DRAFT

TRIBAL DATA SHARING AGREEMENT (TDSA)

BETWEEN

STATE OF WASHINGTON

DEPARTMENT OF HEALTH

AND

[TRIBE]

Approved via Tribal Consultation: [DATE]

CONTACT INFORMATION FOR PARTIES TO AGREEMENT:
Whoever is holding Title will receive contact even if the person in role the changes.

[TRIBE]	WASHINGTON STATE DEPARTMENT OF HEALTH
Organization Name:	Organization Name:
Designated DSA Contact:	Business Contact Name:
Title:	Title:
Address:	Address:
Telephone #:	Telephone #:
Email Address:	Email Address:
Designated Contact for IT Security:	IT Security Contact:
Title:	Title:
Address:	Address:
Telephone #:	Telephone #:
Email Address:	Email Address:
Designated Contact for Information Privacy:	Privacy Contact Name:
Title:	Title:
Address:	Address:
Telephone #:	Telephone #:
Email Address:	Email Address:

This Data Sharing Agreement ("Agreement" or DSA) is made and entered into by the Washington State Department of Health (DOH) and [TRIBE].

1. PURPOSE

This Agreement establishes the terms and conditions under which:

a. the [NAME OF TRIBAL JURISDICTION] and Washington State Department of Health (DOH) collect, manage, use, disclose, and safeguard Tribal ~~and American Indian and Alaska Native information and~~ data; and

b. DOH shares confidential information or limited dataset(s) from the data and information referenced in Section 5 with the [NAME OF TRIBAL JURISDICTION].

This agreement shall not limit the [TRIBE] ownership of data and information under their authority as sovereign nations.

DOH is committed to government-to-government relations with Tribes and honoring Tribal data sovereignty. DOH is committed to upholding Tribal data sovereignty principles in how it approaches the collection and sharing of Tribal data. DOH recognizes that historically, Tribes have been excluded from access, control and ownership over their data that the state collects and are dependent on DOH (and others) for this data. This DSA is a step toward this commitment.

DOH's commitment to uphold Tribal data sovereignty principles will continue to be reflected in DOH's strategic planning as DOH modernizes and invests in its data and systems. DOH commits to continuing to work with Tribes across the state to expand on our shared Tribal data sovereignty principles as expeditiously as possible.

Tribal data sovereignty asserts the rights of Tribal Nations to govern the collection, ownership, and application of their own data, this derives from tribes' inherent right to govern their peoples, lands, and resources.

Additionally, the purpose of this DSA is to identify, describe, and protect the data that will be shared between the parties in alignment with the Washington State Agency Privacy Principles.

2. DEFINITIONS

Analysis means the process of systematically collecting, cleaning, transforming, describing, modeling, and interpreting data into usable information for a specific aim or purpose.

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 and who have signed the Use and Disclosure of Confidential Information form set forth in Appendix A.

Breach of confidentiality means unauthorized access, use or disclosure of information received under this Agreement. Disclosure may be oral or written, in any form or medium.

Breach of security means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal

Commented [MC1]: This template is designed to be between DOH and a Tribe, so it does not govern DOH's data use of population level AI/AN data.

Commented [KP2]: GIHAC Purpose Section One

Commented [KP3]: Principle One: Inherent Authority to Manage Data

information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

Business Day means state business hours Monday through Friday from 8:00 a.m. to 5:00 p.m. except state holidays.

"CDC" means the United States Centers for Disease Control and Prevention.

Confidential information means data or information that is protected from public disclosure by law.

Data means a subset of Information. A representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

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 data and/or information across a network from a sender (or source), to one or more destinations.

Direct identifier means an attribute that alone enables unique identification of an individual within a specific operational context.

Disclosure means to permit access to or release, transfer, or other communication of confidential data or 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 data or information shared, encryption may be required during data transmissions, and/or data storage.

Health care information means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care.

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

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

Human research review is the process used by institutions that conduct human subjects research to ensure that: the rights and welfare of human subjects are adequately protected; the risk to human subjects are minimized, are not unreasonable, and are outweighed by the potential benefits to them or by the knowledge gained; and the proposed study design and methods are adequate and appropriate in light of the stated research objectives. Research that involves human subjects or their identifiable personal records should be

reviewed and approved by an institutional review board (IRB) per requirements in federal and state laws and regulations and state agency policies.

