

Washington Department of Health

WA-DOH TDSA Template

This Template Tribal Data Sharing Agreement (TDSA) is an innovative process developed in partnership with Tribes and the Governor's Indian Health Advisory Council (GIHAC). Our goal is to work with each Tribe individually to establish their own TDSA between [Tribe] and WA-DOH, while also ensuring consistency in training and internal processes.

Tribes can visit the [Tribal Data Hub](#) to complete the External Data Request Form for Tribes or email the Tribal Data Team at WA-DOH at tribaldatateam@doh.wa.gov to initiate the process of developing a Tribal Data Sharing Agreement with WA-DOH.

To request access to the Partner Hub, email partnerhub@doh.wa.gov.

Template
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 the job title will receive contact even if the person in the role 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. [NAME OF TRIBAL JURISDICTION] and Washington State Department of Health (DOH) collect, manage, use, disclose, and safeguard Tribal data and information; and
- b. DOH shares confidential information or limited dataset(s) from the data and information referenced in Section 5 with [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 maintaining strong government-to-government relations with Tribes and honoring Tribal data sovereignty. DOH is dedicated to upholding Tribal data sovereignty principles in its approach to collecting and sharing of Tribal data. The department recognizes that, historically, Tribes have been excluded from access, control, and ownership of data collected by the state, and have been dependent on DOH (and others) for this data. This DSA represents a significant step toward fulfilling that commitment.

DOH's commitment to Tribal data sovereignty will continue to be reflected in its strategic planning as the department modernizes and invests in its data systems. DOH remains committed to working closely with Tribes across the state to expand and enhance 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 use of their own data, which is rooted in their 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, ensuring alignment with the Washington State Agency Privacy Principles.

2. DEFINITIONS

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

Authorized user means any 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 refers to the unauthorized access, use, or disclosure of information received under this Agreement. Disclosure can be either oral or written, in any form or medium.

Breach of security refers to the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. A good faith acquisition of personal information by an employee or agent of the agency for the agency's purposes is not considered a breach of security if the personal information is not further used or subject to unauthorized disclosure.

Business Day is the standard business hours of state offices, Monday through Friday, from 8:00 a.m. to 5:00 p.m., excluding state holidays.

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

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

Data refers to a subset of Information, including representations of knowledge, facts, concepts, computer software and programs, or instructions. Data may exist in any form, whether stored on physical media, in a computer’s memory, in transit, or displayed on a device.

Data storage refers to electronic media on which information is recorded, such as CDs, DVDs, computers, or similar devices.

Data transmission refers to the process of transferring data and/or information across a network from a sender (or source) to one or more destinations.

Direct identifier refers to an attribute that, by itself, enables unique identification of an individual within a specific operational context.

Disclosure means allowing access to, or the release, transfer, or other communication of confidential data or information by any means, including oral, written, or electronic, to any party other than the party identified or the party that provided or created the record.

Encryption refers to the use of algorithms to encode data, making it unreadable without a specific piece of information, commonly referred to as a “key”. Depending on the type of data or information being shared, encryption may be required during data transmissions and/or data storage.

Health care information refers to 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.

Health information includes any data or information related to health behaviors, human exposure to environmental contaminants, health status, and health care. It encompasses health care information as defined in RCW 70.02.010 and health-related data as defined in RCW 43.70.050.

Health Information Exchange (HIE) refers to 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 conducting human subjects research to ensure that: the rights and welfare of human subjects are adequately protected; the risks to human subjects are minimized, reasonable, and outweighed by the potential benefits to them or the knowledge gained; and the proposed study design and methods are appropriate in relation to the stated research objectives. Research involving human subjects or their identifiable personal records must be reviewed and approved by an Institutional Review Board (IRB) in accordance with federal and state laws, regulations, and state agency policies.

Human subject refers to a living individual about whom an investigator (whether a 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 refers to variables that, when combined with other information, may be used to create identifiable data or records about an individual.

