory legal process. Additionally, should the Receiving Registry receive such a subpoena or other compulsory legal process, it shall take all legal steps reasonably necessary to oppose the subpoena or other compulsory legal process.

13. This Agreement shall remain in effect as to any Trading Partner from the date of its execution until a duly authorized representative of that Trading Partner notifies the other Trading Partners of a change or termination of this Agreement through written notification to NAACCR.

14. All notices required or desired to be made to this Agreement by any Trading Partner shall be sent to NAACCR as well as to any Receiving Registry of the Trading Partner.

Trading Partner
Central Cancer Registry: Washington State Cancer Registry

Agency: Washington State Department of Health

Michael Maverick
Michael Maverick
DOH FS CPO, Director 7/7/15

Signature *Title* *Date*

CONTACT PERSON:

Name: Riley Peters
Title: Surveillance and Evaluation Section Manager
Address: 310 Israel Road SE, Tumwater, WA 98501
Email: Riley.Peters@doh.wa.gov
Phone: 360.236.3581 Fax: 360.586.2714

CONTACT PERSON FOR ELECTRONIC EXCHANGE:

Name: Danielle Good
Title: Abstractor
Address: 310 Israel Road SE, Tumwater, WA 98501
Email: Danielle.good@doh.wa.gov
Phone: 360.236.3616 Fax: 360.586.2714

MAIL RECORDS TO:

Name: Danielle Good
Title: Abstractor
Address: 310 Israel Road SE, Tumwater, WA 98501
Email: Danielle.good@doh.wa.gov
Phone: 360.236.3616 Fax: 360.586.2714

Addendum to Trading Partner Agreement of Washington State Cancer Registry

Additional permissions and restrictions on the use of cancer registry information from this Trading Partner.

Please copy and paste the following URL to view the Washington State Cancer Registry's full addendum: (insert URL)

The participation of the Washington State Cancer Registry (WSCR) in this NAACCR Agreement is subject to Revised Code of Washington (RCW) 70.54.230, .240, .250, .260, and .70 (http://apps.leg.wa.gov/rcw/default.aspx?cite=70.54.230) and Chapter 246-10 Washington Administrative Code (WAC) (http://apps.leg.wa.gov/wac/default.aspx?cite=246-102).

Specific additional permissions and restrictions on the use of cancer registry information originating with WSCR include, but are not limited to, the following modifications of the NAACCR agreement:

Paragraph 1: As a Sending Registry, WSCR has authority to send only cancer case information, as that term is defined by WAC 246-102-010, for cases with an address at the time of diagnosis outside the borders of Washington State as required by WAC 246-102-070.

Paragraph 2: Information shall be provided electronically. The Receiving Registry shall assure that its data security practices and safeguards meet or exceed the Washington State Office of the Chief Information Officer (OCIO) IT Security Standards: http://ofm.wa.gov/ocio/policies/documents/141.10.pdf. Compliance with OCIO IT Standards includes:

1. Compliance with Federal Information Security Acts (FISMA) security standards and guidelines for High impact systems, http://csrc.nist.gov/groups/SMA/fisma/compliance.html, and
2. Compliance with "Data Security Requirements" attached below. Questions concerning the Data Security Requirements should be addressed to the Washington Department of Health Information Security Officer identified in the modification to Paragraph 9.

Paragraph 7c: The Receiving Party shall not use or release data originating with WSCR for research without first complying with the requirements of WAC 246-102-070. Under WAC 246-102-070, data originating with WSCR may not be used for research unless the research project has been reviewed and approved by the Washington state institutional review board and written confidentiality agreement between WSCR and the researcher is in place.

Paragraph 9: A compromise or potential compromise of data must be reported to within two (2) business days to:

Washington Department of Health
Information Security Officer (Sharie McCafferty)
ITSO.DIRM@doh.wa.gov

PO Box 47904
101 Israel Rd SE
Olympia, WA 98504-7904

Phone: 360-236-4432

Fax: 360-236-4421

DATA SECURITY REQUIREMENTS

Information received from WSCR (Sending Registry) under this agreement is classified as "Restricted Confidential".

The Receiving Registry agrees to store the information received under this agreement on one or more of the following media and protect it as described:

A. **Hard disk drives -** Information stored on local workstation hard disks:
   1. The information must be encrypted as described under F. Storage on portable devices or media. Access to the information 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 either administrator reset or after a minimum of 15 minutes the account may reset automatically.
   2. Complex Passwords are:
      - At least 8 characters in length
      - Contain at least three of the following four 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 - Information stored on hard disks mounted on network servers and made available through shared folders:
   1. The information must be encrypted at rest as described under F. Storage on portable devices or media.
   2. Access to the information 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 either administrator reset or after a minimum of 15 minutes the account may reset automatically.
   3. Hard disks mounted on such servers must be located in a secured computer area, which is accessible only by authorized personnel through the use of a suitable locking mechanism.

C. Optical discs (CDs or DVDs) used in local workstation optical disc drives -
   1. Optical discs containing the information must be encrypted as described under F. Storage on portable devices or 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.

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

1. Optical discs containing the information must be encrypted as described under F. Storage on portable devices or media.
2. Logical access 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.
3. 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 either administrator reset or after a minimum of 15 minutes the account may reset automatically.
4. When in use optical discs must be located a secured computer area which is accessible only by authorized personnel through the use of a suitable locking mechanism.
5. 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 via remote terminal/workstation over the State Governmental Network (SGN) or the Internet

1. When the information is transferred between the Washington State Cancer Registry Sending Registry and the Receiving Registry, access will be controlled by the Sending Registry, who will issue authentication credentials. Receiving Registry will notify the Sending Registry immediately whenever:
   b. An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Receiving Registry
   c. Whenever a person's duties change such that the person no longer requires access to perform work for this agreement.
   a. The information shall not be transferred or accessed over the Internet by the Receiving Registry in any other manner.

F. Storage on portable devices or media

1. Examples of portable devices include: cellular devices such as smart phones and tablets, laptop/notebook computers. ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), and portable hard disks.
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 information shall not be stored by the Receiving Registry on portable devices or media unless specifically authorized within the terms of this Agreement. If so authorized, the information shall be given the following protections:
   a. Use industry standard encryption mechanisms validated by the National Institute of Standards and Technologies (NIST).
   b. Encrypt the information with a key length of at least 128 bits

c. 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.

d. Manually lock devices whenever they are left unattended and when possible set devices to lock automatically after a period of inactivity. Maximum period of inactivity is 10 minutes.

e. 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

4. When being transported outside of a secure area, portable devices and media containing the information must be under the physical control of explicitly authorized Receiving Registry staff.

G. Backup Media

The information may be backed up as part of Receiving Registry'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.

I. Information Segregation

Information provided under this agreement must be distinguishable from all other data. This is to ensure that information received from the Washington State Cancer Registry (WSCR) is easily identified. It also aids in determining whether the information has or may have been compromised in the event of a security breach.

J. Information Disposition

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

Information stored on:	**Will be destroyed by:**
Server or workstation hard disks	Using a "wipe" utility which will overwrite the information at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the information cannot be reconstructed, or Physically destroying the disk , or Delete the information and physically and logically secure data storage systems that continue to be used for the

	storage of confidential information 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 information.
Paper documents with confidential information	On-site shredding, pulping, or incineration, or Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of the information will be protected.
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 information at least three (3) times using either random or single character data Physically destroying the disk Degaussing magnetic media sufficiently to ensure that the information cannot be reconstructed