Human subject means a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data or information through intervention or interaction with the individual, or (2) identifiable private information.

Identifiable data or records contains information that reveals or can likely be associated with the identity of the person or persons to whom the data or records pertain. Research data or records with direct identifiers removed, but which retain indirect identifiers, are still considered identifiable.

Indirect identifier means variables that may be used together or in conjunction with other information to create Identifiable data or records about an individual.

Information means data that is processed, organized and structured, often presented with an interpretation of their meaning. This includes concepts and constructs.

Limited dataset means a data file that includes potentially identifiable information. A limited dataset does not contain direct identifiers.

Linked data means combining data from different sources that relate to the same person to create a new, enhanced data resource. Matching may be done using computer algorithms or manual review.

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.

Publishing means to distribute or make available a work product to the public in a physical or electronic form.

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Research and other public health activities may be subject to Tribal Research Review based on the determination of the Tribe.

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.

Third Party means any person or entity (this includes, but is not limited to, other state agencies) who is not a signatory to this Agreement. Tribal Epidemiology Centers are exempt from the definition of Third Party unless otherwise specified by a Tribe.

Commented [KP4]: GIHAC vote/decision placeholder – where/how to include?

Tribal Data means data or information that is specific to an individual Tribe and includes public or private data or information on or about a Tribe or its people subject to Tribal rights of ownership and control. Tribal data also includes, but is not limited to, Tribe of membership, Tribe of affiliation, events and conditions within the Tribe's jurisdiction and lands, information about Tribal members and any persons living within

the Tribe's jurisdiction, Tribal census tract, Tribal land, and identification of Tribal facilities, entities, and enterprises and any individuals they serve.

Commented [KP5]: GIHAC definitions

Tribal Data Sovereignty. Tribal Data Sovereignty means the inherent legal authority of Tribes to:

Commented [KP6]: GIHAC definitions

- Manage the collection, ownership, application and interpretation of Tribal data or information even if it is collected by federal, state, or local governments and/or other third parties regardless of where data is collected;
- Have the right to informed consent on how their data, including, but not limited to, protected health information about their Tribal members, are used or shared with third parties;
- Have the same or additional access to state data as other public health jurisdictions in order to carry out their governmental duties; and
- Be notified by other entities holding Tribal data of data breaches and be informed of any policies regarding data disposition, security, confidentiality, storage, and human subjects research limitations.

Tribal Research Review means an entity selected by a Tribe that reviews research to protect the interests of Tribal members and the Tribal community, like a Tribal Institutional Review Board. Tribes have the authority to determine when research is occurring which may follow federal definitions, state definitions, and/or include public health practice.

Tribe or Tribal as defined under Section 4 of the Indian Health Care Improvement Act (codified at 25 U.S.C 1603(14) and RCW 43.71B.010(18), means any Indian Tribe, Band, Nation, or other organized group or community, including any Alaska Native village or group or regional or village corporation as defined in or established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. Sec. 1601 et seq.) which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

Washington State Institutional Review Board means the institutional review board designated by the Department to review research proposals pursuant to chapter 42.48 RCW and the federal common rule, 45 C.F.R. Part 46. The Washington State IRB must review and approve all research involving human subjects in the jurisdiction of the State Agencies subject to chapter 42.48 RCW.

3. RECOGNITION OF TRIBES AS TRIBAL HEALTH JURISDICTIONS AND PUBLIC HEALTH AUTHORITIES

A. Tribes are Public Health Authorities. In implementing this Agreement, DOH shall, in accordance with the law, honor and treat Tribes as public health authorities as recognized under 45 CFR § 164.501 and WAC 246-101-010(38).

B. Tribes are Public Health Jurisdictions. In implementing this Agreement, DOH shall, in accordance with the law, honor and treat Tribes as public health jurisdiction with all the public health powers that exceed those of non-governmental public health authorities.

Commented [KP7]: Section 4: Tribes as PH Jurisdictions and PHA

4. OWNERSHIP OF DATA

Commented [KP8]: Principle 2: Ownership of and Authority Over Tribal Data

Data ownership remains with and is not transferred to those authorized to receive and use the data and information subject to the following conditions:

a. Unless otherwise required by law, the [TRIBE] and DOH shall have joint ownership in data and information in DOH data systems regarding [TRIBE], its Tribal citizens, and persons who reside within the [TRIBE] jurisdiction, under this Agreement;
b. Unless otherwise required by law, this Agreement shall not limit the [TRIBE]'s ownership of data and information under their authority as sovereign nations; and
c. This Agreement shall not transfer data ownership to third parties.