Information refers to data that has been processed, organized, and structured, often accompanied by an interpretation of its meaning. This includes concepts and constructs.

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

Linked data refers to the process of 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 refers to information that includes indirect identifiers that may link an individual to that person's health care information. Examples include birth dates, admission, treatment, diagnosis dates, healthcare facility codes, and other data elements that may identify an individual. These identifiers may vary depending on factors such as geographical location or the rarity of a person's health condition, age, or other characteristic.

Publishing means distributing or making available a work product to the public in a physical or electronic form.

Research refers to 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 Tribe's determination.

Restricted confidential information refers to confidential information that is subject to particularly strict handling requirements due to statutes, rules, regulations, or contractual agreements. Violations may result in enhanced legal sanctions.

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

Tribal Data refers to data or information specific to an individual Tribe, including public or private data about a Tribe or its people, subject to Tribal rights of ownership and control. Tribal data also includes, but is not limited to, information about the Tribe's membership, affiliation, events, conditions within the Tribe's jurisdiction and lands, and information about Tribal members or any individuals living within the Tribe's jurisdiction. It also includes data regarding Tribal census tracts, Tribal land, and Tribal facilities, entities, and enterprises and any individuals they serve.

Tribal Data Sovereignty refers to the inherent legal authority of Tribes to:

- Manage the collection, ownership, application, and interpretation of Tribal data, 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 Tribal members, is used or shared with third parties.
- Have the same or additional access to state data as other public health jurisdictions to carry out their governmental duties; and
- Be notified by other entities holding Tribal data of data breaches and informed about policies related to data disposition, security, confidentiality, storage, and human subjects research limitations.

Tribal Research Review refers to an entity selected by a Tribe to review research to protect the interests of Tribal members and the Tribal community, similar to a Tribal Institutional Review Board. Tribes have the authority to determine when research occurs, which may follow federal and 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 under the Alaska Native Claims Settlement Act (43 U.S.C. Sec. 1601 et seq.), recognized as eligible for special programs and services provided by the United States due to their status as Indians.

Washington State Institutional Review Board refers to the institutional review board designated by the Department to review research proposals in accordance with 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 within the jurisdiction of 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 powers granted to public health authorities that exceed those of non-governmental public health authorities.

4. OWNERSHIP OF DATA

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

- a. Unless otherwise required by law, the [TRIBE] and DOH shall have joint ownership of data and information in DOH data systems concerning [TRIBE], its Tribal citizens, and persons residing within the [TRIBE]'s jurisdiction under this Agreement.
- b. Unless otherwise required by law, this Agreement does not limit the [TRIBE]'s ownership of data and information under its authority as a sovereign nation; and
- c. This Agreement does 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 outlines the conditions under which DOH collects, manages, uses, discloses, and safeguards [TRIBE]'s information and data. Tribes have the right to informed consent regarding how their data, including protected health information about Tribal members, is used or shared with Third Parties.

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

A. Protection of [TRIBE]'s Data and Information. For the purposes of this section, [TRIBE]'s data will be referred to as [PROXY], until a more appropriate proxy is mutually agreed upon by DOH and [TRIBE], which may include consultation with other relevant partners. DOH must obtain permission by using the Tribal Nation Data Use Form (Appendix E), to be completed by [contact], under the following conditions:

1. Publishing and Reports: Prior to DOH publishing data/information that is known or should reasonably be known to be [TRIBE]'s data or information, in a manner that allows identification as [TRIBE]'s, including, but not limited to, republishing data or information from public sources (such as social media, research publications, and online documents);
2. Data Sharing: Prior to sharing data/information that is known or should reasonably be known to be [TRIBE]'s data with a Third Party and/or releasing data/information from [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 made publicly available via sources such as social media, research publications, and/or online documents. DOH may also share data with a Third Party if [TRIBE] has an existing release of information (ROI) or data sharing agreement with the Third Party.
3. Research: Prior to researching [TRIBE]'s data/information in a manner that includes [TRIBE] membership or association or that can uniquely identify [TRIBE]. [TRIBE] may also request prior review by a Tribal Research Review; and
4. Analysis: Prior to analyzing [TRIBE]'s data/information in a manner that includes [TRIBE]'s membership or association or can uniquely identify the [TRIBE].
5. Upon written request from [TRIBE] to DOH's Business Contact or their designee, stating 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 apply to [TRIBE]'s data. Addendums incorporating Tribal Data Sovereignty principles, modeled after the Governor's Indian

Health Advisory Council's (GIHAC) Data Sovereignty Principles, will be added when new DSAs are created, upon the renewal of existing agreements, or no later than January 24, 2030.

- C. Timelines for Submitting Tribal Nation Data Use Form. The [TRIBE] will respond within 30 days after receiving the Tribal Nation Data Use Form. If [TRIBE] does not respond within this period, the DOH request will be considered approved. If DOH needs an expedited process, approval may be requested earlier, with justification provided. DOH will include in the Tribal Nation Data Use Form the date by which a response is needed from [TRIBE] in relation to any deadlines. If [TRIBE] does not respond by the requested deadline, the DOH request will be deemed approved.
- D. Prohibited Collection of Data. Unless otherwise stated in this agreement or 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 outlines exceptions when DOH is not required to seek prior express written permission under Section 5 or be prohibited from sharing information under Section 5(D). However, unless otherwise stated, DOH will still be required to notify [TRIBE] using the Tribal Nation Data Use Form (Appendix E) as soon as DOH becomes aware that the data or information involves [TRIBE]'s data. 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's compliance with Section 5.
 3. Compulsory legal processes, court orders, settlements, or consent decrees that prohibit or limit DOH's compliance with Section 5.
 4. A contract, cooperative agreement, or grant agreement that predates this agreement, which prohibits or limits DOH's 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/Alaska Native individual is suspected of exposure 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 practices.
 6. Data reports and visualizations published prior to the execution of this Agreement. No notification via the Tribal Nation Data Use Form is required.
 7. Data analyses conducted to understand and correct data reporting interruptions or issues. No notification via the Tribal Nation Data Use Form is required.
 8. Data analyses undertaken to address data quality concerns, such as identifying invalid, missing, or incomplete data. No notification via 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, including but not limited to the Tribal Shellfish Consent Decree, shall not require notification of exempted data use using the Tribal Nation Data Use Form.
 10. When an authorized individual requests DOH information or records about a specific individual. No notification via the Tribal Nation Data Use Form is required; and
 11. Any data request made by Washington state local health jurisdictions. No notification via the Tribal Nation Data Use Form required.

6. ACCESS TO DOH DATASETS/DATABASES

DOH is committed to ensuring equitable access to data systems by utilizing existing pathways while prioritizing Tribal access in operational improvements to data systems. Ongoing improvements will be discussed during the [TRIBE] and DOH DSA implementation meetings. The parties will also monitor and track efforts for potential alignment of activities related to Tribal DSAs organized by the Governor's Indian Health Advisory Council.

Access will begin with data systems, followed by data extracts, to facilitate the development of streamlined processes and to build understanding of data availability, including strengths and limitations. DOH's commitment to upholding Tribal Data Sovereignty principles will evolve progressively, enabling continued exploration of improved pathways and processes. Access by [TRIBE] will be at least on par with, or greater than, other public health authorities, to the extent permitted by law.

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

- ☐ 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] may request access to additional DOH datasets and databases. Any access granted will be formalized through an Exhibit and Appendices attached to this Agreement and executed by both parties.