5. INFORMED CONSENT AND PROTECTION OF [TRIBE]'s DATA AND INFORMATION

Subject to any limitations provided in subsection 5(E), this section provides the conditions under which DOH collects, manages, uses, discloses, and safeguards [TRIBE]'s information and data. Tribes have the right to informed consent on how their data, including protected health information about Tribal members, are used or shared with Third Parties.

This section will be implemented according to the terms identified in a DSA implementation plan

A. **Protection of [TRIBE]'s Data and Information.** For purposes of this section, [TRIBE]'s data will be identified as [PROXY] , until a more representative proxy is identified by mutual agreement of DOH and [TRIBE], which could include consultation with other relevant partners. DOH must obtain permission using the Tribal Nation Data Use Form (Appendix E) from the [TRIBE], to be completed by [contact], under the following conditions:
    1. Publishing and Reports: Prior to DOH publishing data/information that DOH knows or has reason to know are the [TRIBE] data or information in a manner that allows those data to be identified as the [TRIBE]'s data or information. This includes, but is not limited to, republishing data or information that is made available through public sources including social media, research publications, and/or online documents;
        a. Data Sharing: Prior to sharing data/information that DOH knows or has reason to know are [TRIBE]'s data/information in a manner that allows those data/information to be identified as [TRIBE]'s data with a Third Party and/or release of data/information from the [TRIBE], except for individual clinical care. This includes, but is not limited to, sharing data/information with third parties conducting research and analysis, and resharing information that is made available through public sources including social media, research publications, and/or online documents. DOH may also share data with a Third Party when [TRIBE] shares that a release of information (ROI) or data sharing agreement exists between [TRIBE] and the Third Party;
    2. Research: Prior to researching [TRIBE]'s' data/information in a manner that includes [TRIBE] membership or association or can uniquely identify [TRIBE]. [TRIBE] may also request prior review by a Tribal Research Review; and
    3. Analysis: Prior to analyzing [TRIBE]'s data/information in a manner that includes [TRIBE]'s membership or association or can uniquely identify the [TRIBE].

Commented [KP9]: GIHAC Section 5: Ownership of Data (added legal requirements) and reflected in Sect 5(A).2

Commented [KP10]: GIHAC Section 6, 1 & 2: Informed Consent/Protection and Sect 15

Commented [KP11]: Principle 3.3: Informed Consent

Commented [MC12]: During the roundtable and consultation process this language was identified as being superfluous.

Commented [KP13]: Principles 5 and 6: Equal Partners in Data Projects and Consulting with Tribes on Use of their Data

Commented [KP14]: Flag this template language - AI/AN data for a specific Tribe needs to be defined when entering the DSA

Commented [KP15]: GIHAC Principle 8: Tribal Data Sovereignty

Commented [KP16]: GIHAC Section 6.3

Commented [KP17]: Section 6.13

Commented [KP18]: This is the mechanism for GIHAC sec 5.8

4. Upon a request of [TRIBE] made in writing to DOH Business Contact or their designee, that [TRIBE] data, provided by DOH to a Third Party, is being used in a manner that violates Tribal Data Sovereignty principles.

B. Updating New and Existing DSA Agreements. DOH will update all data sharing agreements where DOH shares data externally with third parties that apply or could reasonably be assumed to apply to [TRIBE]'s data to add an addendum that includes Tribal Data Sovereignty principles, which are mutually agreed upon by [TRIBE] and DOH, at creation of new DSAs, upon renewal of agreements, or no later than five years after signing of the DSA.

C. Timelines for Submitting Tribal Nation Data Use Form. The [TRIBE] will respond no later than 30 days after receipt of the Tribal Nation Data Use Form. If [TRIBE] does not respond within 30 days of receiving DOH's request, the DOH request will be deemed approved. DOH can request approval prior to 30 days by providing justification for an expedited process. DOH shall include in the Tribal Nation Data Use Form the date a response is needed from [TRIBE] linked to any deadlines. If [TRIBE] does not respond by the deadline requested by DOH, the DOH request will be deemed approved.

D. Prohibited Collection of Data. Unless otherwise stated in this agreement, or unless agreed to by the [TRIBE] in the Tribal Nation Data Use Form (Appendix X), DOH will not intentionally collect [TRIBE] membership, [TRIBE] affiliation, or [TRIBE] Census Tract identification in any DOH database.

E. Notification and Exceptions. This section provides exceptions for when DOH shall not be required to seek prior express written permission under Section 5 or be prohibited from sharing information under Section 5(D). Unless otherwise stated, DOH shall still be required to provide notification to the [TRIBE] utilizing the Tribal Nation Data Use Form (Appendix E) as soon as DOH has reason to know whether the data or information involves [TRIBE] data or information. The exceptions include the following:

1. A request under the Public Records Act (RCW 42.56.520).
2. A Washington state or federal statute or regulation prohibits or limits DOH compliance with Section 5;
3. Compulsory legal process, court order, a settlement, or a consent decree which prohibits or limits DOH compliance with Section 5;
4. A contract, cooperative agreement, or grant agreement that predates this agreement prohibits or limits DOH compliance with Section 5. This subsection is subject to Subsection 5B;
5. Sharing with a state agency, federal agency, local health jurisdiction, or Tribe when DOH receives notification that a Tribal citizen or American Indian or Alaska Native individual is suspected of having been exposed or having exposed other persons, or has been diagnosed with a notifiable condition listed under WAC 246-101-101 within that agency's jurisdiction, a local health jurisdiction, or Tribal jurisdiction in alignment with current public health tribal/local/state practice;
6. Data reports and data visualizations published prior to execution of this Agreement. No notification of exempted data use using the Tribal Nation Data Use Form is required;
7. Data analyses that are conducted to understand and correct data reporting interruptions or problems. No notification of exempted data use using the Tribal Nation Data Use Form is required;

Commented [KP19]: Principle 8

Commented [KP20]: GIHAC Principle 8 and sect. 6.4

Commented [KP21]: GIHAC Sect. 6.14

Commented [KP22]: Largely aligned with GIHAC checklist but where noted

Commented [KP23]: Addition - Exception to advance notice and consent for disease investigation even if DOH has reason to know the person may be a tribal member

8. Data analyses undertaken to address data quality concerns, such as to identify invalid data, missing or incomplete data. No notification of exempted data use using the Tribal Nation Data Use Form is required;
9. Any matter relating to United States v. Washington, 443 U.S. 658 (1979) or any related sub-proceeding, which includes but is not limited to the Tribal Shellfish Consent Decree. No notification of exempted data use using the Tribal Nation Data Use Form is required;
10. Whenever an authorized individual is requesting DOH information or records about a specific individual. No notification of exempted data use using the Tribal Nation Data Use Form is required; and
11. Any data request from Washington state local health jurisdictions. No notification of excepted data use using the Tribal Nation Data Use Form required.

Commented [KP24]: Addition to checlist

Commented [KP25]: Similar to checklist - just worded so that it could include a family member, ie, if authorized and allowed

Commented [KP26]: Exception addition - for other public health authorities

6. ACCESS TO DOH DATASETS/DATABASES

DOH is committed to ensuring access to data systems by utilizing current pathways and also prioritizing Tribal access when making operational improvements to data systems. Ongoing improvements will be discussed at the [TRIBE] and DOH DSA implementation meetings. The parties will also participate and track for potential alignment of efforts and activities related to Tribal DSAs organized by the Governor's Indian Health Advisory Committee.

Commented [KP27]: Principle 4: Equitable Access to Data

Access will begin with data systems followed by data extracts to allow for the development of streamlined processes and build understanding of data availability including strengths and limitations. DOH's commitment to uphold Tribal Data Sovereignty principles will develop sequentially to allow for continued exploration of improved pathways and processes. Access by [TRIBE] will be at the same level, if not greater, than other public health authorities, to the extent permitted by law.