7. AUTHORIZED USERS

The authorized users of the data/information listed above 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 it receives approval through an official Tribal process. This may include approval by the Tribal Council, a Tribal Research Review, a Tribe's Institutional Review Board (IRB), or any designated office, committee, or IRB selected by the Tribe in accordance with 45 C.F.R. § 46.
- B. Data reporting must adhere to DOH's Small Numbers Guidelines (Appendix D).
- C. [TRIBE] must use the data received or accessed under this Agreement solely for the purposes outlined in Section 1 and any specific purposes and justification identified in each Exhibit. Section 16 references state law, which prescribes and restricts DOH's use of the data described in Section 6. [TRIBE] agrees to use data in accordance with these laws, and each Exhibit will reference authorized uses and restrictions in the applicable legal authorities as detailed in Section 16.

9. CONFIDENTIALITY

A. DOH and [TRIBE] agree to:

- 1. Adhere to DOH's Small Numbers Guidelines and any dataset-specific Small Numbers requirements. (Appendix D).
 - a. Limit access and use of the data/information:
 - i. To the minimum necessary amount of data/information,
 - ii. To the fewest number of individuals necessary, and
 - iii. For the shortest duration required to complete the work
 - b. Ensure that all individuals with access to the data/information understand their responsibilities regarding the information.
 - c. Ensure that every individual (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 data.
 - d. Retain a copy of the signed and dated "Use and Disclosure of Confidential Information" form as required in the Data Disposition Section.

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

10. SECURITY

[TRIBE] assures that its security practices and safeguards meet Washington State Office of Washington Technology Solutions (WaTech) security standard 141.10 [Securing Information Technology Assets](#).

For purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates satisfies WaTech 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 implemented necessary measures to prevent unauthorized access, use, or modification of the data/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 it has been used for the purposes specified in the Agreement. [TRIBE] will send the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact, who will forward to relevant data steward.

13. BREACH NOTIFICATION

[TRIBE] shall notify the DOH Chief Information Security Officer (security@doh.wa.gov) within one (1) business day of any suspected or actual Breach of Security or Breach of Confidentiality involving data covered by this Agreement.

The DOH Chief Information Security Officer (security@doh.wa.gov) shall notify [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 the purpose of this section, [TRIBE]'s data will be identified as [proxy], until a more representative proxy is identified by mutual agreement between DOH and [TRIBE], which may involve consultation with relevant partners. Any breach involving [TRIBE]'s data or information will require the resubmission of the corresponding Tribal Nation Data Use Form.

14. RE-DISCLOSURE OF DATA/INFORMATION

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

If DOH is required to comply with state or federal public record disclosure laws and receives a request for records where all or part of the data/information covered by this Agreement is responsive, DOH will notify [TRIBE] of the request at least ten (10) business days before disclosing the data to the requestor.

The notice will include:

- Written notification;
- A copy of the request or another document showing:
 - The date the request was received;
 - The DOH records believed to be responsive to the request; and

- The identity of the requester, 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 subject to 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 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

WAC 246-101-615 (3) – Data dissemination and notification – Department - Notifiable Conditions

WAC 246-102-070 – Access and release of information - Cancer Registry

WAC 246-455-085 - Data files—Release of data files and data use agreements - Hospital patient discharge information reporting

WAC 246-492-200 – Requests from government agencies for birth and fetal death record data that contains direct identifiers for non-research public health purposes. - Vital Statistics Data Release

LOCATION OF DATA STORAGE

All data must be stored within the United States.

17. COMPLIANCE WITH DSA

Following the guidance of the Implementation plan:

- A. DOH will establish written Tribal data sharing policies and procedures for DOH personnel implementing the requirements under this Agreement.
- B. DOH will provide regular staff orientations and training on the policies and procedures referenced in subsection A. These orientations and training will include education on protecting Tribal data and the 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, as well as DOH human resources policies and procedures.

18. AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement, including all Exhibits, Appendices, and the Tribal Nation Data Use Form may be amended by mutual agreement of the parties. Such amendments will not be binding unless made in writing and signed by personnel authorized to bind each party.