Commented [KP28]: Section 7: Access to State Agency Datasets

A. Data access can include, but is not limited to the following DOH datasets, including upgraded systems to those datasets for [TRIBE]. DOH will provide data as outlined in its respective Exhibits for the purposes outlined in Section 1 of this Agreement:

Commented [KP29]: Section 7.4

- ❑ Notifiable Conditions: Washington Disease Reporting System (WDRS), Public Health Issue Management System (PHIMS)
- ❑ Emergency Department and Hospital Inpatient/Outpatient Data Repository: Rapid Health Information Network (RHINO)
- ❑ Birth Data: Washington Health and Life Events System (WHALES)
- ❑ Death Data: Washington Health and Life Events System (WHALES)
- ❑ Hospital Discharge Data: Comprehensive Hospital Abstract Reporting System (CHARS)
- ❑ Immunization Data: Washington State Immunization Information System (WA IIS)
- ❑ Survey Data: Behavioral Risk Factor Surveillance System (BRFSS), Healthy Youth Survey (HYS), Pregnancy Risk assessment Monitoring System (PRAMS)
- ❑ Cancer Registry

B. Future Dataset/Database Access. The [TRIBE] can choose to request access to additional DOH datasets

and databases, and any access provided to additional datasets and databases will be added in the form of an Exhibit and Appendices attached to this Agreement and executed by both parties.

7. AUTHORIZED USERS

The authorized users for the above-listed data/information are public health professionals and/or contracted staff working for the [TRIBE] who have signed the Use and Disclosure of Confidential Information form set forth in Appendix A.

8. USE OF DATA AND INFORMATION

A. This Agreement does not prevent [TRIBE] from conducting human subjects research, provided there is approval through official Tribal process, which may include approval by Tribal council, a Tribal Research Review, a Tribe's Institutional Review Board (IRB), or a designated office/committee/other IRB approval selected by the Tribe consistent with 45 C.F.R. § 46.

B. Data reporting must align with DOH's Small Numbers Guidelines (Appendix D).

C. [TRIBE] must use the data received or accessed under this DSA only to carry out the purpose and justification of this DSA as set out in Section 1, coupled with the specific purpose and justification listed in each Exhibit. Section 16 references state law that prescribes and restricts DOH's use of the data referenced in Section 6. [TRIBE] will use data in alignment with those laws and each Exhibit will reference authorized uses and restrictions in the applicable legal authorities listed in Section 16.

9. CONFIDENTIALITY

A. DOH and [TRIBE] agree to:

1. Follow DOH small numbers guidelines as well as dataset specific small numbers requirements. (Appendix D)

a. Limit access and use of the data/information:
   i. To the minimum amount of data/information
   ii. To the fewest people
   iii. For the least amount of time required to do the work
b. Ensure that all people with access to the data/information understand their responsibilities regarding it.
c. 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.
d. Retain a copy of the signed and dated "Use and Disclosure of Confidential Information" form as long as required in Data Disposition Section.

The parties to this Agreement acknowledge the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

10. SECURITY

Commented [KP30]: GIHAC Principle 7: Privacy and Security Protections (see section 13 also)

[TRIBE] 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."

[TRIBE] agrees to adhere to the Data Security Requirements in Appendix B and this data sharing agreement. [TRIBE] further assures that it has taken steps necessary to prevent unauthorized access, use, or modification of the information in any form.

11. ACCESS TO DATA/INFORMATION

The method and frequency of access will be specified within each Exhibit, specific to the unique dataset/database.

12. DATA DISPOSITION

[TRIBE] will destroy all copies of any data provided under this Agreement after the data has been used for the purposes specified in the Agreement and will send the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact. The DOH Business Contact will then provide the Certification of Data Disposition to the relevant data steward.

13. BREACH NOTIFICATION

[TRIBE] 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 Breach of Confidentiality of information covered by the Agreement.

The DOH Chief Information Security Officer (security@doh.wa.gov) shall notify the [TRIBAL CONTACT] within ten (10) business days of any suspected or actual Breach of Security or Breach of Confidentiality of information pertaining to [TRIBE]'s data/information/ For purposes of this section [TRIBE]'s data will be identified as[proxy], until a more representative proxy is identified by mutual agreement of DOH and [TRIBE], which could include consultation with other relevant partners. Any breach that includes [TRIBE]'s data or information will require a resubmission of the corresponding Tribal Nation Data Use Form.

14. RE-DISCLOSURE OF DATA/INFORMATION

The parties to this Agreement agree to not disclose in any manner all or part of the data/information identified in this Agreement except as the law requires or as this Agreement permits.

If DOH must comply with state or federal public record disclosure laws and receives a records request where all or part of the data/information subject to this Agreement is responsive to the request, DOH will notify [TRIBE] who is the subject of the data/information of the request no less than 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 party received the request; and
  - The DOH records that the party believes are responsive to the request and the identity of the requestor, if known.