In recognition that this is a new type of DSA, and with anticipation that other Tribes may seek and negotiate a Tribal DSA with DOH, either party may request amendments based on new learnings, principles, or other inputs as statewide efforts advance 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 its 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 [TRIBE]'s right 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 DOH with the intent of securing this Agreement or gaining favorable treatment in relation to the awarding, amending, or making of any determination regarding this Agreement.

In the event this Agreement is terminated as provided in this section, DOH may pursue the same remedies it could pursue in the event of a breach of the Agreement by [TRIBE]. The rights and remedies of DOH under this section are in addition to any other rights and remedies provided by law. Any determination made by the Contracting Office under this clause 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 arising from lost data/information, 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 from the use of the data/information. DOH does not guarantee the accuracy or reliability of the data/information in any way and disclaims all liability, including, but not limited to 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, if a genuine dispute arises between DOH and [TRIBE] that cannot be resolved, or if DOH or [TRIBE] indicate on the Tribal Nation Data Use Form that Consultation is

requested regarding the disapproval of data use or the application of a data use form exception, the following process will apply:

- The party invoking Consultation will submit a written request outlining the disputed issues to the Office of Tribal Public Health and Relations at OTPHR@doh.wa.gov.
- The parties will collaborate in the Consultation process, respecting the government-to-government relationship.
- During Consultation, both parties will communicate in good faith and work toward finding 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, or procedure, including the right to elevate an issue 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 Agreement, [TRIBE] may inadvertently become aware of data or information unrelated to this contract. [TRIBE] agrees to treat such data with respect, recognizing that DOH relies on public trust to conduct its work. This data/information may be handwritten, typed, electronic, or verbal form and may come from a variety of sources.

24. REIMBURSEMENT TO DOH

Services for creating and providing data/information under this Agreement will be provided to [TRIBE] at no charge, unless a program generally charges fees for data requests, such as vital record fees.

25. CHOICE OF LAW

This Agreement is entered into pursuant to the authority granted by the laws of the state of Washington, [TRIBE]'s law, and any applicable federal laws. The provisions of this Agreement shall be construed in accordance with these laws.

In the event of any inconsistency between the terms of this Agreement 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]'s 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 [TRIBE] shall cooperate in the defense of tort lawsuits when possible.

27. NON-WAIVER OF SOVEREIGN IMMUNITY

By contracting with the DOH, neither party waives any rights, including treaty rights, immunities (including sovereign immunity), or jurisdiction. This agreement does not diminish any rights or protections afforded either party under State or Federal law.

28. LIMITATION OF AUTHORITY

Only the Authorized Signatory for DOH has the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of DOH. No alteration, modification, or waiver of any clause or condition of this Agreement shall be effective or binding unless made in writing and signed by the Authorized Signatory for DOH.

29. MONITORING

[TRIBE] agrees to make itself and its facilities accessible for periodic monitoring and evaluation of performance, compliance, and/or quality assurance under this Agreement, if mandated by statute or audit. DOH will request permission to enter Tribal land in advance and will provide the reason for the visit.

30. SEVERABILITY

If any term or condition of this Agreement is held invalid, the invalidity will not affect the validity of the other terms or conditions, provided that the remaining terms and conditions can still be fairly given effect.

31. SURVIVORSHIP

The terms and conditions of this Agreement that, by their nature and context, are intended to survive the completion, cancellation, termination, or expiration of the Agreement shall remain in effect.

32. TERMINATION

Either party may terminate this Agreement by providing 30 days' prior written notice to the other party.

33. WAIVER OF DEFAULT

Failure or delay by either party in exercising any right, power, privilege, or remedy under this Agreement shall not constitute a waiver of such right, power, privilege, or remedy. No provision of this Agreement may be waived except in writing signed by both parties.