15. ATTRIBUTION REGARDING DATA/INFORMATION

[TRIBE] agrees to cite "Washington State Department of Health" or other citation as specified, as the source of interpretations, calculations or manipulations of the data/information that are the subject of this Agreement in all text, tables and references in reports, presentations and scientific papers when DOH is the sole owner of the data/information.

16. STATUTORY AUTHORITY TO SHARE DATA/INFORMATION

The following is a non-exhaustive list of the laws authorizing DOH to obtain and disclose the confidential information or limited Dataset(s) identified in this Agreement to [TRIBE]:

RCW 43.20.050 – Powers and duties of state board of health
RCW 43.70.040 - Secretary's powers—Rule-making authority—Report to the legislature
RCW 43.70.050 – Collection, use, and accessibility of health-related data
RCW 43.70.052 – Hospital financial and patient discharge data
RCW 43.70.057 – Emergency department electronic reporting of syndromic surveillance data [RHINO data in Exhibit IV]
RCW 43.70.130 – Powers and duties of secretary--General
RCW 70.02.050 – Disclosure without patient's authorization
RCW 70.54.240 – Cancer registry program – Confidentiality
RCW 70.58A.520 – Vital Statistics [Death data in Exhibit III]
WAC 246-101 – Notifiable Conditions
WAC 246-102 – Cancer Registry
WAC 246-455 - Hospital patient discharge information reporting
WAC 246-492 – Vital Statistics Data Release [Death data in Exhibit III]

LOCATION OF DATA STORAGE

All data must be stored within the United States.

17. COMPLIANCE WITH DSA

Commented [KP31]: Section 8: Compliance with DSA (and breach language above)

Following the guidance of the Implementation plan:

A. DOH will establish written Tribal data sharing policies and procedures for DOH personnel who implement the requirements under this Agreement.
B. DOH will provide regular staff orientations and trainings on the policies and procedures referenced in subsection A under this section. Orientations and trainings shall include education and information on protecting Tribal data and information and use of the Tribal Nation Data Use Form.
C. DOH will work to ensure staff compliance with Tribal data sharing policies and address any violations in accordance with the DOH Tribal data sharing policies and procedures and DOH human resources policies and procedures.

18. AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement including all Exhibits and Appendices and the Tribal Nation Data Use Form 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.

This DSA is the first such agreement between DOH and a Tribe. In recognition of this, and in anticipation of other Tribes seeking and negotiating a Tribal DSA with DOH, either party may request amendments to this DSA based on new learnings, principles, or other inputs as statewide efforts continue in furtherance of Tribal data sovereignty.

19. CAUSE FOR IMMEDIATE TERMINATION

[TRIBE] and DOH acknowledge that unauthorized use or disclosure of the data/information, use of data inconsistent with this data sharing agreement and appendices, or any other violation of sections II or III, and appendices A or B, may result in the immediate termination of this Agreement.

20. CONFLICT OF INTEREST

The DOH may, by written notice to [TRIBE] terminate the right of [TRIBE]s 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 [TRIBE], or an agency or representative of [TRIBE], 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 this section, the DOH shall be entitled to pursue the same remedies against [TRIBE] as it could pursue in the event of a breach of the Agreement by [TRIBE]. 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 "consultation" clause of this Agreement.

21. NO WARRANTY

In no event shall the parties to this Agreement be liable for any damages, including, without limitation, damages resulting from lost data/information or lost profits or revenue, the costs of recovering such data/Information, the costs of substitute data/information, claims by third parties or for other similar costs, or any special, incidental, or consequential damages, arising out of the use of the data/information. The accuracy or reliability of the data/information is not guaranteed or warranted in any way and DOH disclaims liability of any kind whatsoever, including, without limitation, liability for quality, performance, merchantability and fitness for a particular purpose arising out of the use, or inability to use the data/information.

22. CONSULTATION

Except as otherwise provided in this Agreement, when a genuine dispute arises between the DOH and the [TRIBE] and it cannot be resolved or if DOH or [TRIBE] indicate on the Tribal Nation Data Use Form that Consultation is requested regarding the disapproval of a data use or the application of data use form exception, the following process will occur:

- The party invoking the consultation will submit in writing to the Office of Tribal Public Health and Relations at OTPHR@doh.wa.gov the disputed issues
- The parties will collaborate on the consultation process in honor of the government-to-government relationship
- During the consultation both parties will communicate in good faith and work to find a mutually agreeable resolution.
- This section does not diminish any rights or protections afforded to [TRIBE] or other Tribes under state or federal law, policy, and procedure including the right to elevate an issue of importance to any decision-making authority of another party.

23. EXPOSURE TO DOH BUSINESS DATA/INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO CONTRACT WORK

During the course of this contract, [TRIBE] may inadvertently become aware of data/information unrelated to this agreement. [TRIBE] will treat such data/information respectfully, recognizing DOH relies on public trust to conduct its work. This data/information may be handwritten, typed, electronic, or verbal, and come from a variety of sources.

24. REIMBURSEMENT TO DOH

Services to create and provide the data/information under this Agreement are provided at no charge to the [TRIBE], unless a program charges all requestors fees for the release of data, such as vital record fees

25. CHOICE OF LAW

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington, [TRIBE]s, 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:

- Federal statutes and rules, to the extent applicable;
- Applicable Washington state statutes and rules;
- [TRIBE] laws, to the extent applicable;
- Any other provisions of the Agreement, including materials incorporated by reference.

26. 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 [TRIBE] shall cooperate in the defense of tort lawsuits, when possible.

27. 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.

28. MONITORING

[TRIBE] will make itself and its facilities accessible if mandated by statue or audit to periodically monitor and evaluate performance, compliance, and/or quality assurance under the Agreement. DOH will request beforehand to come onto Tribal land and provide the reason for the visit.

29. 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.

30. 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.

31. TERMINATION

Either party may terminate this Agreement upon 30 days prior written notification to the other party.

32. WAIVER OF DEFAULT

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 both parties.

33. ALL WRITINGS CONTAINED HEREIN

The Agreement and attached Exhibit(s) contain all the terms and conditions agreed upon by the parties with the exception that additional Exhibits may be added in accordance with Section 6 of this Agreement.

34. ENTIRE AGREEMENT/OTHER AGREEMENT

This Agreement and the attached Exhibit(s) and Appendice(s) embody the entire Agreement between the parties hereto and supersedes all prior conversations, proposals, negotiations, understandings, and contracts/agreements, whether written or oral unless otherwise agreed to in writing by the parties. All exhibits and appendices hereto constitute part of this Agreement and are expressly incorporated herein.

35. TERM OF AGREEMENT AND EFFECTIVE DATE

A. **Effective Dates.** All provisions of this Agreement will be effective on the date of execution.

B. **Term of Agreement.** The term of this agreement shall be five years from the date of execution. After execution of this agreement, both parties may agree in writing to a different term or to renew the term of this agreement.

36. INCORPORATION OF EXHIBITS

The Attached Exhibits, and any additional Exhibits agreed to after the execution of this Agreement in accordance with Section 6 of this Agreement, are incorporated into this Agreement and are binding on DOH and [TRIBE].

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

State of Washington Department of Health [TRIBE]

_____ _____

_____	_____
Signature	Signature
_____	_____
Print Name	Print Name
_____	_____
Date	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 Authorized User 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 Authorized User 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 Authorized User's unauthorized use or disclosure of confidential information is the basis for the DOH immediately terminating the Agreement. The Authorized User 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 Confidential data and 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 organization's network must be done securely.

[TRIBE] 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 [TRIBE], access is controlled by the DOH, who will issue authentication credentials.

2. [TRIBE] will notify DOH immediately whenever:

    a) An authorized person in possession of such credentials is terminated or otherwise leaves the employ of [TRIBE];

    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 [TRIBE] 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 [TRIBE] 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 [TRIBE]'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 are 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 [TRIBE], 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

- DOH and [TRIBE] will aggregate data so that the need for suppression is minimal. [TRIBE] has the sovereign authority over its data to self-determine whether and how it will suppress data related to small numbers.
- DOH and [TRIBE] will suppress rates or proportions derived from those suppressed counts.
- DOH and [TRIBE] 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%).
- DOH's Small Number Standards are posted on the DOH website: Guidelines for Working With Small Numbers (wa.gov) (https://www.doh.wa.gov/Portals/1/Documents/1500/SmallNumbers.pdf).

APPENDIX E

TRIBAL NATION DATA USE FORM

Tribal Nation Data Use Form

The intent of the data use form is to provide information to [TRIBE] to process the data request. [TRIBE] may require additional information from the Department of Health Contact to determine if the form will be approved.