34. ALL WRITINGS CONTAINED HEREIN

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

35. ENTIRE AGREEMENT/OTHER AGREEMENT

This Agreement, together with the attached Exhibits and Appendices, represents the complete and final understanding between the parties and supersedes all prior discussions, proposals, negotiations, understandings, and contracts/agreements, whether written or oral, unless otherwise agreed to in writing by the parties. All Exhibits and Appendices are considered integral parts of this Agreement and are expressly incorporated herein.

36. 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. Following execution, both parties may mutually agree in writing to a different term or to renew the term of this agreement.

37. INCORPORATION OF EXHIBITS

The Attached Exhibits, as well as any additional Exhibits agreed to after the execution of this Agreement in accordance with Section 6, are incorporated into binding upon both 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

TEMPLATE

APPENDIX A

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

People with access to confidential information are responsible for understanding and adhering to the laws, policies, procedures, and practices that govern its use. The following outlines key elements:

A. CONFIDENTIAL INFORMATION

Confidential information refers to data protected from public disclosure by federal and state laws. Examples include Social Security numbers and identifiable healthcare information as defined under RCW 70.02. The general public disclosure law, including exemption, is outlined in RCW 42.56.

B. ACCESS AND USE OF CONFIDENTIAL INFORMATION

1. Access to confidential information must be restricted to individuals whose job responsibilities specifically require it.
2. Use of confidential information is limited to purposes explicitly defined 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 the individual or their personal representative, consistent with applicable laws.
2. An Authorized User may only disclose an individual's confidential information as permitted under the **Re-Disclosure of Information** section of this Agreement, and in compliance with relevant state and federal laws.

D. CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE

An Authorized User's unauthorized use or disclosure of confidential information will result in the immediate termination of the Agreement by DOH. The Authorized User may also be subject to administrative, civil, and criminal penalties as defined by 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 applied using industry-standard algorithms validated by the NIST Cryptographic Algorithm Validation Program. The encryption must render the data unusable to anyone except authorized personnel, and the encryption key or other means to decipher the information must be protected from unauthorized access. All manipulations or transmissions of data within the organization's network must be securely handled.

[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 kept in a secured environment 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 in 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 dictionary word, although a passphrase may be used.
 - Do not include personal information (e.g., birthdates, pets' names, addresses, etc.).
 - Must be unique and not reused across multiple systems and accounts.
 - Must be 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 outlined in 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 or Solid-State Drives. Temporary storage refers to thirty (30) days or less.
2. Access to the data is restricted to authorized users by requiring login to the local workstation using a unique user ID and a complex password, or other authentication mechanisms providing equivalent or greater security, such as biometrics or smart cards. Accounts must lock after five (5) unsuccessful access attempts and remain locked for at least 15 minutes, or until an administrator manually resets the account.

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 include smart phones, tablets, laptops, notebook or netbook computers, and personal media players.
2. Examples of portable storage media include 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 when left unattended and set to automatically lock after no more than 3 minutes of inactivity.
 - 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 that is only accessible to authorized personnel. When not in use, such records are stored in a locked container, for example, 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:

Hard Disk Drives / Solid State Drives

Paper documents with Confidential or Restricted information

Optical discs (e.g. CDs or DVDs)

Magnetic tape

Is destroyed by:

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.

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.

Incineration, shredding, or completely defacing the readable surface with a course abrasive.

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.

TEMPLATE

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 crosscut 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 to minimize the need for suppression. [TRIBE] retains sovereign authority over its data and has the right to self-determine whether and how to suppress data related to small numbers.
- DOH and [TRIBE] will suppress rates or proportions derived from suppressed counts.
- DOH and [TRIBE] will ensure that suppressed cells cannot be recalculated through subtraction, 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, no suppression is required for the weighted survey estimates.
- When a survey includes less than 80% of the eligible population, and the respondents are equally weighted, survey estimates based on fewer than 10 respondents should be “top-coded” (estimates 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) (<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.