PART 1 – To be completed by Department of Health (DOH)

I. DOH Contact

Name: Title:

Program: Department:

Email: Phone:

II. DATA USE APPROVAL REQUEST OR TYPE OF NOTIFICATION

Is DOH requesting [TRIBE] approval to use the Tribal Nation's data? Or is DOH notifying the Tribal Nation of an exception use that is exempt from prior express written permission under Section 5E of the Tribal Data Sharing Agreement Between State of Washington Department of Health and [TRIBE]?

☐ Data Use Approval Request *(If this is an approval request, skip to Description of Data Use Request or Exempted Data Use Notification)*

☐ Notification of Exceptions – Exempted Data Use

Tribal Data Use Form Exceptions: Please specify the type of exempted use this notification qualifies for.

☐ A request under the Public Records Act (RCW 42.56.520).

☐ A WA State or federal statute or regulation prohibits or limits DOH compliance with Section 5 of the Tribal Data Sharing Agreement between State of Washington Department of Health and [TRIBE].

☐ A compulsory legal process, court order, a settlement, or a consent decree prohibits or limits DOH compliance with Section 5 of the Tribal Data Sharing Agreement between State of Washington Department of Health and [TRIBE].

☐ A contract, cooperative agreement, or grant agreement that predates this agreement that prohibits or limits DOH compliance with Section 5 of the Tribal Data Sharing Agreement between State of Washington Department of Health and [TRIBE].

☐ Sharing with a state agency, federal agency, local health jurisdiction, or Tribe when DOH receives notification that a Tribal citizen or American Indian or Alaska Native individual is suspected of having been exposed or having exposed other persons, or has been diagnosed with a notifiable condition listed under WAC 246-101-101 within that agency's jurisdiction, a local health jurisdiction, or Tribal jurisdiction in alignment with current public health tribal/local/state practice.

☐ [TRIBE]has shared that release of information (ROI) agreement exists between [TRIBE] and the third party.

III. DESCRIPTION OF DATA USE REQUEST OR EXEMPTED DATA USE NOTIFICATION

Brief title for data use approval request or notification of exempted data use

Date approval is needed (N/A, if this is a notification of exempted data use)

If approval is needed in less than 30 days from submission of this form, please provide justification for expedited approval (N/A, if this is a notification of exempted data use)

Is this a one-time use, or a recurring use?

☐ One-Time Use

☐ Recurring Use

Please describe the anticipated frequency of use (e.g., daily, monthly, annually, etc.)

What category of data (see definitions at link) does your data use require?

☐ **Category 1: Public Information**

☐ **Category 2: Sensitive Information**

☐ **Category 3: Confidential Information**

☐ **Category 4: Confidential information requiring special handling**

Has an Institutional Review Board (IRB) reviewed this data use?
An example of a specific IRB is the Washington State Institutional Review Board (WSIRB).

☐ Yes, determined to be exempt.

☐ Yes, approved by IRB.

☐ No, not a research project.

If so, which IRB?

Please describe with specificity [TRIBE] data to which this request or notification applies

Please describe how the data will be used (published, analyzed, shared, or used in research, etc.) and why it is necessary

Please describe any products that will be derived from this request or notification

Who will gain access to these data or to products that include or are derived from this data use?
Select all that apply

- [ ] **Internal – WA Department of Health Staff**
- [ ] **Other Public Health Authorities (WA DOH, LHJs, Tribes, Tribal Epidemiology Centers)**
- [ ] **General Public**
- [ ] **Other (Please Describe Below)**

Please provide any additional information that will be useful to [TRIBE] in their review.

TO BE COMPLETED BY [TRIBE] (Separate form)

Is the requested data use a responsible use of [TRIBE] data?

- ☐ **Yes**
- ☐ **No**

Do you approve or disapprove of this request (select all that apply)?

- ☐ Approve
- ☐ Disapprove
- ☐ Additional Information Needed from Requestor
- ☐ Request for Consultation
- ☐ Request Tribal Research Review. *See definition for **Tribal Research Review**
- ☐ [TRIBE] has an existing ROI or DSA that approves this data use
- ☐ N/A – This is a Notification of Exempted Data Use

Additional comments:

*Add section for attachments for proposers to add Research Proposal, IRB application, etc.